ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ THU HƯƠNG

TÍNH BẤT KHẢ QUY CỦA CÁC ĐA THỨC LẶP CỦA MỘT SỐ LỚP ĐA THỨC TRÊN MỘT TRƯỜNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2016

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ THU HƯƠNG

TÍNH BẤT KHẢ QUY CỦA CÁC ĐA THỨC LẶP CỦA MỘT SỐ LỚP ĐA THỨC TRÊN MỘT TRƯỜNG

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.TS. LÊ THỊ THANH NHÀN

THÁI NGUYÊN - 2016

Mục lục

Lời mở đầu

Cho K là một trường. Một đa thức $f(x) \in K[x]$ được gọi là bất khả quy nếu $f(x)$ có bậc dương và $f(x)$ không là tích của hai đa thức có bậc bé hơn. Khi đó mỗi đa thức $0 \neq f(x) \in K[x]$ đều có sự phân tích bất khả quy

$$f(x) = af_1(x)\dots f_k(x)$$

trong đó a là hệ số cao nhất của $f(x)$ và $f_i(x)$ là đa thức bất khả quy dạng chuẩn (tức là có hệ số cao nhất bằng 1). Hơn nữa, sự phân tích bất khả quy này là duy nhất nếu không kể đến thứ tự các nhân tử $f_i(x)$. Kết quả này là một sự tương tự như Định lí cơ bản của Số học trong Lí thuyết số. Như vậy, trong vành đa thức $K[x]$, các đa thức bất khả quy đóng một vai trò quan trọng giống như vai trò của số nguyên tố trong vành $\mathbb{Z}$ các số nguyên. Nếu Định lí cơ bản của Số học cho phép coi các số nguyên tố như là những viên gạch xây nên vành số nguyên, thì các đa thức bất khả quy chính là những viên gạch xây nên vành đa thức.

Nhiều bài toán về đa thức bất khả quy được đặt ra xuất phát từ việc giải quyết các bài toán liên quan về số nguyên tố. Một trong những bài toán như thế là xét tính bất khả quy của các đa thức lặp của một số lớp đa thức. Cho $f(x) \in K[x]$ là một đa thức bậc dương. Đặt $f_0(x) = x$, $f_1(x) = f(x)$, $f_{r+1}(x) = f(f_r(x))$ với mọi $r \geq 1$. Ta gọi các đa thức $f_r(x)$ là các đa thức lặp của đa thức $f(x)$. Theo R. W. K. Odoni [O], ta nói rằng $f(x)$ là ổn định trên K nếu $f_r(x)$ là bất khả quy với mọi $r \geq 1$. Chú ý rằng các đa thức bậc 1 luôn bất khả quy trên trường K, vì thế mọi đa thức bậc 1 đều ổn định vì các đa thức lặp của nó luôn có bậc 1.

Mục đích của luận văn là trình bày lại chi tiết các kết quả trong hai bài báo sau đây về tính bất khả quy trên trường K của các đa thức lặp của hai lớp đa thức: đa thức bậc hai và đa thức dạng $x^n - b$.

[1]. M. Ayad and D. L. McQuillan (2000), *Irreducibility of the iterates of a quadratic polynomial over a field*, Acta Arithmetica, **93**, pp. 87-97.

[2]. L. Danielson and B. Fein (2001), *On the irreducibility of iterates of* $x^n - b$, Proc. Amer. Math. Soc., **130**, pp. 1589-1596.

Luận văn chia làm hai chương. Chương 1 trình bày những kiến thức cơ bản về đa thức bất khả quy và mở rộng trường. Chương 2 trình bày tính bất khả quy trên một trường của các đa thức lặp của hai lớp đa thức: đa thức bậc hai và đa thức dạng $x^n - b$. Chương 2 chia làm ba tiết. Tiết 2.1 trình bày tính bất khả quy của một đa thức lặp trên trường đặc số khác 2. Tiết 2.2 trình bày tính bất khả quy của các đa thức lặp của đa thức bậc hai. Tiết 2.3 trình bày tính bất khả quy của các đa thức lặp của đa thức dạng $x^n - b$.

Trong quá trình học tập và nghiên cứu tại trường Đại học Khoa học - Đại học Thái Nguyên, tôi được nhận đề tài nghiên cứu "Tính bất khả quy của các đa thức lặp của một số lớp đa thức trên một trường" dưới sự hướng dẫn của GS. TS Lê Thị Thanh Nhàn. Đến nay luận văn đã được hoàn thành. Có được kết quả này là do sự dạy bảo và hướng dẫn hết sức tận tình và nghiêm khắc của Cô. Tôi xin bày tỏ lòng biết ơn chân thành và sâu sắc tới Cô và gia đình!

Tôi cũng xin gửi lời cảm ơn chân thành đến Ban giám hiệu, Phòng Đào tạo và khoa Toán - Tin của trường Đại học Khoa học - Đại học Thái Nguyên đã tạo mọi điều kiện thuận lợi giúp đỡ tôi trong quá trình học tập tại Trường và trong thời gian nghiên cứu hoàn thành luận văn này. Sự giúp đỡ nhiệt tình và thái độ thân thiện của các thầy cô giáo, các cán bộ thuộc Phòng Đào tạo, Khoa Toán - Tin đã để lại trong lòng mỗi chúng tôi những ấn tượng hết sức tốt đẹp. Không biết nói gì hơn, một lần nữa tôi xin trân trọng cảm ơn.

Tôi xin cảm ơn gia đình, bạn bè và các thành viên trong lớp cao học toán K8A (2014 - 2016) đã quan tâm, tạo điều kiện, cổ vũ và động viên để tôi có thể hoàn thành nhiệm vụ của mình.

Tôi xin trân trọng cảm ơn!

Tác giả

Nguyễn Thị Thu Hương

Chương 1

Một số kiến thức chuẩn bị

1.1 Khái niệm đa thức bất khả quy

Trong suốt chương này, luôn giả thiết K là một trường. Ta gọi đa thức $f(x) \in K[x]$ là có dạng chuẩn nếu hệ số cao nhất của $f(x)$ bằng 1.

Định nghĩa 1.1.1. Cho $f(x) \in K[x]$. Ta nói rằng $f(x)$ là bất khả quy trên K nếu $f(x)$ có bậc dương và $f(x)$ không là tích của hai đa thức có bậc thấp hơn.

Chú ý rằng tính bất khả quy của đa thức phụ thuộc vào trường cơ sở. Chẳng hạn, đa thức $x^2 - 2$ là bất khả quy trên $\mathbb{Q}$ nhưng không bất khả quy trên $\mathbb{R}$. Tương tự, đa thức $x^2 + 1$ bất khả quy trên $\mathbb{R}$ nhưng không bất khả quy trên $\mathbb{C}$.

Bổ đề 1.1.2. *Đa thức $f(x)$ là bất khả quy nếu và chỉ nếu $f(x+a)$ là bất khả quy với mọi $a \in K$.*

Chứng minh. Cho $a \in K$. Với mỗi $h(x) \in K[x]$ 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 đa thức $f(x+a)$ thành tích 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. □

Bổ đề 1.1.3. *Trên một trường K, các phát biểu sau đây là đúng.*
(i) Đa thức bậc nhất luôn bất khả quy.
(ii) Đa thức bậc 2 và bậc 3 là bất khả quy nếu và chỉ nếu nó không có nghiệm trong K.

Chứng minh. (i) Đa thức bậc nhất rõ ràng không thể là tích của hai đa thức bậc thấp hơn, do đó nó bất khả quy.
(ii) Cho $f(x) \in K[x]$ là một đa thức bậc 2 hoặc 3. Giả sử $f(x)$ có nghiệm $x = a \in K$. Vì $\deg f(x) > 1$ nên

$$f(x) = (x-a)g(x),$$

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 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 luôn 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 thì $f(x)$ khả quy. Tuy nhiên, tồn tại những đa thức không có nghiệm trong K nhưng vẫn khả quy. Chẳng hạn đa thức $(x^2+1)^2$ không có nghiệm trong $\mathbb{R}$ nhưng nó khả quy trên $\mathbb{R}$.

Cho F là một trường chứa K. Một phần tử $a \in F$ được gọi là phần tử đại số trên K nếu nó là nghiệm của một đa thức khác 0 với hệ số trên K. Nếu a không đại số trên K thì ta nói a là siêu việt trên K.

Mệnh đề 1.1.4. *Cho F là một trường chứa K và $a \in F$ là phần tử đại số trên K. Khi đó tồn tại duy nhất một đa thức $p(x) \in K[x]$ bất khả quy dạng chuẩn nhận a làm nghiệm. Hơn nữa, nếu $g(x) \in K[x]$ nhận a làm nghiệm thì $g(x)$ là bội của $p(x)$.*

Chứng minh. Vì a là phần tử đại số trên K nên tồn tại $f(x) \in K[x]$ là đa thức khác 0 có bậc bé nhất nhận a làm nghiệm. Đặt $p(x) = b^{-1}f(x)$, trong đó b là hệ số cao nhất của $f(x)$. Khi đó $p(x) \in K[x]$ là đa thức dạng chuẩn có bậc bé nhất nhận a làm nghiệm. Rõ ràng $\deg p(x) > 0$. Nếu $p(x)$ khả quy thì $p(x)$ là tích của hai đa thức trong $K[x]$ với bậc bé hơn và một trong hai đa thức này phải nhận a làm nghiệm, điều này mâu thuẫn với cách chọn $p(x)$. Do đó $p(x)$ bất khả quy. Giả sử $g(x) \in K[x]$ nhận a làm nghiệm. Nếu $g(x)$ không chia hết cho $p(x)$ thì vì $p(x)$ bất khả quy nên $\gcd(g(x), p(x)) = 1$. Do đó tồn tại $q(x), h(x) \in K[x]$ sao cho $1 = p(x)q(x) + g(x)h(x)$. Thay $x = a$

vào cả hai vế ta được $1 = 0$, điều này là vô lý. Vậy $g(x)$ chia hết cho $p(x)$. Giả sử $q(x) \in K[x]$ cũng là đa thức bất khả quy dạng chuẩn nhận a làm nghiệm. Theo chứng minh trên, $q(x)$ là bội của $p(x)$. Viết $q(x) = p(x)k(x)$ với $k(x) \in K[x]$. Vì $q(x)$ bất khả quy nên $k(x) = c$ với $0 \neq c \in K$. Do đó $q(x) = cp(x)$. Đồng nhất hệ số cao nhất của hai vế với chú ý rằng $q(x)$ và $p(x)$ đều có dạng chuẩn, ta suy ra $c = 1$.Vì thế $p(x) = q(x)$. □

Định nghĩa 1.1.5. Cho a là phần tử đại số trên K. Đa thức $p(x) \in K[x]$ bất khả quy dạng chuẩn nhận a làm nghiệm được gọi là đa thức bất khả quy của a.

Đa thức $x^3 - 2 \in \mathbb{Q}[x]$ là bất khả quy (vì có bậc 3 và không có nghiệm hữu tỷ), do đó nó là đa thức bất khả quy của phần tử $\sqrt[3]{2}$. Đa thức $x^2 + 1 \in \mathbb{R}[x]$ là bất khả quy (vì có bậc 2 và không có nghiệm thực), do đó nó là đa thức bất khả quy của số phức i.

Mệnh đề 1.1.6. *Cho $p(x) \in K[x]$ là đa thức có bậc dương. Khi đó $p(x)$ bất khả quy nếu và chỉ nếu $p(x) \mid a(x)b(x)$ kéo theo $p(x) \mid a(x)$ hoặc $p(x) \mid b(x)$ với mọi $a(x), b(x) \in K[x]$. Đặc biệt, nếu đa thức bất khả quy $p(x)$ là ước của một tích hữu hạn đa thức thì $p(x)$ phải là ước của ít nhất một trong các đa thức đó.*

Chứng minh. Cho $p(x)$ bất khả quy. Giả sử $p(x) \mid a(x)b(x)$ và $a(x), b(x)$ đều không là bội của $p(x)$. Do $p(x)$ bất khả quy nên $\gcd(p(x), a(x)) = 1$ và $\gcd\ (p(x), b(x)) = 1$. Suy ra tồn tại $s(x), r(x), e(x), f(x) \in K[x]$ sao cho $1 = s(x)p(x) + r(x)a(x)$ và $1 = e(x)p(x) + f(x)b(x)$. Nhân vế với vế của hai đẳng thức này ta có

$$1 = p(x)g(x) + r(x)f(x)a(x)b(x)$$

với $g(x) \in K[x]$ là một đa thức nào đó. Vì $p(x) \mid a(x)b(x)$ nên đa thức bên vế phải của đẳng thức trên là bội của $p(x)$, trong khi đó đa thức bên vế trái là 1 không chia hết cho $p(x)$. Điều này là vô lý.

Ngược lại, do $p(x)$ có bậc dương nên $p(x) \neq 0$ và không khả nghịch. Giả sử $p(x) = a(x)b(x)$ với $a(x), b(x) \in K[x]$. Khi đó $p(x) \mid a(x)b(x)$. Theo giả thiết, $p(x) \mid a(x)$ hoặc $p(x) \mid b(x)$. Vì thế $p(x)$ không có ước thực sự, do đó $p(x)$ bất khả quy. □

Định lý cơ bản của Số học nói rằng mỗi số tự nhiên lớn hơn 1 đều phân tích được thành tích các thừa số nguyên tố và sự phân tích này là duy nhất nếu không kể đến thứ tự các thừa số. Kết quả sau đây là một sự tương tự đối với đa thức.

Định lý 1.1.7. *Mỗi đa thức dạng chuẩn bậc dương trong $K[x]$ có thể phân tích được thành tích các đa thức bất khả quy dạng chuẩn và sự phân tích này là duy nhất nếu không kể đến thứ tự các nhân tử.*

Chứng minh. Trước hết, ta chứng minh sự tồn tại phân tích bằng quy nạp theo bậc của đa thức. Giả sử $f(x) \in K[x]$ là đa thức dạng chuẩn bậc $d > 0$. Nếu $d = 1$ thì $f(x)$ là bất khả quy và sự phân tích bất khả quy của $f(x)$ là $f(x) = f(x)$. Cho $d > 1$ và giả sử kết quả đã đúng cho các đa thức bậc nhỏ hơn d. Nếu $f(x)$ bất khả quy thì $f(x)$ có sự phân tích bất khả quy là $f(x) = f(x)$. Vì thế ta giả thiết $f(x)$ khả quy. Khi đó $f(x) = g(x)h(x)$ với $\deg g(x), \deg h(x) < \deg f(x)$. Đặt $g^*(x) = a^{-1}g(x)$ với a là hệ số cao nhất của $g(x)$. Khi đó ta có $f(x) = g^*(x)(ah(x))$. Đồng nhất hệ số ở hai vế ta suy ra $ah(x)$ có dạng chuẩn. Do đó $f(x) = g^*(x)h^*(x)$ với $g^*(x), h^*(x) = ah(x)$ là các đa thức dạng chuẩn có bậc nhỏ hơn d. Theo giả thiết quy nạp, $g^*(x)$ và $h^*(x)$ phân tích được thành tích của hữu hạn đa thức bất khả quy dạng chuẩn. Vì thế $f(x)$ phân tích được thành tích của hữu hạn đa thức bất khả quy dạng chuẩn.

Bây giờ ta chứng minh tính duy nhất của phân tích. Giả sử $f(x)$ có hai sự phân tích thành nhân tử bất khả quy dạng chuẩn

$$f(x) = p_1(x)\, p_2(x) \ldots p_n(x) = q_1(x)\, q_2(x) \ldots q_m(x).$$

Ta chứng minh bằng quy nạp theo n rằng $n = m$ và sau khi đánh lại thứ tự các nhân tử vế bên phải ta có $p_i(x) = q_i(x)$ với mọi $i = 1, 2, \ldots, n$. Do $p_1(x)$ bất khả quy và $p_1(x) \mid q_1(x)\, q_2(x) \ldots q_m(x)$ nên ta có $p_1(x) \mid q_i(x)$ với i nào đó. Không mất tính tổng quát ta giả thiết $p_1(x) \mid q_1(x)$. Biểu diễn $q_1(x) = p_1(x)t_1(x)$. Vì $q_1(x)$ bất khả quy nên $t_1(x) = a \in K$. Do đó $q_1(x) = ap_1(x)$. Do $p_1(x)$ và $q_1(x)$ có dạng chuẩn nên $a = 1$. Vì thế $p_1(x) = q_1(x)$. Cho $n = 1$. Nếu $m > 1$ thì giản ước cả hai vế cho $p_1(x)$ ta được $1 = q_2(x) \ldots q_m(x)$, điều này là vô lí. Vậy, kết quả đúng cho $n = 1$. Cho $n > 1$. Vì $p_1(x) = q_1(x)$

nên

$$p_2(x)\,p_3(x)\ldots p_n(x) = q_2(x)\,q_3(x)\ldots q_m(x).$$

Theo giả thiết quy nạp ta có $n-1 = m-1$ và bằng việc đánh số lại thứ tự các nhân tử bất khả quy ở vế phải ta suy ra $p_i(x) = q_i(x)$ với mọi $i = 2,\ldots,n$. $\square$

Từ định lý trên ta có kết quả sau:

Hệ quả 1.1.8. *Cho $f(x) \in K[x]$ là đa thức với hệ số cao nhất là a_n. Khi đó tồn tại phân tích $f(x) = a_n f_1(x)\ldots f_k(x)$ với $f_1(x),\ldots,f_k(x)$ là các nhân tử bất khả quy dạng chuẩn, và sự phân tích này là duy nhất nếu không kể đến thứ tự các nhân tử.*

1.2 Một số tiêu chuẩn bất khả quy trên $\mathbb{Q},\mathbb{R},\mathbb{C}$

Định lí cơ bản của Đại số phát biểu rằng mọi đa thức bậc dương với hệ số phức đều có ít nhất một nghiệm phức. Vì thế đa thức bất khả quy trên $\mathbb{C}$ là và chỉ là các đa thức bậc nhất. Sử dụng Định lí cơ bản của Đại số, chúng ta có thể chỉ ra rằng các đa thức bất khả quy trên $\mathbb{R}$ là và chỉ là các đa thức bậc nhất hoặc các đa thức bậc hai vô nghiệm thực (tức là có biệt thức âm). Như vậy, bài toán xét tính bất khả quy của đa thức trên $\mathbb{R}$ và trên $\mathbb{C}$ đã được giải quyết trọn vẹn. Tuy nhiên, bài toán xét tính bất khả quy của các đa thức trên trường $\mathbb{Q}$ các số hữu tỷ cho đến nay vẫn là bài toán mở. Tiết này sẽ trình bày một số tiêu chuẩn bất khả quy của các đa thức trên $\mathbb{Q},\mathbb{R},\mathbb{C}$. Trước hết ta xét tiêu chuẩn bất khả quy trên $\mathbb{Q}$.

Giả sử $f(x) \in \mathbb{Q}[x]$. Chú ý rằng để xét tính bất khả quy trên trường $\mathbb{Q}$, bằng việc quy đồng mẫu số chúng ta chỉ cần xét các đa thức với hệ số nguyên. Từ nay đến hết mục này luôn giả thiết $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, trong đó $a_n \neq 0$ và $n > 0$.

Chú ý rằng một đa thức bậc lớn hơn 1 nếu có nghiệm trong $\mathbb{Q}$ thì khả quy trên $\mathbb{Q}$. Vì vậy, trong nhiều trường hợp ta có thể tìm nghiệm hữu tỷ để xét tính bất khả quy của $f(x)$ trên $\mathbb{Q}$. Sau đây là một ví dụ minh họa.

Ví dụ 1.2.1. (i) $f(x) = 10x^3 + 3x^2 - 106x + 21$ là khả quy trên $\mathbb{Q}$.
(ii) $g(x) = 9x^3 + 6x^2 - 8x + 7$ là bất khả quy trên $\mathbb{Q}$.