ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN HUY QUÝ

TÍNH BẤT KHẢ QUY CỦA ĐA THỨC CÓ HỆ SỐ LÀ SỐ NGUYÊN

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2016

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN HUY QUÝ

TÍNH BẤT KHẢ QUY CỦA ĐA THỨC CÓ HỆ SỐ LÀ SỐ NGUYÊN

LUẬN VĂN THẠC SĨ TOÁN HỌC

Chuyên ngành: Phương pháp Toán sơ cấp
Mã số: 60 46 01 13

NGƯỜI HƯỚNG DẪN KHOA HỌC:
GS.TSKH. Hà Huy Khoái

THÁI NGUYÊN - 2016

Mục lục

Lời cảm ơn **iii**

Mở đầu **1**

Chương 1. Tiêu chuẩn bất khả quy Eisenstein, Osada và ứng dụng **3**

1.1 Khái niệm đa thức bất khả quy 3

1.1.1 Vành đa thức 3

1.1.2 Đa thức bất khả quy 4

1.1.3 Đa thức bất khả quy trên $\mathbb{Q}$ 8

1.2 Đa thức bất khả quy với hệ số nguyên 13

1.2.1 Tiêu chuẩn Eisenstein 13

1.2.2 Tiêu chuẩn Osada 15

1.3 Vận dụng Tiêu chuẩn Eisenstein 16

1.4 Vận dụng Tiêu chuẩn Osada 17

Chương 2. Tiêu chuẩn bất khả quy của Ore, Ram Murty, Chahal, Girstmair và ứng dụng **18**

2.1 Tính bất khả quy và giá trị nguyên tố 18

2.1.1 Tiêu chuẩn Ore 19

2.1.2 Các giá trị nguyên tố và tính bất khả quy. 26

2.2 Tính bất khả quy và đồng dư modulo p. 28

Kết luận **33**

Tài liệu tham khảo **34**

Lời cảm ơn

Luận văn này được hoàn thành dưới sự hướng dẫn của GS.TSKH Hà Huy Khoái. Xin trân trọng gửi đến Thầy lời cảm ơn sâu sắc nhất.

Tôi xin trân trọng cảm ơn Ban giám hiệu, Khoa Toán - Tin, Phòng Đào tạo của trường Đại học Khoa học - Đại học Thái Nguyên.

Xin kính gửi lời cảm ơn chân thành đến các thầy cô giáo đã tham gia giảng dạy lớp cao học Toán K8B - khóa học 2014 - 2016 . Những người đã bằng tâm huyết và sự nhiệt tình trong giảng dạy để trang bị cho tôi những kiến thức toán học cơ bản, đồng thời động viên và tạo mọi điều kiện thuận lợi giúp tôi hoàn thành nhiệm vụ học tập trong thời gian qua.

Tôi xin bày tỏ lòng biết ơn đến gia đình, bạn bè, cơ quan nơi tôi công tác đã luôn động viên, hỗ trợ và tạo điều kiện tốt nhất cho tôi trong suốt thời gian học tập và hoàn thành luận văn này.

Mở đầu

Nếu như trong số học, số nguyên tố giữ một vai trò quan trọng, thì trong đại số, đa thức bất khả quy với hệ số nguyên hay hệ số hữu tỷ cũng có vai trò quan trọng không kém, bởi vì mọi đa thức đều phân tích được thành tích các đa thức bất khả quy. Trên trường phức, các đa thức bất khả quy là đa thức bậc nhất, trên trường thực các đa thức bất khả quy là đa thức bậc nhất hoặc bậc hai. Trên trường hữu tỷ thì các đa thức bất khả quy không đơn giản như vậy. Theo bổ đề Gauss thì một đa thức là bất khả quy trên trường hữu tỷ khi và chỉ khi nó bất khả quy trên vành số nguyên. Do vậy, việc nghiên cứu tính bất khả quy của các đa thức với hệ số nguyên là cần thiết và luôn luôn thời sự.

Nhà toán học nổi tiếng L.Kronecker đã từng nói " Chúa đã cho chúng ta các số nguyên, tất cả còn lại là tác phẩm của con người." Từ thời học phổ thông, tất cả chúng ta đều quen thuộc với những điểm tương đồng giữa tập hợp các số nguyên và tập hợp các đa thức một biến. Một mô hình dạng này là thuật toán Ơ-clit (với phép chia).

Mục đích của luận văn này là trình bày một cách tổng quan về *tính bất khả quy của các đa thức hệ số nguyên* trên trường $\mathbb{Q}$. Trong đó, trình bày một số khái niệm đã biết xung quanh khái niệm *đa thức bất khả quy*, một số tiêu chuẩn bất khả quy của một đa thức và một số bài tập vận dụng. Với mục đích trên luận văn được chia làm hai chương:

Chương 1. **Tiêu chuẩn bất khả quy Eisenstein, Osada và ứng dụng**.

Trong chương này, trình bày khái niệm vành đa thức, đa thức bất khả quy; đa thức bất khả quy trên $\mathbb{Q}$; đa thức bất khả quy với hệ số nguyên; một số tiêu chuẩn bất khả quy Eisenstein và ứng dụng.

Chương 2. **Tiêu chuẩn bất khả quy của Ore, Ram Murty, Chahal, Girstmair và ứng dụng**.

Mục tiêu của chương này là trình bày một số kết quả tương đối gần đây của Ore; Ram Murty; Chahal; Girstmair; Schur và một số ứng dụng.

Thái Nguyên, ngày 25 tháng 5 năm 2016

Tác giả

Nguyễn Huy Quý

Chương 1

Tiêu chuẩn bất khả quy Eisenstein, Osada và ứng dụng

1.1 Khái niệm đa thức bất khả quy

1.1.1 Vành đa thức

Nhắc lại rằng một tập $V \neq \varnothing$ cùng với phép cộng được gọi là một *nhóm* nếu các điều kiện sau thỏa mãn:
(i) Phép cộng có tính kết hợp: $a+(b+c)=(a+b)+c$ với mọi $a,b,c \in V$.
(ii) Tồn tại phần tử $0 \in V$ sao cho $a+0=0+a=a$ với mọi $a \in V$.
(iii) Mỗi $a \in V$, tồn tại phần tử đối $-a \in V$ sao cho $a+(-a)=(-a)+a=0$.
Nếu thêm điều kiện $a+b=b+a$ với mọi $a,b \in V$ thì V được gọi là *nhóm giao hoán*. Nhóm cộng V được trang bị thêm phép toán nhân được gọi là một *vành* nếu 3 điều kiện sau thỏa mãn:
(i) Phép nhân có tính kết hợp: $(ab)c=a(bc)$ với mọi $a,b \in V$.
(ii) Tồn tại phần tử đơn vị $1 \in V$ sao cho $a1 = 1a = a$ với mọi $a \in V$.
(iii) $a(b+c) = ab+ac$ và $(b+c)a=ba+ca$ với mọi $a,b,c \in V$.
Nếu thêm điều kiện $ab=ba$ với mọi $a,b \in V$ thì V là *vành giao hoán*.

Định nghĩa 1.1.1. Một *đa thức biến x với hệ số trên V* là một tổng hữu hạn $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, trong đó $a_0, a_1, \cdots, a_n \in V$. Ta cũng viết đa thức này dưới dạng $f(x) = \sum_{i=0}^{\infty} a_i x^i$, trong đó $a_i = 0$ với mọi $i > n$. Hai đa thức $\sum_{i=0}^{\infty} a_i x^i$ và $\sum_{i=0}^{\infty} b_i x^i$ là *bằng nhau* nếu $a_i = b_i$ với mọi i.
Kí hiệu $V[x]$ là tập các đa thức một biến x với hệ số trên V.
Cho $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in V[x]$. Ta gọi a_0 là *hệ số tự do* của $f(x)$. Nếu $a_n \neq 0$ thì n được gọi là *bậc* của $f(x)$ và được kí hiệu bởi $degf(x)$. Trong trường hợp này, a_n được gọi là *hệ số cao nhất* của $f(x)$. Nếu a_n=1 thì $f(x)$ được gọi là *đa thức dạng chuẩn* (monic polynomial). Ta không định nghĩa bậc cho đa thức 0. Nếu $f(x) = a \in V$ thì $f(x)$ được gọi là *đa thức hằng*. Các đa thức bậc 1 được gọi là *đa thức tuyến tính*.

Định nghĩa 1.1.2. Với hai đa thức $f(x) = \sum a_i x^i$ và $g(x) = \sum b_i x^i$ trong $V[x]$, định nghĩa
$f(x) + g(x) = \sum (a_i + b_i)x^i$.
$f(x)g(x) = \sum c_k x^k$, trong đó $c_k = \sum_{i+j=k} a_i b_j$ với mọi k.
Khi đó $V[x]$ là vành giao hoán với phép cộng và phép nhân đa thức. Vành $V[x]$ được gọi là *vành đa thức một biến x với hệ số trong V*. Phần tử không của vành là đa thức 0, phần tử đơn vị của vành là đa thức 1.

1.1.2 Đa thức bất khả quy

Trước khi trình bày khái niệm đa thức bất khả quy, xin nhắc lại khái niệm phần tử bất khả quy trong một miền nguyên.
Cho $a, b \in \mathbb{V}$. Ta nói a là *ước* của b nếu tồn tại $c \in \mathbb{V}$ sao cho $b = ac$. Một ước a của b được gọi là *ước thực sự* nếu b không là ước của a. Phần tử $p \in \mathbb{V}$ được gọi là *phần tử bất khả quy* nếu nó khác 0, không khả nghịch và không có ước thực sự. Từ đây ta có khái niệm đa thức bất khả quy trong vành đa thức $V[x]$. Chú ý rằng $V[x]$ là miền nguyên.

Định nghĩa 1.1.3. Cho $f(x) \in V[x]$ là đa thức khác 0 và không khả nghịch. Ta nói *f(x) là bất khả quy* trên V nếu nó không có ước thực sự. Ta nói *f(x) khả quy* nếu $f(x)$ có ước thực sự.
Chú ý rằng tính bất khả quy của đa thức phụ thuộc vào vành cơ sở. Chẳng

hạn, đa thức $2x+2$ là bất khả quy trên trường $\mathbb{Q}$. Tuy nhiên $2x+2$ không bất khả quy trên vành $\mathbb{Z}$ bởi vì các đa thức 2 và $x+1$ đều là ước thực sự của $2x+2$. Tương tự, đa thức x^2+1 là bất khả quy trên $\mathbb{R}$ nhưng không bất khả quy trên $\mathbb{C}$.

Bổ đề 1.1.4. (i) *Đa thức f(x) là bất khả quy nếu và chỉ nếu f(x+a) là bất khả quy với mọi $a \in V$.*

Chứng minh. Cho $a \in V$. Với mỗi đa thức $h(x) \in V[x]$ ta đặt $h_1(x) = h(x-a)$. Chú ý rằng $\deg h_1(x) = \deg h(x)$. Vì thế $f(x+a) = k(x)g(x)$ là phân tích của $f(x+a)$ thành tích của hai đa thức có bậc thấp hơn khi và chỉ khi $f(x) = k_1(x)g_1(x)$ là phân tích của $f(x)$ thành tích của hai đa thức có bậc thấp hơn. Vì vậy $f(x)$ bất khả quy khi và chỉ khi $f(x+a)$ bất khả quy.□

Từ nay đến hết mục này chúng ta làm việc với đa thức có các hệ số trên một trường K. Trong trường hợp này, các đa thức hằng khác 0 đều khả nghịch. Do đó ta có ngay kết quả sau:

(ii) *Đa thức f(x) với hệ số trên trường K là bất khả quy nếu và chỉ nếu* deg*f(x)>0 và f(x) không phân tích được thành tích của hai đa thức có bậc bé hơn.*

Sau đây là tính bất khả quy của các đa thức bậc thấp.

(iii) *Trên một trường K, các phát biểu sau là đúng.*

Đa thức bậc nhất luôn bất khả quy.

Đa thức bậc 2 và bậc 3 là bất khả quy nếu và chỉ nếu nó không có nghiệm trong K.

Chứng minh. Rõ ràng đa thức bậc nhất không thể là tích của hai đa thức bậc thấp hơn, do đó nó bất khả quy.

Giả sử $f(x)$ có nghiệm $x = a \in K$. Vì $\deg f(x) > 1$ nên theo kết quả đã chứng minh được ta có $f(x) = (x-a)g(x)$, trong đó $g(x) \in K[x]$ và $\deg g(x)$=$\deg f(x)$-1$\geq$1. Do đó $f(x)$ khả quy.

Ngược lại, giả sử $f(x)$ khả quy. Vì $f(x)$ có bậc 2 hoặc 3 nên $f(x)$ phân tích được thành tích của hai đa thức có bậc thấp hơn, một trong hai đa thức đó phải có bậc 1. Rõ ràng đa thức bậc 1 trên một trường có nghiệm trong trường đó, vì thế $f(x)$ có nghiệm trong K.□

Chú ý rằng phát biểu (ii) trong bổ đề trên là không đúng cho trường hợp bậc của đa thức lớn hơn 3. Cụ thể, nếu $f(x)$ bậc lớn hơn 3 và có nghiệm trong K