ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

BÙI ĐỨC THẮNG

CƠ SỞ GROEBNER VÀ CHỨNG MINH ĐỊNH LÝ HÌNH HỌC BẰNG MÁY TÍNH

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2015

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

BÙI ĐỨC THẮNG

CƠ SỞ GROEBNER VÀ CHỨNG MINH ĐỊNH LÝ HÌNH HỌC BẰNG MÁY TÍNH

Chuyên ngành: Phương pháp Toán sơ cấp
Mã số: 60.46.01.13

LUẬN VĂN THẠC SĨ TOÁN HỌC

Người hướng dẫn khoa học: TS. Nguyễn Danh Nam

THÁI NGUYÊN - 2015

Công trình được hoàn thành tại
Trường Đại học Khoa học – Đại học Thái Nguyên

Người hướng dẫn khoa học: TS. Nguyễn Danh Nam

Phản biện 1: PGS.TS. Nguyễn Việt Hải

Phản biện 2: PGS.TS. Trịnh Thanh Hải

Luận văn sẽ được bảo vệ trước hội đồng chấm luận văn họp tại:
Trường Đại học Khoa học – Đại học Thái Nguyên
Ngày 31 tháng 5 năm 2015

Có thể tìm hiểu tại:
Thư viện Trường Đại học Khoa học và
Trung tâm Học liệu - Đại học Thái Nguyên

MỤC LỤC

Trang

MỞ ĐẦU

Với sự phát triển nhanh chóng của công nghệ thông tin và truyền thông, các phương tiện - thiết bị dạy học hiện đại đã và đang được sử dụng một cách có hiệu quả trong giáo dục. Phần mềm dạy học là một trong những phương tiện dạy học hỗ trợ giáo viên thực hiện được phần nào các ý tưởng sư phạm của mình. Maple là một phần mềm toán học tạo ra một cách tiếp cận mới sinh động và sáng tạo. Ngoài các câu lệnh có chức năng kiểm tra, tính toán, minh hoạ hình ảnh,…nó còn cho phép các giáo viên có thể sử dụng ngôn ngữ lập trình của Maple để tạo các công cụ mới, các gói câu lệnh mới. Vì thế, Maple có khả năng đầy đủ để giảng dạy và học tập từ bậc phổ thông (các gói chức năng về đại số, số học, giải tích, hình học,…) lên đại học (đại số tuyến tính, phương trình vi phân, hình học cao cấp, đại số hiện đại,…).

Xuất phát từ ý tưởng rằng có rất nhiều định lý hình học hoàn toàn được mô tả bằng các khái niệm đại số bằng cách biểu diễn các hình hình học trong toạ độ Đề-các vuông góc. Khi đó, hầu hết các hình hình học và biên của nó có thể xem là tập không điểm của các đa thức, và các quan hệ giữa chúng đều có thể mô tả bằng các phương trình đa thức cũng như tập không điểm phải xét trên trường số thực. Như vậy, để kiểm tra tính đúng - sai của một giả thuyết hay một định lý hình học nào đó hoàn toàn có thể thực hiện được nhờ những kết quả quan trọng liên quan đến khái niệm cơ sở Groebner được nhà toán học Bruno Buchberger đưa ra năm 1965 trong luận án phó tiến sĩ của mình.

Tính toán hình thức hay còn gọi là Đại số máy tính, xuất hiện khoảng ba chục năm nay và gần đây trở thành một chuyên ngành độc lập. Đây là một chuyên ngành kết hợp chặt chẽ toán học và khoa học máy tính. Nó được ra đời dưới ảnh hưởng của sự phát triển và phổ cập máy tính cá nhân. Một mặt, sự phát triển này đòi hỏi phải xây dựng các lý thuyết toán học làm cơ sở cho việc thiết lập thuật toán và các phần mềm toán học. Mặt khác, khả năng tính toán mỗi ngày một tăng của máy tính giúp triển khai tính toán thực sự nhiều thuật toán. Sự phát triển của Đại số máy tính cũng có tác dụng tích cực trở lại trong nghiên cứu toán học lý thuyết.

Nhiều kết quả lý thuyết đã được phán đoán hoặc có được phản ví dụ nhờ sử dụng máy tính.

Hầu hết những vấn đề mà lý thuyết cơ sở Groebner cho lời giải bằng thuật toán đã được biết trước đó, đó là tính giải được. Tuy nhiên giữa việc chứng minh tính giải được và thực hiện tính toán trên thực tế là khoảng cách lớn. Hơn nữa, nhiều đối tượng trong các ngành khá trừu tượng như Đại số giao hoán và Hình học đại số có thể tính toán thông qua cơ sở Groebner chứng tỏ có một tầm quan trọng của lý thuyết này.

Mục đích của luận văn là giới thiệu thuật toán tính cơ sở Groebner cho các Iđêan đa thức, để trình bày một số ứng dụng của lý thuyết cơ sở Groebner trong tính toán hình thức bằng máy tính là Đại số giao hoán và Hình học đại số. Hiện nay, có nhiều phần mềm xử lý toán học như Maple, Macaulay, CoCoA ... để phục vụ cho việc tính toán. Nhưng luận văn này chọn phần mềm Maple để trình bày cách đại số hóa bài toán hình học và chứng minh định lý hình học bằng máy tính. Tuy nhiên, nếu chỉ đơn thuần sử dụng gói công cụ Groebner của Maple thì giáo viên nhiều khi khó thực hiện được kịch bản sư phạm của mình. Giải pháp cho vấn đề này là giáo viên sử dụng ngôn ngữ lập trình của Maple để xây dựng các gói công cụ phù hợp. Do đó, chúng tôi đã xây dựng gói *GeoProver* để hỗ trợ chứng minh một số định lý hình học sơ cấp.

Chương 1
CƠ SỞ GROEBNER

Khái niệm cơ sở Groebner ra đời trong những năm 1970 để giải quyết bài toán chia đa thức. Sau hơn 20 năm khái niệm này đã có những ứng dụng to lớn trong nhiều chuyên ngành toán học khác nhau từ Đại số đến Hình học, Tô pô, Tổ hợp và Tối ưu [9].

Việc sử dụng các hệ đa thức giống như cơ sở Groebner đã xuất hiện từ đầu thế kỉ này với các công trình của Gordan, Macaulay, Hilbert. Người đầu tiên thấy được tầm quan trọng của thuật toán chia là nhà toán học người Áo Broebner. Ông đã đặt vấn đề tính cơ sở Groebner làm một đề tài luận án phó tiến sĩ cho học trò của ông là Buchberger. Năm 1970, Buchberger tìm thấy một thuật toán hữu hiệu để tính cơ sở Groebner. Sau này người ta mới phát hiện ra rằng Groebner đã biết những nét cơ bản của thuật toán này từ những năm 50. Cùng thời gian này cũng xuất hiện những kĩ thuật tương tự giống như thuật toán chia trong các công trình của Hironaka về giải kì dị, của Grauert trong Giải tích phức và của Cohn trong Lý thuyết vành không giao hoán [9].

Cơ sở Groebner được nghiên cứu đúng thời kì máy tính cá nhân ra đời và bắt đầu trở nên phổ cập. Ngay lập tức người ta thấy rằng có thể lập trình thuật toán chia để giải quyết các bài toán với các biến số mà ngày nay được gọi là tính toán hình thức (symbol computation). Bản thân thuật toán chia đã chứa đựng những thuận lợi cơ bản cho việc lập trình như:

(1) Việc sắp xếp thứ tự các hạng tử của một đa thức cho phép ta biểu diễn một đa thức như một véc-tơ các hệ số và do đó ta có thể đưa dữ liệu về các đa thức vào trong máy tính một cách dễ dàng.

(2) Việc xét hạng tử lớn nhất của các đa thức cho phép máy tính chỉ cần thử tọa độ đầu tiên của các véc-tơ tương ứng.

Về mặt lý thuyết khái niệm cơ sở Groebner cũng đưa ra những phương pháp và vấn đề nghiên cứu mới. Trước tiên, người ta thấy rằng nhiều khi chỉ cần xét tập hợp các hạng tử đầu của cơ sở Groebner là đủ để có các thông tin cần thiết về hệ đa

thức ban đầu. Có thể thay các hạng tử này bằng các đơn thức nên thực chất là ta phải xét một số hữu hạn các bộ số tự nhiên ứng với các số mũ của các biến trong đơn thức. Ta có thể coi các bộ số tự nhiên này như những điểm nguyên là các điểm có tọa độ là các số nguyên. Vì vậy, nhiều bài toán Hình học và Đại số có thể quy về việc xét các tính chất tổ hợp hay tô pô của một tập hợp hữu hạn các điểm nguyên.

Sau đây luận văn trình bày một số kiến thức cơ bản về cơ sở Groebner trước khi đưa ra thuật toán để chứng minh định lý hình học.

1.1. THỨ TỰ TỪ

1.1.1. Định nghĩa

Định nghĩa 1.1. *Thứ tự từ* $\leq$ là một thứ tự toàn phần trên tập M tất cả các đơn thức của vành $K[x]$ thoả mãn các tính chất sau:

i) Với mọi $m \in M$, $1 \leq m$.

ii) Nếu $m_1, m_2, m \in M$ mà $m_1 \leq m_2$ thì $mm_1 \leq mm_2$.

1.1.2. Một số thứ tự từ

Định nghĩa 1.2. *Thứ tự từ điển* là thứ tự $\leq_{lex}$ xác định như sau: $x_1^{\alpha_1}...x_n^{\alpha_n} <_{lex} x_1^{\beta_1}...x_n^{\beta_n}$ nếu thành phần đầu tiên khác không kể từ bên trái của véctơ $(\alpha_1 - \beta_1,..., \alpha_n - \beta_n)$ là một số âm. Nói cách khác, nếu tồn tại $0 \leq i < n$ sao cho $\alpha_1 = \beta_1,..., \alpha_n = \beta_n$, nhưng $\alpha_{i+1} < \beta_{i+1}$.

Thứ tự từ điển tương tự như cách sắp xếp các từ trong từ điển, và do đó có tên gọi như vậy.

Định nghĩa 1.3. *Thứ tự từ điển phân bậc* là thứ tự $\leq_{glex}$ xác định như sau: $x_1^{\alpha_1}...x_n^{\alpha_n} <_{glex} x_1^{\beta_1}...x_n^{\beta_n}$ nếu $\deg(x_1^{\alpha_1}...x_n^{\alpha_n}) < \deg(x_1^{\beta_1}...x_n^{\beta_n})$ hoặc $\deg(x_1^{\alpha_1}...x_n^{\alpha_n}) = \deg(x_1^{\beta_1}...x_n^{\beta_n})$ và thành phần đầu tiên khác không kể từ bên trái của véctơ $(\alpha_1 - \beta_1,..., \alpha_n - \beta_n)$ là một số âm. Nói cách khác, $x_1^{\alpha_1}...x_n^{\alpha_n} <_{glex} x_1^{\beta_1}...x_n^{\beta_n}$ nếu $\alpha_1 + ... + \alpha_n < \beta_1 + ... + \beta_n$ hoặc $\alpha_1 + ... + \alpha_n = \beta_1 + ... + \beta_n$ và $x_1^{\alpha_1}...x_n^{\alpha_n} <_{lex} x_1^{\beta_1}...x_n^{\beta_n}$.

Định nghĩa 1.4. *Thứ tự từ điển ngược* là thứ tự $\leq_{rlex}$ xác định như sau: $x_1^{\alpha_1}...x_n^{\alpha_n} <_{rlex} x_1^{\beta_1}...x_n^{\beta_n}$ nếu $\deg(x_1^{\alpha_1}...x_n^{\alpha_n}) < \deg(x_1^{\beta_1}...x_n^{\beta_n})$ hoặc $\deg(x_1^{\alpha_1}...x_n^{\alpha_n}) = \deg(x_1^{\beta_1}...x_n^{\beta_n})$

và thành phần đầu tiên khác không kể từ bên phải của véctơ $(\alpha_1-\beta_1,...,\alpha_n-\beta_n)$ là một số dương. Nói cách khác, $x_1^{\alpha_1}...x_n^{\alpha_n} <_{rlex} x_1^{\beta_1}...x_n^{\beta_n}$ nếu $\alpha_1+...+\alpha_n<\beta_1+...+\beta_n$ hoặc $\alpha_1+...+\alpha_n=\beta_1+...+\beta_n$ và và tồn tại $1\le i\le n$ sao cho $\alpha_n=\beta_n,...,\alpha_{i+1}=\beta_{i+1}$ nhưng $\alpha_i>\beta_i$.

Thứ tự từ điển ngược được định nghĩa như theo sơ đồ của thứ tự từ điển phân bậc, chứ không phải của thứ tự từ điển - một điều tưởng chừng không tự nhiên. Thực ra việc so sánh bậc tổng thể trước trong trường hợp này là bắt buộc để đảm bảo đơn thức 1 là nhỏ nhất.

Mệnh đề 1.1. *Ba thứ tự kể trên là các thứ tự từ.*

1.2. IĐÊAN KHỞI ĐẦU VÀ CƠ SỞ GROEBNER

1.2.1. Từ khởi đầu, đơn thức khởi đầu

Định nghĩa 1.5. Cho $\le$ là một thứ tự từ và $f\in R=K[x_1,...,x_n]$. *Từ khởi đầu* của f, kí hiệu là $in_{\le}(f)$, là từ lớn nhất của đa thức f đối với thứ tự từ $\le$.

Nếu $in_{\le}(f)=\alpha x^a, 0\ne\alpha\in K$, thì $lc_{\le}(f)=\alpha$ được gọi là *hệ số đầu* và $lm_{\le}(f)=x^a$ là *đơn thức đầu* của f đối với thứ tự từ $\le$.

Nếu thứ tự từ $\le$ đã được ngầm hiểu, ta sẽ viết $in(f)$ (tương ứng $lc(f)$, $lm(f)$) thay cho $in_{\le}(f)$ (tương ứng $lc_{\le}(f)$, $lm_{\le}(f)$).

Từ khởi đầu của đa thức 0 được xem là không xác định (có thể nhận giá trị tuỳ ý).

Từ khởi đầu còn gọi là từ đầu hay từ đầu tiên. Như vậy nếu trong biểu diễn chính tắc của đa thức f ta viết các từ theo thứ tự giảm dần, thì $in(f)$ sẽ xuất hiện đầu tiên. Đương nhiên cách viết này cũng như từ khởi đầu của f phụ thuộc vào thứ tự từ đã chọn.

1.2.2. Iđêan khởi đầu và cơ sở Groebner

Định nghĩa 1.6. Cho *I* là iđêan của *R* và $\leq$ là một thứ tự từ, *Iđêan khởi đầu* của *I*, kí hiệu là $in_{\leq}(I)$, là iđêan của *R* sinh bởi các từ khởi đầu của các phần tử của *I*, nghĩa là:

$$in_{\leq}(I) = \left(in_{\leq}(f) \middle| f \in I\right)$$

Cũng như trên ta sẽ viết $in(I)$ thay vì $in_{\leq}(I)$ nếu $\leq$ đã rõ. Rõ ràng cũng có $in(I) = \left(\mathrm{Im}(f) \middle| f \in I\right)$ nên $in(I)$ là iđêan đơn thức.

Vấn đề đặt ra là làm thế nào để xác định được iđêan khởi đầu $in(I)$ của một iđêan *I* cho trước. Cách tốt nhất là tìm một hệ sinh tối tiểu của nó. Tuy nhiên, mọi iđêan đơn thức đều có một tập sinh đơn thức và tập đó hữu hạn. Do đó ta có thể đưa vào khái niệm quan trọng sau đây:

Định nghĩa 1.7. Cho $\leq$ là một thứ tự từ và *I* là iđêan của *R*. Tập hữu hạn các đa thức khác không $g_1,...,g_s \in I$ được gọi là một *cơ sở Groebner* của *I* đối với thứ tự từ $\leq$, nếu:

$$in_{\leq}(I) = \left(in_{\leq}(g_1),...,in_{\leq}(g_s)\right)$$

Tập $g_1,...,g_s \in I$ được gọi là một *cơ sở Groebner*, nếu nó là cơ sở Groebner của iđêan sinh bởi chính các phần tử này.

Mệnh đề 1.2. *Cho I là một iđêan tuỳ ý của R. Nếu* $g_1,...,g_s \in I$ *là cơ sở Groebner của I đối với một thứ tự từ nào đó, thì* $g_1,...,g_s$ *là cơ sở của I.*

Định nghĩa 1.8. *Cơ sở Groebner rút gọn* của iđêan *I* đối với một thứ tự từ đã cho là một cơ sở Groebner *G* của *I* thoả mãn các tính chất sau:

i) $lc(g) = 1$ với mọi $g \in G$.

ii) Với mọi $g \in G$ và mọi từ *m* của g không tồn tại $g' \in G \setminus \{g\}$ để $in(g') \mid m$.

Mệnh đề 1.3. *Cho* $I \neq 0$. *Khi đó đối với mỗi thứ tự từ, I có duy nhất một cơ sở Groebner rút gọn. Mọi cơ sở Groebner rút gọn đều là cơ sở Groebner tối tiểu.*