ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ LINH

GIÁ TRỊ NGUYÊN TỐ CỦA ĐA THỨC BẤT KHẢ QUY

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - 2014

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ LINH

GIÁ TRỊ NGUYÊN TỐ CỦA ĐA THỨC BẤT KHẢ QUY

Chuyên ngành: **PHƯƠNG PHÁP TOÁN SƠ CẤP**
Mã số: 60.46.01.13

LUẬN VĂN THẠC SĨ TOÁN HỌC

Người hướng dẫn khoa học: **PGS.TS. Lê Thị Thanh Nhàn**

Thái Nguyên - 2014

Mục lục

LỜI CẢM ƠN

Trước hết, tôi xin gửi lời biết ơn chân thành và sâu sắc nhất đến PGS.TS Lê Thị Thanh Nhàn. Mặc dù rất bận rộn trong công việc nhưng cô vẫn dành rất nhiều thời gian và tâm huyết trong việc hướng dẫn. 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 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 thiện luận văn này.

Cuối cùng tôi xin chân thành bày tỏ lòng biết ơn tới gia đình, bạn bè và các thành viên trong lớp cao học Toán K6C (khóa 2012-2014) 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.

Tôi xin chân trọng cảm ơn!

LỜI NÓI ĐẦU

Vai trò của đa thức bất khả quy trong tập các đa thức cũng quan trọng giống như vai trò của số nguyên tố trong tập số nguyên. Chính vì vậy, sự tương tự giữa số nguyên tố và đa thức bất khả quy là một chủ đề quan trọng trong sự phát triển và sự liên hệ qua lại của Lí thuyết số và Hình học Đại số. Cho đến nay, còn nhiều giả thuyết, nhiều câu hỏi liên quan đến sự tương tự này vẫn chưa được giải quyết. Chẳng hạn, một giả thuyết nổi tiếng của Buniakowski đặt ra năm 1854 phát biểu rằng nếu đa thức bậc dương $f(x) \in \mathbb{Z}[x]$ là bất khả quy trên $\mathbb{Q}$ sao cho tập các giá trị $\{f(n) \mid n \in \mathbb{N}, n > 0\}$ của $f(x)$ không có ước chung lớn hơn 1 thì $f(n)$ là số nguyên tố với vô hạn điểm $n \in \mathbb{N}$ (xem S. Lang [La, Trang 323]). Giả thuyết này là một trong những bài toán lớn của Lí thuyết số chưa được giải quyết khi bậc của $f(x)$ lớn hơn 1.

Mục đích chính của luận văn là trình bày một số mối quan hệ giữa số nguyên tố và đa thức bất khả quy. Cụ thể, nếu một đa thức bậc dương (với hệ số nguyên) nhận giá trị nguyên tố tại vô hạn điểm thì đa thức đó bất khả quy trên trường hữu tỷ $\mathbb{Q}$. Luận văn quan tâm đến câu hỏi ngược lại, nếu một đa thức bất khả quy thì nó có nhận giá trị nguyên tố tại vô hạn điểm không. Nội dung luận văn chủ yếu trình bày lại các kết quả trong bài báo ``Prime numbers and irreducible polynomials" của M. Ram Murty [Mu] về mối liên hệ giữa tính bất khả quy trên $\mathbb{Q}$ và giá trị nguyên tố của đa thức với hệ số nguyên. Bên cạnh đó, luận văn cũng trình bày một số tính chất của đa thức bất khả quy tương tự như tính chất của số nguyên tố.

Luận văn được viết chủ yếu dựa theo 4 tài liệu sau đây:

1. D. Cox, J. Little, D. O'Shea, *Ideals, varieties, and algorithms*, Springer-Verlag, 2006 (Third Edition).

2. S. Lang, *Algebra*, 3rd edition, Addison-Wesley, Reading, 1993.

3. M. Ram Murty,*Prime numbers and irreducible polynomials*, The American Math. Monthly, 109 (2002), 452-458.

4. J. Stillwell, *Elements of Number Theory*, Springer, 2003.

Luận văn gồm 3 chương. Chương 1 trình bày lại các khái niệm cơ bản của đa thức bất khả quy, sự tương tự của đa thức bất khả quy với số nguyên tố và một số tiêu chuẩn xét tính bất khả quy của đa thức trên trường $\mathbb{Q}$. Chương 2 trình bày về khái niệm trường phân rã của đa thức, tính bất khả quy của đa thức trên $\mathbb{C}$ và trên $\mathbb{R}$. Chương 3 là nội dung chính của luận văn, trình bày về mối quan hệ giữa tính bất khả quy và giá trị nguyên tố, trong chương này luận văn cũng chỉ ra một phương pháp khác để xây dựng các đa thức bất khả quy trên $\mathbb{Q}$ xuất phát từ các số nguyên tố.

Chương 1

Đa thức bất khả quy

1.1 Đa thức bất khả quy và sự tương tự với số nguyên tố

Trong suốt chương này luôn giả thiết F là một trường.

1.1.1 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 $f(x)$ *khả quy*.

1.1.2 Ví dụ. (i) Đa thức $f(x) = x^2 + 1 \in \mathbb{R}[x]$ bất khả quy trên $\mathbb{R}$.
(ii) Đa thức $f(x) = x^2 - 1 \in \mathbb{R}[x]$ khả quy trên $\mathbb{R}$, vì $x^2 - 1 = (x-1)(x+1)$.

Sau đây là một số tính chất đơn giản về đa thức bất khả quy.

1.1.3 Bổ đề. *Cho $f(x) \in F[x]$. Các phát biểu sau là đúng.*
(i) Nếu $f(x)$ có bậc 1 thì $f(x)$ 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) Nếu $f(x)$ có bậc dương và $a \in F$ thì $f(x)$ là bất khả quy nếu và chỉ nếu $f(x+a)$ là bất khả quy.

Chứng minh. (i) Rõ ràng đa thức bậc nhất không thể là tích của hai đa thức bậc thấp hơn.
(ii) Vì $f(x) > 1$ và $f(x)$ có nghiệm $x = a \in F$ nên $f(x) = (x-a)g(x)$, trong đó $\deg g(x) = \deg f(x) - 1 \geq 1$. Vì thế $f(x)$ khả quy.
(iii) Cho $f(x)$ có bậc 2 hoặc 3. Nếu f khả quy thì nó phân tích thành tích của hai đa thức bậc thấp hơn, một trong hai đa thức đó phải có bậc 1, do đó $f(x)$ có nghiệm trong F. Nếu $f(x)$ có nghiệm trong F thì theo (ii), $f(x)$ khả quy.
(iv) Với mỗi $h(x) \in F[x]$, 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 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 $f(x)$ khả quy khi và chỉ khi $f(x+a)$ khả quy. $\square$

Chú ý rằng tính bất khả quy phụ thuộc vào trường cơ sở. Chẳng hạn, đa thức $x^3 - 2$ là bất khả quy trên $\mathbb{Q}$ vì nó có bậc 3 và nó không có nghiệm trong $\mathbb{Q}$. Trong khi đó đa thức này lại không bất khả quy trên $\mathbb{R}$ vì nó có sự phân tích $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$ trong $\mathbb{R}[x]$.

Tiếp theo chúng ta định nghĩa khái niệm đa thức bất khả quy của một phần tử.

1.1.4 Định nghĩa. Cho K là một trường chứa F và $a \in K$. Ta nói a là *phần tử đại số trên* F nếu tồn tại đa thức $0 \neq f(x) \in F[x]$ nhận a làm nghiệm. Nếu a không đại số trên F thì a là *siêu việt* trên F. Một số phức α được gọi là *số đại số* nếu α là phần tử đại số trên $\mathbb{Q}$. Nếu α không đại số trên $\mathbb{Q}$ thì ta nói α là *số siêu việt*.

Chẳng hạn, $\sqrt[3]{2}$ là số đại số vì nó là nghiệm của đa thức $x^3 - 2 \in \mathbb{Q}[x]$. Người ta đã chứng minh được số π là số siêu việt.

Một đa thức $f(x) \in F[x]$ được gọi là có *dạng chuẩn* nếu hệ số cao nhất của $f(x)$ bằng 1. Chú ý rằng nếu $0 \neq f(x) \in F[x]$ là một đa thức với hệ số cao nhất a_n thì $f^*(x) = a_n^{-1} f(x)$ là một đa thức dạng chuẩn.

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

Chứng minh. Vì a là nghiệm của một đa thức khác 0 với hệ số trong F nên tồn tại đa thức khác 0 với hệ số trong F có bậc bé nhất nhận a làm nghiệm. Gọi $p(x) \in F[x]$ là dạng chuẩn của đa thức này. Khi đó a là nghiệm của $p(x)$. Ta chứng minh $p(x)$ bất khả quy. Giả sử $p(x)$ không bất khả quy. Khi đó $p(x)$ phân tích được thành tích của hai đa thức trong $F[x]$ có bậc bé hơn, và do đó một trong hai đa thức này phải nhận a làm nghiệm, điều này là mâu thuẫn với cách chọn $p(x)$. Giả sử $g(x) \in F[x]$ nhận a làm nghiệm. Nếu $p(x)$ không là ước của $g(x)$ thì vì $p(x)$ bất khả quy nên $\gcd(g(x), p(x)) = 1$, do đó $1 = p(x)q(x) + g(x)h(x)$ với $q(x), h(x) \in F[x]$. Thay $x = a$ và cả hai vế ta được $1 = 0$, điều này là vô lí. Vậy $g(x)$ chia hết cho $p(x)$. Giả sử $q(x) \in F[x]$ 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 $q(x) = p(x)k(x)$. Vì $q(x)$ bất khả quy nên $k(x) = b \in F$. Do đó $q(x) = bp(x)$. 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 $b = 1$. Vì thế $p(x) = q(x)$. □

Đa thức $p(x) \in F[x]$ bất khả quy dạng chuẩn nhận a làm nghiệm được gọi là *đa thức bất khả quy* của a.

1.1.6 Ví dụ. (i) Đa thức $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ là đa thức bất khả quy của phần tử $\sqrt{2} + \sqrt{3} \in \mathbb{R}$. Thật vậy, giả sử $x^4 - 10x^2 + 1$ không bất khả quy trên trường hữu tỷ. Khi đó nó phân tích được thành tích của hai đa thức với hệ số hữu tỷ là $f(x)$ và $g(x)$, trong đó $f(x)$ có bậc 3 và $g(x)$ có bậc 1, hoặc $f(x)$ và $g(x)$ có cùng bậc 2. Nếu f có bậc 3 và g có bậc 1 thì g có nghiệm hữu tỷ, và do đó $x^4 - 10x^2 + 1$ cũng có nghiệm hữu tỷ, điều này là vô lí. Do đó f và g có cùng bậc 2. Không mất tính tổng quát ta có thể giả thiết hệ số cao nhất của f và g là 1. Viết $f(x) = x^2 + ax + b$ và $g(x) = x^2 + cx + d$, trong đó a, b, c, d là những số hữu tỷ. Từ đẳng thức $x^4 - 10x^2 + 1 = f(x)g(x)$, đồng nhất các hệ số ở hai vế ta được

$$a = -c, ac + b + d = -10, ad + bc = 0, bd = 1.$$

Với $a = -c$ thay vào phương trình $ad + bc = 0$ ta được $-cd + bc = 0$ hay $c(b - d) = 0$. Suy ra $c = 0$ hoặc $b = d$.

+ Trường hợp $c = 0$. Ta thay c vào $ac + b + d = -10$ ta được $b + d = -10$ hay $b = -10 - d$. Thay b vào phương trình $bd = 1$ ta được phương trình $d^2 + 10d + 1 = 0$. Giải phương trình này ta được $d = -5 \pm 2\sqrt{6} \notin \mathbb{Q}$.

+ Trường hợp $b = d$. Kết hợp với điều kiện $bd = 1$ ta được $b = d = 1$ hoặc $b = d = -1$. Với $b = d = 1$ thay vào phương trình $ac + b + d = -10$ ta được $c = \pm\sqrt{12} \notin \mathbb{Q}$. Với $b = d = -1$ thay vào phương trình $ac + b + d = -10$ ta được $c = \pm\sqrt{8} \notin \mathbb{Q}$.

Như vậy, trong mọi trường hợp đều có ít nhất một trong các số a, b, c, d không là số hữu tỷ. Điều này vô lí. Vậy, $x^4 - 10x^2 + 1$ là bất khả quy trên trường hữu tỷ và rõ ràng đa thức này nhận $\sqrt{2} + \sqrt{3}$ làm nghiệm.

(ii) $x^2 - 2x + 2 \in \mathbb{R}[x]$ là đa thức bất khả quy của phần tử $1 + i \in \mathbb{C}$. Thật vậy, đa thức $x^2 - 2x + 2$ là bất khả quy trên trường số thực vì nó có bậc hai và nó không có nghiệm thực. Rõ ràng đa thức này nhận $1 + i$ làm nghiệm, do đó nó là đa thức bất khả quy của $1 + i$.

Đa thức bất khả quy có những tính chất tương tự như tính chất của số nguyên tố. Trước hết, chúng ta đã biết, Bổ đề Euclid phát biểu rằng số tự