ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN HÀ LINH

ĐA THỨC BẤT KHẢ QUY

LUẬN VĂN THẠC SỸ TOÁN HỌC

Thái Nguyên – 2012

Mục lục

LỜI CẢM ƠN

Tôi xin gửi lời biết ơn chân thành nhất đến PGS.TS Lê Thị Thanh Nhàn. Cô đã dành rất nhiều thời gian và tâm huyết trong việc hướng dẫn tôi. Cho đến hôm nay, luận văn thạc sĩ của tôi đã được hoàn thành cũng chính là nhờ sự nhắc nhở, đôn đốc, sự giúp đỡ nhiệt tình của Cô.

Tôi xin trân trọng cảm ơn Ban Giám hiệu, Khoa Toán - Tin và Phòng Đào tạo - Khoa học và Quan hệ quốc tế của trường Đại học Khoa học - Đại học Thái Nguyên. Tôi xin trân trọng cảm ơn các Thầy Cô đã tận tình truyền đạt những kiến thức quý báu cũng như tạo mọi điều kiện thuận lợi nhất để tôi hoàn thành luận văn này.

Tôi xin chân thành bày tỏ lòng biết ơn đến gia đình, bạn bè, những người đã không ngừng động viên, hỗ trợ và tạo mọi điều kiện tốt nhất cho tôi trong suốt thời gian học tập và thực hiện luận văn.

LỜI NÓI ĐẦU

Trong lý thuyết đa thức, đa thức bất khả quy đóng một vai trò quan trọng giống như vai trò của số nguyên tố trong tập các số nguyên. Nếu Định lý cơ bản của Số học cho phép coi các số nguyên tố như là những viên gạch xây nên tập các số nguyên, thì các đa thức bất khả quy chính là những viên gạch xây nên tập tất cả đa thức. Bởi vì mỗi đa thức bậc dương dạng chuẩn (tức là hệ số cao nhất bằng 1) với hệ số trên một trường đều viết được thành tích của hữu hạn đa thức bất khả quy dạng chuẩn và sự phân tích đó là duy nhất nếu không kể đến thứ tự các nhân tử.

Bài toán xét tính bất khả quy của các đa thức trên trường phức $\mathbb{C}$ và trên trường thực $\mathbb{R}$ đã được giải quyết từ đầu thế kỉ 19, khi người ta chứng minh được Định lý cơ bản của Đại số. Cụ thể, các đa thức bất khả quy trên $\mathbb{C}$ là và chỉ là các đa thức bậc nhất; các đa thức bất khả quy trên $\mathbb{R}$ là và chỉ là các đa thức bậc nhất hoặc bậc hai với biệt thức âm. Tuy nhiên bài toán xét tính bất khả quy của đa thức trên trường hữu tỷ $\mathbb{Q}$ hoặc trên trường thặng dư $\mathbb{Z}_p$ (với p là số nguyên tố) vẫn đang thử thách các nhà toán học trên thế giới.

Mục đích của luận văn là trình bày một số kết quả về đa thức bất khả quy trên một trường, đặc biệt là trên trường $\mathbb{Q}$ và trường $\mathbb{Z}_p$. Nội dung của luận văn được viết dựa theo cuốn sách ``Lý thuyết Galois" của J. Rotman [Rot], cuốn sách ``Đa thức và tính bất khả quy" của A. Schinzel [Sc], bài báo ``Tính bất khả quy của đa thức" đăng trên Tạp chí Đại số của I. Seres [S] và bài báo ``Tiêu chuẩn bất khả quy của đa thức" đăng trên tạp chí nổi tiếng Ann. Math của H. L. Dorwart - O. Ore [DO].

Luận văn gồm 3 chương. Chương 1 trình bày một số kiến thức cơ sở về đa thức bất khả quy và sử dụng đa thức bất khả quy để chứng minh Định

lý Kronecker về sự tồn tại của trường phân rã của đa thức (Định lý 1.3.2) và Định lý của Galois về sự tồn tại một trường có hữu hạn phần tử (Định lý 1.3.5). Chương 2 trình bày một số phương pháp xét tính bất khả quy của đa thức trên trường $\mathbb{Q}$ như phương pháp tìm nghiệm hữu tỷ, phương pháp dùng Bổ đề Gauss, tiêu chuẩn Eisenstein và phương pháp rút gọn theo môđun một số nguyên tố. Bằng cách sử dụng Định lý Kronecker về sự tồn tại trường phân rã và Định lý Lagrange về cấp của nhóm hữu hạn (Định lý 3.1.7), tính bất khả quy của một số đa thức trên trường $\mathbb{Z}_p$ (với p là một số nguyên tố) được trình bày trong Chương 3.

Chương 1

Đa thức bất khả quy

Trước khi trình bày khái niệm và một số kết quả về đa thức bất khả quy, chúng ta trình bày kiến thức cơ sở về đa thức.

1.1 Khái niệm đa thức

1.1.1 Định nghĩa. Một tập F cùng với hai phép toán, kí hiệu là phép cộng và phép nhân, được gọi là *trường* nếu các tính chất sau thỏa mãn

(i) Kết hợp: $a + (b + c) = (a + b) + c$ và $(ab)c = a(bc)$ với mọi $a, b, c \in F$.

(ii) Giao hoán: $a + b = b + a$ và $ab = ba$ với mọi $a, b \in F$.

(iii) Luật phân phối: $a(b + c) = ab + ac$ với mọi $a, b, c \in F$.

(iv) Tồn tại *phần tử đơn vị* $1 \in F$ sao cho $a1 = 1a = a$ với mọi $a \in F$.

(v) Tồn tại phần tử $0 \in F$ sao cho $a + 0 = 0 + a = a$ với mọi $a \in F$.

(vi) Mỗi $a \in F$, tồn tại phần tử đối $-a \in F$ sao cho $a + (-a) = 0$.

(vii) Mỗi $0 \neq a \in F$, tồn tại *phần tử nghịch đảo* $a^{-1} \in F$ sao cho $aa^{-1} = 1$.

1.1.2 Định nghĩa. Cho F là một trường và $a_0, a_1, \ldots, a_m \in F$. Một biểu thức có dạng $f(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0$ được gọi là một *đa thức* một biến x. Tập các đa thức với hệ số trên F được kí hiệu là $F[x]$. Nếu

$a_m \neq 0$ thì ta nói *bậc* của $f(x)$ là m và kí hiệu là $\deg f(x) = m$. Hệ số a_m được gọi là *hệ số cao nhất* của f. Nếu $a_m = 1$ thì $f(x)$ được gọi là *đa thức dạng chuẩn* (monic polynomial). Hai đa thức là *bằng nhau* nếu nó có cùng bậc và các hệ số tương ứng là bằng nhau. Với hai đa thức $f(x) = \sum a_i x^i$ và $g(x) = \sum b_i x^i$, ta định nghĩa *tổng* $f(x) + g(x) = \sum (a_i + b_i)x^i$ và *tích* $f(x)g(x) = \sum c_k x^k$, trong đó $c_k = \sum_{i+j=k} a_i b_j$.

Từ định nghĩa trên ta có ngay các tính chất sau đây.

1.1.3 Bổ đề. *Cho $f(x), g(x), h(x) \in F[x]$. Khi đó*

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

(ii) Nếu $f(x) \neq 0$ và $g(x) \neq 0$ thì $f(x)g(x) \neq 0$ và

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x).$$

(iii) Nếu $f(x) \neq 0$ và $f(x)g(x) = f(x)h(x)$ thì $g(x) = h(x)$.

1.1.4 Định nghĩa. Cho $f(x), g(x) \in F[x]$. Nếu $f(x) = q(x)g(x)$ với $q(x) \in F[x]$ thì ta nói rằng $g(x)$ là *ước* của $f(x)$ hay $f(x)$ là *bội* của $g(x)$ và ta viết $g(x)|f(x)$. Tập các bội của $g(x)$ được kí hiệu là (g).

Ta có ngay các tính chất đơn giản sau đây.

1.1.5 Bổ đề. *Các phát biểu sau là đúng.*

(i) Với $c \in F$ và k là số tự nhiên ta có $(x - c)|(x^k - c^k)$.

(ii) Nếu $f(x) \in F[x]$ và $c \in F$ thì tồn tại $q(x) \in F[x]$ sao cho

$$f(x) = q(x)(x - c) + f(c).$$

1.1.6 Định nghĩa. Cho $f(x) = a_m x^m + \ldots + a_0 \in F[x]$. Giả sử K là một trường chứa F. Một phần tử $c \in K$ được gọi là nghiệm của $f(x)$ nếu $f(c) = a_m c^m + \ldots + a_0 = 0$. Trong trường hợp này ta cũng nói c là nghiệm của phương trình $f(x) = 0$.

1.1.7 Bổ đề. *Cho $f(x) \in F[x]$ và $c \in F$. Khi đó*

(i) c là nghiệm của $f(x)$ nếu và chỉ nếu $f(x)$ là bội của $x - c$.

(ii) Số nghiệm của $f(x)$ không vượt quá $\deg f(x)$.

1.1.8 Mệnh đề. (Thuật toán chia với dư). *Cho $f(x), g(x) \in F[x]$ với $g(x) \neq 0$. Khi đó tồn tại duy nhất cặp đa thức $q(x), r(x) \in F[x]$ sao cho*

$$f(x) = q(x)g(x) + r(x)$$

trong đó $r(x) = 0$ hoặc $\deg r(x) < \deg g(x)$.

1.1.9 Định nghĩa. Một tập con $I \neq \emptyset$ của $F[x]$ được gọi là một *iđêan* của $F[x]$ nếu nó thỏa mãn các điều kiện sau

(i) Nếu $f(x), g(x) \in I$ thì $f(x) + g(x) \in I$;

(ii) Nếu $f(x) \in I$ và $q(x) \in F[x]$ thì $q(x)f(x) \in I$.

Chú ý rằng tập con $I \neq \emptyset$ của $F[x]$ là iđêan nếu và chỉ nếu $f - g \in I$ và $fh \in I$ với mọi $f(x), g(x) \in I$ và $h(x) \in F[x]$.

1.1.10 Mệnh đề. *Nếu $I \neq \{0\}$ là một iđêan trong $F[x]$ và $d(x) \neq 0$ là đa thức có bậc bé nhất trong I thì*

$$I = (d) = \{d(x)q(x) \mid q(x) \in F[x]\}.$$

Chứng minh. Cho đa thức $f(x) \in I$. Viết $f(x) = d(x)q(x) + r(x)$ trong đó $r(x) = 0$ hoặc $\deg r(x) < \deg d(x)$. Vì $f(x), d(x) \in I$ nên ta có $r(x) = f(x) - d(x)q(x) \in I$. Do đó $r(x) = 0$ theo cách chọn $d(x)$. Suy ra $f(x) = d(x)q(x)$. Ngược lại, vì $d(x) \in I$ nên $d(x)q(x) \in I$ với mọi $q(x) \in F[x]$. □

1.1.11 Định nghĩa. Một đa thức dạng chuẩn $d(x) \in F[x]$ được gọi là *ước chung lớn nhất* của $f(x), g(x) \in F[x]$ nếu $d(x)|f(x)$, $d(x)|g(x)$ và nếu $h(x)|f(x)$ và $h(x)|g(x)$ thì $h(x)|d(x)$. Ta kí hiệu ước chung lớn nhất của

$f(x)$ và $g(x)$ là $\gcd(f(x), g(x))$. Nếu $\gcd(f(x), g(x)) = 1$ thì ta nói $f(x)$ và $g(x)$ là *nguyên tố cùng nhau.*

Từ Mệnh đề 1.1.10 ta có kết quả sau.

1.1.12 Mệnh đề. *Nếu $f(x), g(x)$ là hai đa thức không đồng thời bằng 0 thì $\gcd(f(x), g(x))$ luôn tồn tại và là tổ hợp tuyến tính của $f(x)$ và $g(x)$, tức là tồn tại $a(x), b(x) \in F[x]$ sao cho*

$$\gcd(f(x), g(x)) = a(x)f(x) + b(x)g(x).$$

1.1.13 Hệ quả. *Cho $p(x), f(x), g(x) \in F[x]$. Nếu $\gcd(p(x), f(x)) = 1$ và $p(x)|f(x)g(x)$ thì $p(x)|g(x)$.*

Chứng minh. Theo giả thiết, $1 = p(x)a(x) + f(x)b(x)$. Suy ra

$$g(x) = p(x)a(x)g(x) + f(x)b(x)g(x).$$

Do $p(x)$ là ước của đa thức ở vế phải nên $p(x)|g(x)$. □

Với $0 \neq g(x) \in F[x]$, kí hiệu $g^*(x) = g(x)/a_n$ trong đó a_n là hệ số cao nhất của $g(x)$. Chú ý rằng $g^*(x)$ là đa thức dạng chuẩn. Để tìm ước chung lớn nhất ta có thuật toán sau:

1.1.14 Mệnh đề. (Thuật toán Euclid tìm ước chung lớn nhất). *Cho hai đa thức $f(x), g(x) \in F[x]$ với $g(x) \neq 0$. Nếu $g(x)|f(x)$ thì*

$$\gcd(f(x), g(x)) = g^*(x).$$

Nếu ngược lại, chia liên tiếp ta được

$$\begin{aligned}
f(x) &= q(x)g(x) + r(x),\ r(x) \neq 0, \deg r(x) < \deg g(x).\\
g(x) &= q_1(x)r(x) + r_1(x),\ r_1(x) \neq 0, \deg r_1(x) < \deg r(x).\\
&\cdots\cdots\cdots\\
r_{n-2}(x) &= q_n(x)r_{n-1}(x) + r_n(x),\ r_n(x) \neq 0, \deg r_n(x) < \deg r_{n-1}(x).\\
r_{n-1}(x) &= q_{n+1}(x)r_n(x).
\end{aligned}$$

Khi đó $\gcd(f(x), g(x)) = r_n^*(x)$.

Chứng minh. Từ đẳng thức cuối ta có $r_n(x)|r_{n-1}(x)$. Thay vào đẳng thức thứ hai từ dưới lên ta có $r_n(x)|r_{n-2}(x)$. Cứ tiếp tục lập luận với các đẳng thức từ dưới lên trên ta suy ra $r_n(x)|g(x)$ và $r_n(x)|f(x)$. Do đó $r_n^*(x)|f(x)$ và $r_n^*(x)|g(x)$. Giả sử $h(x)|f(x)$ và $h(x)|g(x)$. Từ đẳng thức đầu tiên ta có $h(x)|r(x)$. Từ đẳng thức thứ hai ta có $h(x)|r_1(x)$. Cứ tiếp tục lập luận trên với các đẳng thức từ trên xuống dưới ta có $h(x)|r_n(x)$. Do đó $h(x)|r_n^*(x)$. □

1.2 Đa thức bất khả quy

1.2.1 Định nghĩa. Một đa thức $f(x) \in F[x]$ được gọi là *bất khả quy* nếu $\deg f(x) > 0$ và $f(x)$ không phân tích được thành tích của hai đa thức có bậc bé hơn. Nếu $\deg f(x) > 0$ và $f(x)$ là tích của hai đa thức có bậc bé hơn thì ta nói $f(x)$ là *khả quy*.

Sau đây là một số ví dụ về đa thức bất khả quy.

1.2.2 Bổ đề. *Các phát biểu sau là đúng.*

(i) Đa thức bậc nhất luôn bất khả quy.

(ii) Nếu $f(x)$ *bậc lớn hơn* 1 *và có nghiệm trong* F *thì* $f(x)$ *khả quy.*

(iii) Đa thức bậc 2 *và bậc* 3 *là bất khả quy nếu và chỉ nếu nó không có nghiệm trong* F.

(iv) Đa thức $f(x)$ *có bậc dương là bất khả quy nếu và chỉ nếu* $f(x+a)$ *là bất khả quy với mọi* $a \in F$.

Chứng minh. (i) Rõ ràng đa thức bậc nhất không thể là tích của hai đa thức bậc thấp hơn.

(ii) Nếu $\deg f(x) > 1$ và $f(x)$ có nghiệm $x = a \in F$ thì $f = (x-a)g$ trong đó $\deg g = \deg f - 1 \geq 1$. Vì thế f khả quy.