ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN VĂN LẬP

VỀ ĐA THỨC KHẢ QUY TRÊN $\mathbb{Z}_p$ NHƯNG BẤT KHẢ QUY TRÊN $\mathbb{Q}$

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - 2015

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN VĂN LẬP

VỀ ĐA THỨC KHẢ QUY TRÊN $\mathbb{Z}_p$ NHƯNG BẤT KHẢ QUY TRÊN $\mathbb{Q}$

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

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC

GS.TS. LÊ THỊ THANH NHÀN

Thái Nguyên - 2015

Mục lục

Lời cảm ơn

Luận văn này được hoàn thành tại trường Đại học Khoa học - Đại học Thái Nguyên. Tác giả xin bày tỏ lòng biết ơn sâu sắc với GS. TS. Lê Thị Thanh Nhàn, đã trực tiếp hướng dẫn tận tình và động viên tác giả trong suốt thời gian nghiên cứu vừa qua.

Tác giả xin chân thành cảm ơn các Thầy cô thuộc Khoa Toán - Tin, trường Đại học Khoa học và GS.TSKH Hà Huy Khoái, GS.TSKH Nguyễn Văn Mậu, PGS.TS Đàm Văn Nhỉ đã giảng dạy, trang bị cho chúng em những kiến thức cần thiết. Xin chân thành cảm ơn Phòng Đào tạo, trường Đại học Khoa học đã tạo điều kiện thuận lợi, động viên, khuyến khích tác giả trong suốt quá trình học tập.

Tác giả cũng xin bày tỏ lòng biết ơn sâu sắc tới gia đình và người thân luôn khuyến khích, động viên tác giả trong suốt quá trình học tập và làm luận văn.

Thái Nguyên, 2015 **Nguyễn Văn Lập**

Học viên Cao học Toán K7D,

Trường ĐH Khoa học - ĐH Thái Nguyên

Danh sách ký hiệu

K	là một trường.
$K[x]$	là vành đa thức một biến x trên K
$\mathbb{Z}$	là vành các số nguyên
$\mathbb{Q}$	là trường các số hữu tỷ
$\mathbb{R}$	là trường các số thực
$\mathbb{C}$	là trường các số phức

Mở đầu

Cho K là một trường và $f(x) \in K[x]$ là một đa thức có bậc dương. Ta nói $f(x)$ là *bất khả quy* nếu $f(x)$ không là tích của hai đa thức có bậc thấp hơn. Ngược lại, nếu $f(x)$ là tích của hai đa thức có bậc thấp hơn thì ta nói $f(x)$ là *khả quy* trên K. Trong vành đa thức trên một trường, đa thức bất khả quy đóng vai trò quan trọng tương tự như vai trò của số nguyên tố trong vành số nguyên. Vì thế, rất nhiều nhà toán học đã quan tâm nghiên cứu tính bất khả quy của đa thức.

Cho $f(x)$ là một đa thức với hệ số nguyên. Để xét tính bất khả quy của $f(x)$ trên $\mathbb{Q}$, người ta thường sử dụng phương pháp rút gọn theo môđun một số nguyên tố. Cụ thể, nếu tồn tại một số nguyên tố p sao cho khi chuyển qua vành $\mathbb{Z}_p[x]$, đa thức $f(x)$ có bậc không đổi và là bất khả quy trên trường $\mathbb{Z}_p$, thì $f(x)$ là bất khả quy trên $\mathbb{Q}$.

Một câu hỏi tự nhiên được đặt ra. Giả sử $f(x)$ là khả quy trên trường $\mathbb{Z}_p$ với mọi số nguyên tố p. Liệu rằng $f(x)$ cũng khả quy trên $\mathbb{Q}$? Người đầu tiên đưa ra câu trả lời phủ định cho câu hỏi trên là nhà toán học nổi tiếng David Hilbert. Một trong những đa thức như thế là $x^4 - 10x^2 + 1$, nó bất khả quy trên $\mathbb{Q}$ nhưng khả quy trên mọi trường $\mathbb{Z}_p$.

Mục đích của luận văn là trình bày lại hai bài báo gần đây về lớp đa thức bất khả quy trên $\mathbb{Q}$ nhưng khả quy trên mọi trường $\mathbb{Z}_p$.

1. E. Driver, P. A. Leonard, K. S. Williams, Irreducible quartic polynomials with factorization modulo p, The Amer. Math. Monthly, 112 (2005),

876-890.

2. Kelly J. Pearson and Tan Zhang, Reducible over any finite field but irreducible over $\mathbb{Q}$, Inter. Math. Forum, 33 (2008), 1607-1610.

Ngoài phần mở đầu và tài liệu tham khảo, luận văn gồm 2 chương với nội dung chính như sau.

Chương 1 trình bày một số khái niệm cơ bản về đa thức bất khả quy.

Chương 2 là nội dung chính của luận văn, chương này trình bày một số tiêu chuẩn bất khả quy trên $\mathbb{Q}$, mối quan hệ giữa tính bất khả quy trên $\mathbb{Q}$ và trên $\mathbb{Z}_p$, tính bất khả quy của đa thức bậc bốn trùng phương và tính bất khả quy trên $\mathbb{Z}_p$ của đa thức bất khả quy của $\sqrt{a} + \sqrt{b}$.

Thái Nguyên, ngày 20 tháng 11 năm 2015

Nguyễn Văn Lập

Email: `nvlap.cg@gmail.com`

Chương 1

Đa thức bất khả quy

Trong suốt chương này, luôn giả thiết K là một trường và $K[x]$ là vành đa thức một biến x với hệ số trong K.

1.1 Định nghĩa, ví dụ và tính chất

Định nghĩa 1.1.1. Đa thức $f(x) \in K[x]$ được gọi là *bất khả quy* trên K nếu $\deg f(x) > 0$ và $f(x)$ không là tích của hai đa thức có bậc thấp hơn.

Nhận xét: Tính chất bất khả quy phụ thuộc vào vành cơ sở. Chẳng hạn, đa thức $x^2 - 7$ là bất khả quy trên $\mathbb{Q}$ nhưng không bất khả quy trên $\mathbb{R}$; đa thức $x^2 + 3$ là bất khả quy trên $\mathbb{R}$ nhưng không bất khả quy trên $\mathbb{C}$.

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

Chứng minh. Cho $a \in K$, với mỗi $h(x) \in K[x]$ 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 hai đa thức có bậc thấp hơn khi và chỉ khi $f(x) = k_1(x)g_1(x)$ là phân 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. $\square$

Cho T là một trường chứa trường K. Nhắc lại rằng một phần tử $a \in T$ được gọi là *nghiệm* của đa thức $f(x) \in K[x]$ nếu $f(a) = 0$.

Kết quả sau đây thường được gọi là Định lí Bezout bé.

Bổ đề 1.1.3. *Phần tử $a \in K$ là nghiệm của đa thức $f(x) \in K[x]$ nếu và chỉ nếu tồn tại đa thức $g(x) \in K[x]$ sao cho $f(x) = (x - a)g(x)$.*

Bổ đề 1.1.4. *Trên một trường K các phát biểu sau 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) Rõ ràng đa thức bậc nhất không thể là tích của hai đa thức bậc thấp hơn, do đó đa thức bậc nhất là bất khả quy.

ii) Giả sử $f(x)$ có nghiệm $a \in K$. Vì $\deg f(x) > 1$ nên theo Bổ đề 1.1.3 ta có $f(x) = (x - a)g(x)$ trong đó $g(x) \in K[x]$ có bậc dương và $\deg g(x) = \deg f(x) - 1$. Do đó $f(x)$ khả quy.

Giả sử $f(x)$ khả quy trên K, tức là $f(x) = g(x)h(x)$ với $\deg g(x) < \deg f(x)$ và $\deg h(x) < \deg f(x)$. Vì $f(x)$ có bậc 2 hoặc bậc 3 nên một trong hai đa thức $g(x)$ hoặc $h(x)$ là bậc nhất. Mà đa thức bậc nhất luôn có nghiệm trên trường đó. Vì vậy $f(x)$ có nghiệm trong K. □

Chú ý rằng phát biểu (ii) của Bổ đề 1.1.4 là không đúng trong trường hợp đa thức có bậc lớn hơn 3. Cụ thể nếu đa thức bậc lớn hơn 3 có nghiệm trong K thì khả quy. Tuy nhiên tồn tại những đa thức không có nghiệm trong K nhưng vẫn khả quy. Ví dụ đa thức $x^4 + 5x^2 + 6 = (x^2 + 2)(x^2 + 3)$ không có nghiệm trong $\mathbb{R}$ nhưng vẫn khả quy trên $\mathbb{R}$.

1.2 Đa thức bất khả quy của một phần tử

Trước hết chúng ta nhắc lại khái niệm phần tử đại số, phần tử siêu việt.

Định nghĩa 1.2.1. Cho F là một trường chứa trường K và $\alpha \in F$. Ta nói rằng α là *phần tử đại số* trên K nếu α là nghiệm của đa thức khác 0 với hệ số trên K. Nếu α không đại số trên K thì ta nói α là *phần tử siêu việt* trên K. Đặc biệt, nếu $\alpha \in \mathbb{C}$ là *đại số* (siêu việt) trên $\mathbb{Q}$ thì α được gọi là *số đại số* (số siêu việt) trên K.

Ví dụ 1.2.2. Mọi số phức $\alpha = a + bi$ đều là đại số trên trường số thực $\mathbb{R}$ vì α là nghiệm của đa thức $x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$. Số thực $\sqrt{3}$ là số đại số vì nó là nghiệm của đa thức $x^2 - 3 \in \mathbb{Q}[x]$. Người ta đã chứng minh rằng số π (tỷ số giữa chu vi và bán kính của một đường tròn) không là nghiệm của bất cứ đa thức khác 0 nào trong $\mathbb{Q}[x]$. Vì thế π là số siêu việt.

Đa thức $f(x) \in K[x]$ được gọi là *có dạng chuẩn* nếu hệ số cao nhất của nó bằng 1.

Mệnh đề 1.2.3. *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 dạng chuẩn $p(x) \in K[x]$ bất khả quy 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 một 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 $p(x)$ và một trong hai đa thức này nhận a làm nghiệm, điều này mâu thuẫn với cách chọn $p(x)$. Do đó $f(x)$ bất khả quy.

Giả sử $g(x) \in K[x]$ nhận a làm nghiệm. Nếu $g(x)$ không chia hết cho $p(x)$ thì $\gcd(g(x), p(x)) = 1$ vì $p(x)$ bất khả quy. Do đó tồn tại $q(x), h(x) \in K[x]$ sao cho $1 = p(x).q(x)+g(x).h(x)$. Thay $x = a$ ta được $1 = p(a).q(a)+$