ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

ĐỖ NGỌC THỦY

CƠ SỞ GRÖBNER
VÀ GIẢI HỆ PHƯƠNG TRÌNH ĐA THỨC

LUẬN VĂN THẠC SỸ KHOA HỌC TOÁN HỌC

Thái Nguyên - 2012

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

ĐỖ NGỌC THỦY

CƠ SỞ GRÖBNER
VÀ GIẢI HỆ PHƯƠNG TRÌNH ĐA THỨC

LUẬN VĂN THẠC SỸ KHOA HỌC TOÁN HỌC
Chuyên ngành : Phương pháp toán sơ cấp
Mã số: 60.46.40

Người hướng dẫn khoa học:
PGS.TS. Tạ Duy Phượng

Thái Nguyên - 2012

Mục lục

Chương 1. Cơ sở Gröbner 4

1.1. Cấu trúc đại số cơ bản 4

1.1.1. Vành 4
1.1.2. Ideal 6
1.1.3. Trường 7

1.2. Vành đa thức 8

1.2.1. Đa thức và bậc đa thức 8
1.2.2. Định lý Hilber về cơ sở 10
1.2.3. Đa thức một biến 11
1.2.4. Iđêan đơn thức 13

1.3. Cơ sở Gröbner 14

1.3.1. Thứ tự từ 14
1.3.2. Một số thứ tự từ 16
1.3.3. Từ khởi đầu, đơn thức đầu 18
1.3.4. Ideal khởi đầu 20
1.3.5. Định nghĩa cơ sở Gröbner 21
1.3.6. Thuật toán chia 26
1.3.7. Tiêu chuẩn Buchberger 28
1.3.8. Thuật toán Buchberger 35

Chương 2. Hệ phương trình đa thức 38

2.1. Nghiệm của hệ phương trình đa thức 38

2.2. Cách giải hệ phương trình đa thức 40

2.3. Các hàm liên quan tới Gröbner của Maple 49

Chương 3. Giải hệ phương trình đa thức 56

Kết luận 72

Tài liệu tham khảo 73

Phụ lục 75

MỞ ĐẦU

Lý thuyết cơ sở Gröbner được nghiên cứu lần đầu tiên vào khoảng thập kỉ 60 của thế kỉ 20, nó nhanh chóng trở thành hạt nhân của ngành Đại số máy tính (Computer Algebra) và là một công cụ hữu hiệu trong rất nhiều bài toán cơ bản của Đại số giao hoán, Hình học đại số. Dưới sự hướng dẫn của Giáo sư Wolfgang Gröbner, năm 1965, Bruno Buchberger đã đưa ra thuật toán Buchberger trong luận án tiến sĩ của mình. Điểm mấu chốt khởi đầu cho sự hình thành lý thuyết của Buchberger chính là việc mở rộng thuật toán chia hai đa thức một biến sang trường hợp các đa thức nhiều biến. Cơ sở Gröbner về phương diện lý thuyết còn được khẳng định bằng việc cung cấp chứng minh cho ba định lý của Hilbert: Định lý Hilbert về cơ sở, Định lý Hilbert về xoắn và Định lý Hilbert về không điểm.

Trong các ứng dụng gần gũi nhất của lý thuyết cơ sở Gröbner, chúng tôi quan tâm tới việc giải hệ phương trình đa thức. Thực chất việc tìm cơ sở Gröbner của một hệ phương trình đa thức là đưa hệ phương trình ban đầu về một hệ phương trình mới có dạng tam giác. Từ đó ta tìm được nghiệm của hệ. Dưới góc độ của một giáo viên phổ thông, hy vọng đề tài này sẽ đem đến cho chúng tôi cơ hội được học hỏi thêm nhiều hơn các công cụ toán học hiện đại, góp phần soi sáng cho những nội dung liên quan trong chương trình toán phổ thông.

- Luận văn *Cơ sở Gröbner và giải hệ phương trình đa thức* có mục đích cung cấp cho giáo viên phổ thông, các em học sinh và những người yêu toán một hướng tiếp cận mới, một công cụ giải hệ phương trình đa thức, một phương pháp chung cho hầu hết các bài toán dạng này. Luận văn cũng cung cấp cho người sử dụng một số hàm quan trọng

trong Maple liên quan tới cơ sở Gröbner.

- Luận văn gồm ba Chương.
- *Chương 1*: Trình bày tổng quan lý thuyết cơ sở Gröbner.
- *Chương 2*: Trình bày điều kiện có nghiệm và cách giải tổng quát hệ phương trình đa thức.
- *Chương 3*: Trình bày một số hệ phương trình đa thức được giải dựa vào cơ sở Gröbner và các hàm liên quan tới cơ sở Gröbner trong Maple.

Luận văn được hoàn thành dưới sự hướng dẫn của PGS TS Tạ Duy Phượng. Tác giả xin bày tỏ lòng kính trọng và biết ơn thầy hướng dẫn đã tận tình giúp đỡ tác giả trong suốt quá trình tập dượt nghiên cứu và viết luận văn.

Tác giả xin trân trọng cảm ơn các thầy cô giáo trường Đại học khoa học - Đại học Thái Nguyên và các thầy cô giáo Viện Toán học đã tận tâm giảng dạy và giúp đỡ tác giả hoàn thành khóa học.

Đồng thời tác giả xin chân thành cảm ơn Trường THPT Bạch Đằng - Hải Phòng, nơi tác giả đang công tác, các đồng nghiệp, gia đình và bạn bè đã động viên, giúp đỡ và tạo điều kiện về mọi mặt trong quá trình học tập.

Thái Nguyên, tháng 07 năm 2012

Chương 1

Cơ sở Gröbner

1.1. Cấu trúc đại số cơ bản

1.1.1. Vành

Định nghĩa 1.1.1 Vành là một tập hợp $R \neq \emptyset$ được trang bị phép toán cộng "+": $(a,b) \mapsto a+b$ và phép toán nhân ".": $(a,b) \mapsto a.b$ thỏa mãn các tính chất sau:

(i) Đối với phép cộng, R là một nhóm giao hoán.

(ii) Phép nhân có tính kết hợp, tức là với mọi $a,b,c \in R$:

$$a.(b.c) = (a.b).c$$

(iii) Phép nhân có tính chất phân phối đối với phép cộng, tức là $a,b,c \in R$:

$$a.(b+c) = a.b + a.c \text{ và } (b+c).a = b.a + c.a.$$

Phần tử "không" của vành được kí hiệu là 0. Để cho tiện, thông thường ta viết ab thay cho tích $a.b$. R được gọi là vành có đơn vị nếu nó chứa phần tử 1 thỏa mãn $a1 = 1a = a$ với mọi $a \in R$. Khi cần nhấn mạnh vành R ta dùng kí hiệu $0_R, 1_R$ để chỉ các phần tử không và đơn vị của R. Vành R được gọi là vành giao hoán nếu với mọi $a,b \in R, ab = ba$. Trong luận văn này ta chỉ xét đến vành giao hoán, có đơn vị. Do đó vành luôn hiểu theo nghĩa này.

Ví dụ :

1. Tập số nguyên $\mathbb{Z}$, số thực $\mathbb{R}$, số phức $\mathbb{C}$, với các phép cộng và phép nhân thông thường lập thành các vành. Tuy nhiên tập $\mathbb{N}$ không phải là vành.

2. Tập $R[x]$ các đa thức một biến x với hệ số thực lập thành một vành.

Định nghĩa 1.1.2 Cho R là một vành và $a \in R$. Phần tử a được gọi là:

(i) ước của không nếu $a \neq 0$ và tồn tại $0 \neq b \in R$ sao cho $ab = 0$.

(ii) khả nghịch (hoặc đơn vị) nếu tồn tại $c \in R$ sao cho $ac = 1$.

Vành R không chứa ước của 0 được gọi là *miền nguyên*.

Ví dụ :

Vành $\mathbb{Z}$ là miền nguyên với hai phần tử đơn vị là 1 và -1.

Định nghĩa 1.1.3 Giả sử R là một vành, A là một bộ phận ổn định của R đối với hai phép toán trong R nghĩa là $x+y \in A$ và $xy \in A$ với mọi $x, y \in A$. A là một vành con của vành R nếu A cùng với hai phép toán cảm sinh trên A là một vành.

Định lý 1.1.4 Giả sử A là một bộ phận khác rỗng của vành R. Các điều kiện sau đây là tương đương:

(i) A là một vành con của vành R.

(ii) Với mọi $x, y \in A$, $x+y \in A$, $xy \in A$, $-x \in A$.

(iii) Với mọi $x, y \in A$, $x-y \in A$, $xy \in A$.

1.1.2. Ideal

Định nghĩa 1.1.5 Cho R là một vành. Tập con $I \neq \emptyset$ của R được gọi là *iđêan* nếu hai điều kiện sau thỏa mãn:

(i) Với mọi $a, b \in I$, $a + b \in I$.

(ii) Với mọi $a \in I$ và $r \in R$, $ra \in I$.

Ví dụ :

1. Mọi vành R đều chứa iđêan tầm thường $I = 0$ và chính nó $I = R$.

2. Tập $n\mathbb{Z}$ là các iđêan trong vành $\mathbb{Z}$.

Định nghĩa 1.1.6 Ta gọi là *đêan trái (iđêan phải)* của một vành R, là một vành con A của R thỏa mãn điều kiện $xa \in A\,(ax \in A)$ với mọi $a \in A$ với mọi $x \in R$. Một vành con A của vành R gọi là một *iđêan* của R nếu và chỉ nếu A vừa là iđêan trái, vừa là iđêan phải của R.

Định lý 1.1.7 Một tập A khác rỗng của một vành R là một iđêan của R nếu và chỉ nếu các điều kiện sau thỏa mãn:

(i) $a - b \in A$ với mọi $a, b \in A$.

(ii) $xa \in A$, $ax \in A$ với mọi $a \in A$ và mọi $x \in X$.

Ví dụ :

1. Tập $\{0\}$ và X là hai iđêan của vành X.

2. Tập $m\mathbb{Z}$ gồm các số nguyên là bội của một số nguyên m cho trước.

Định lý 1.1.8 Giao của một họ bất kì những iđêan của một vành R là một iđêan của R.

Định lý 1.1.9 Giả sử X vành giao hoán có đơn vị và $a_1, a_2, ..., a_n \in X$. Bộ phận A của X gồm các phần tử có dạng $x_1a_1 + x_2a_2 + ... + x_na_n$ với

$x_1, x_2, ..., x_n \in X$ là iđêan của X sinh bởi $a_1, a_2, ..., a_n$.

1.1.3. Trường

Định nghĩa 1.1.10 Ta gọi trường là một miền nguyên R trong đó mọi phần tử khác 0 đều có một nghịch đảo trong vị nhóm nhân R. Vậy một vành R giao hoán, có đơn vị, có nhiều hơn một phần tử là một trường nếu và chỉ nếu $R\setminus\{0\}$ là một nhóm đối với phép nhân của R.

Ví dụ :

Tập hợp $\mathbb{Q}$ các số hữu tỉ cùng với phép cộng và phép nhân các số là một trường. Ta cũng có trường số thực $\mathbb{R}$ và trường số phức $\mathbb{C}$.

Định nghĩa 1.1.11 Giả sử X là một trường, A là một bộ phận của X ổn định đối với hai phép toán trong X. A gọi là một *trường con* của trường X nếu A cùng với hai phép toán cảm sinh trên A là một trường.

Định lý 1.1.12 Giả sử A là một bộ phận có nhiều hơn một phần tử của một trường X. Các điều kiện sau đây là tương đương:
(i). A là một trường con của trường X.
(ii). Với mọi $x, y \in A$, $x+y \in A$, $xy \in A$, $-x \in A$, $x^{-1} \in A$ nếu $x \neq 0$.
(iii). Với mọi $x, y \in A$, $x-y \in A$, $xy^{-1} \in A$ nếu $y \neq 0$.

Ví dụ :

1 . X là một trường con của trường X. Bộ phận $\{0\}$ không phải là một trường con của X, vì theo định nghĩa một trường có ít nhất hai phần tử.

2 . Trường số hữu tỉ $\mathbb{Q}$ là trường con của trường số thực $\mathbb{R}$, bản thân $\mathbb{R}$ lại là trường con của trường số phức $\mathbb{C}$.

1.2. Vành đa thức

1.2.1. Đa thức và bậc đa thức

Cho R là một vành và $x_1, x_2, ..., x_n$ $(n \geqslant 1)$ là các biến. Ta gọi *đơn thức* là một biểu thức có dạng $x_1^{a_1}...x_n^{a_n}$ trong đó $a_i \in N$, $i = 1, .., n$ được gọi là bộ số mũ của đơn thức. Nếu $a_1 = ... = a_n = 0$ thì đơn thức được kí hiệu là 1. Phép nhân trên tập các đơn thức được định nghĩa như sau

$$\left(x_1^{a_1}...x_n^{a_n}\right)\left(x_1^{b_1}...x_n^{b_n}\right) = x_1^{a_1+b_1}...x_n^{a_n+b_n}.$$

Từ là biểu thức có dạng $\alpha x_1^{a_1}...x_n^{a_n}$, trong đó $\alpha \in R$ gọi là hệ số của *từ*. Hai từ khác không $\alpha x_1^{a_1}...x_n^{a_n}$ và $\beta x_1^{a_1}...x_n^{a_n}$ là *đồng dạng* với nhau.

Để cho tiện ta kí hiệu $x = (x_1, ...x_n)$, $a = (a_1, ..., a_n) \in N^n$ và $x^a = x_1^{a_1}...x_n^{a_n}$. Đa thức n biến $x_1, ..., x_n$ trên vành R là một tổng hình thức của các từ:

$$f(x) = \sum \alpha_a x^a,$$

trong đó chỉ có hữu hạn hệ số $\alpha_a \neq 0$. Từ $\alpha_a x^a$ với $\alpha_a \neq 0$ được gọi là từ của đa thức $f(x)$ và x^a là đơn thức của $f(x)$.

Hai đa thức $f(x) = \sum_{a \in N^n} \alpha_a x^a$ và $g(x) = \sum_{a \in N^n} \beta_a x^a$ được xem là bằng nhau nếu $\alpha_a = \beta_a$ với mọi $a \in N^n$.

Phép cộng đa thức được định nghĩa như sau:

$$\left(\sum_{a \in N^n} \alpha_a x^a\right) + \left(\sum_{a \in N^n} \beta_a x^a\right) = \sum_{a \in N^n} (\alpha_a + \beta_a) x^a.$$

Vì $\alpha_a + \beta_a \neq 0$ nếu một trong hai hệ số α_a hoặc β_a bằng 0, nên trong