ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

VŨ VĂN HẢO

VỀ ĐA THỨC BẤT KHẢ QUY TRÊN TRƯỜNG HỮU HẠN

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2019

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

VŨ VĂN HẢO

VỀ ĐA THỨC BẤT KHẢ QUY TRÊN TRƯỜNG HỮU HẠN

Chuyên ngành: Phương pháp Toán sơ cấp

Mã số: 8 46 01 13

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
TS. Ngô Thị Ngoan

THÁI NGUYÊN - 2019

Mục lục

Lời cảm ơn

Luận văn này được thực hiện tại Trường Đại học Khoa học – Đại học Thái Nguyên và hoàn thành dưới sự hướng dẫn của TS. Ngô Thị Ngoan. Tác giả xin được bày tỏ lòng biết ơn chân thành và sâu sắc tới người hướng dẫn khoa học của mình, người đã đặt vấn đề nghiên cứu, dành nhiều thời gian hướng dẫn và tận tình giải đáp những thắc mắc của tác giả trong suốt quá trình làm luận văn.

Tác giả cũng đã học tập được rất nhiều kiến thức chuyên ngành bổ ích cho công tác và nghiên cứu của bản thân. Tác giả xin bày tỏ lòng cảm ơn sâu sắc tới các thầy giáo, cô giáo đã tham gia giảng dạy lớp Cao học Toán K11D (khóa 2017–2019); Nhà trường và các phòng chức năng của Trường; Khoa Toán – Tin, trường Đại học Khoa học – Đại học Thái Nguyên đã quan tâm và giúp đỡ tác giả trong suốt thời gian học tập tại trường.

Tác giả cũng xin gửi lời cảm ơn sâu sắc tới Trường Trung học phổ thông Quang Hà đã giúp đỡ, tạo mọi điều kiện thuận lợi giúp tôi có thể hoàn thành luận văn này.

Tác giả cũng xin gửi lời cảm ơn tới tập thể lớp Cao học Toán K11D (khóa 2017–2019) đã luôn động viên và giúp đỡ tác giả rất nhiều trong quá trình học tập, nghiên cứu.

Cuối cùng, tôi xin gửi lời cảm ơn chân thành tới gia đình, bạn bè, lãnh đạo đơn vị công tác và đồng nghiệp đã động viên, giúp đỡ và tạo điều kiện tốt nhất cho tôi khi học tập và nghiên cứu.

Thái Nguyên, tháng 5 năm 2019

Tác giả

Vũ Văn Hảo

Mở đầu

Đa thức bất khả quy là khái niệm đóng vai trò quan trọng và có nhiều áp dụng. Đây cũng là vấn đề kinh điển trong lý thuyết đa thức nói riêng và trong toán học nói chung. Các bài toán về đa thức bất khả quy và bài toán phân tích một đa thức thành nhân tử bất khả quy đã được đưa vào giảng dạy ngay từ THCS. Việc phân tích trên cho phép học sinh chuyển việc giải một phương trình đại số về các phương trình có bậc thấp hơn. Trong chương trình toán học cao cấp, khái niệm đa thức bất khả quy được đưa vào giảng dạy trong các năm đầu tiên của chương trình đào tạo Đại học. Lúc này, sinh viên được tiếp xúc với những tiêu chuẩn về tính bất khả quy của các đa thức trên $\mathbb{Z}[x], \mathbb{Q}[x]$ như tiêu chuẩn Eisenstein, tiêu chuẩn Person, tiêu chuẩn Dumas. Đặc biệt có thể sử dụng một kỹ thuật quan trọng là xét tính bất khả quy của đa thức hệ số nguyên thông qua việc rút gọn theo modulo p nguyên tố.

Trong khuôn khổ luận văn này, tôi trình bày những tìm hiểu về đa thức bất khả quy trên trường hữu hạn: Một số lớp đa thức bất khả quy; việc xây dựng được những đa thức bất khả quy mới từ hai đa thức bất khả quy đã cho; việc xây dựng được dãy vô hạn các đa thức bất khả quy với bậc tăng dần từ một đa thức bất khả quy ban đầu trên các trường hữu hạn.

Nội dung luận văn bao gồm hai chương:

Chương 1 của luận văn trình bày về trường hữu hạn. Nội dung chương 1 được tham khảo chủ yếu từ các tài liệu [1] và [6]. Chúng ta sẽ trình bày về mở rộng trường, trường phân rã của đa thức, cấu trúc của trường hữu hạn và công thức nghịch đảo Möbius [6] giúp ta xác định các đa thức dạng chuẩn (đa thức monic) bất khả quy trên trường hữu hạn $\mathbb{F}_q$ bất kỳ có bậc n.

Chương 2 của luận văn trình bày về đa thức bất khả quy trên trường hữu hạn. Chúng ta sẽ trình bày một lớp đa thức bất khả quy trên trường $\mathbb{F}_q[x]$

với $q = p^n$; xây dựng những đa thức bất khả quy từ hai đa thức bất khả quy đã cho; xây dựng được dãy vô hạn những đa thức bất khả quy trên trường hữu hạn có đặc số 2 bằng cách sử dụng $Q-$ biến đổi; xây dựng dãy vô hạn những đa thức bất khả quy có bậc tăng dần trên trường hữu hạn có đặc số lẻ bằng cách sử dụng $R-$ biến đổi từ một đa thức bât khả quy ban đầu.

Thái Nguyên, ngày 25 tháng 5 năm 2019

Tác giả luận văn

Vũ Văn Hảo

Chương 1

Trường hữu hạn

1.1 Một số khái niệm

Ta nhắc lại, một trường F là một vành giao hoán khác không và không có ước của 0. Một trường có hữu hạn phần tử được gọi là một *trường hữu hạn.*

Định nghĩa 1.1.1. Trường F được gọi là một *trường nguyên tố* nếu nó không có trường con nào ngoài bản thân nó.

Nhận xét 1.1.2.
(i) Cho F là trường nguyên tố. Khi đó chỉ có thể xảy ra một trong hai trường hợp: nếu F có đặc số 0 thì $F \cong \mathbb{Q}$; nếu F có đặc số p thì $F \cong \mathbb{Z}_p$. Trường hợp $F \cong \mathbb{Z}_p$. Ta thường kí hiệu $\mathbb{F}_p$ thay cho F.
(ii) Cho E là một trường tùy ý, khi đó nếu gọi F là giao của mọi trường con của E thì F cũng là một trường con của E, rõ ràng F là trường con nhỏ nhất của E, do đó F là trường nguyên tố. Trong trường hợp này, ta nói F là trường con nguyên tố của E. Như vậy, mọi trường đều chứa một trường con nguyên tố.

Bổ đề 1.1.3 (Cấu trúc trường hữu hạn)**.**
(i) *Cho F là trường hữu hạn có q phần tử. Khi đó tồn tại số nguyên tố p sao cho $q = p^n$ với số tự nhiên n nào đó.*
(ii) *Với mỗi số nguyên tố p và số tự nhiên $n \neq 0$, tồn tại duy nhất một trường hữu hạn có p^n phần tử (sai khác một đẳng cấu trường).*

Chứng minh.
(i) Gọi p là đặc số của trường F, khi đó p là số nguyên tố. Gọi $\mathbb{F}_p$ là trường con nguyên tố của F, khi đó $\mathbb{F}_p \cong \mathbb{Z}_p$. Ta biết rằng F là $\mathbb{F}_p-$không gian vectơ hữu hạn chiều. Giả sử $\dim_{\mathbb{F}_p}(F) = n < \infty$, khi đó F có một cơ sở là $\{e_1, \ldots, e_n\}$ và vì thế mỗi phần tử của F có dạng $x = \sum_{i=1}^{n} a_i e_i$ với $a_1, \ldots, a_n \in \mathbb{F}_p$. Từ đó suy ra số phần tử của F bằng số các bộ phần tử $(a_1, \ldots, a_n) \in \mathbb{F}_p \times \ldots \times \mathbb{F}_p$ (n lần). Do đó $q = p^n$.
(ii) Sự tồn tại của trường có $q = p^n$ phần tử. Xét đa thức $f(x) = x^q - x \in \mathbb{F}_p[x]$ với $\mathbb{F}_p \cong \mathbb{Z}_p$ là trường nguyên tố có đặc số nguyên tố p. Gọi E là trường phân rã của $f(x)$ trên $\mathbb{F}_p$. Đặt

$$K = \{\alpha \in E \mid f(\alpha) = 0\}$$

đó chính là tập hợp các nghiệm của $f(x)$. Khi đó K là một trường con của E. Thật vậy, với mọi $\alpha, \beta \in K$ ta có

$$(\alpha - \beta)^q = \alpha^q - \beta^q = \alpha - \beta, (\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$$

Do đó $\alpha - \beta, \alpha\beta \in K$. Nếu $\alpha \in K^*$ thì $(\alpha^{-1})^q = (a^q)^{-1} = \alpha^{-1}$ suy ra $\alpha^{-1} \in K$. Ngoài ra, rõ ràng $1^q = 1$ nên $1 \in K$. Cuối cùng, ta thấy rằng mọi $a \in \mathbb{F}_p$ đều thỏa mãn $a^p = a$ do đó $a^q = a^{p^n} = a$ chứng tỏ $\mathbb{F}_p \subseteq K$. Như vậy K chính là trường phân rã của $f(x)$ trên $\mathbb{F}_p$, trường này có $q = p^n$ phần tử (lưu ý rằng $f(x)$ không có nghiệm bội).

Tính duy nhất của trường có $q = p^n$ phần tử. Giả sử $\mathbb{F}_q$ là trường có $q = p^n$ phần tử. Khi đó $\mathbb{F}_q$ có đặc số là p (giả sử p_1 là đặc số của $\mathbb{F}_q$ thì theo (i) suy ra $q = p_1^{n'}$; do đó $p^n = p_1^{n'}$ vì thế $p = p_1$). Vì $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ là nhóm với phép nhân nên $\alpha^{q-1} = 1$ với mọi $\alpha \in \mathbb{F}_q^*$; do đó $\alpha^q = \alpha$ với mọi $\alpha \in \mathbb{F}_q$. Chứng tỏ mọi phần tử của $\mathbb{F}_q$ đều là nghiệm của đa thức $f(x) = x^q - x \in \mathbb{F}_p[x]$ với $\mathbb{F}_p$ là trường nguyên tố của $\mathbb{F}_q$. Suy ra trường $\mathbb{F}_q$ chính là trường phân rã của $f(x)$ trên $\mathbb{F}_p$. Điều đó khẳng định tính duy nhất của $\mathbb{F}_q$ sai khác một đẳng cấu trường. □

Trong luận văn, chúng ta sẽ quan tâm nghiên cứu về đa thức bất khả quy trên trường hữu hạn $\mathbb{F}_q$. Đa thức bất khả quy trên trường $\mathbb{F}_q$ chính là phần tử bất khả quy của vành đa thức $\mathbb{F}_q[x]$.

Định nghĩa 1.1.4. Một đa thức với hệ số trên một trường được gọi là *bất khả quy* nếu nó có bậc dương và không phân tích được thành tích của hai đa thức có bậc thấp hơn.

Định lý 1.1.5. *Cho F là trường hữu hạn có đặc số p. Khi đó ta có*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n},\ (a-b)^{p^n} = a^{p^n} - b^{p^n}$$

với mọi $a, b \in F,\ n \in \mathbb{N} \setminus \{0\}$.

Chứng minh. Ta có khai triển

$$(a+b)^p = \sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} a^k b^{p-k} \text{ với } \begin{pmatrix} p \\ k \end{pmatrix} = C_p^k,$$

mà $p \mid \begin{pmatrix} p \\ k \end{pmatrix}$ với mỗi $0 < k < p$ vì vậy $(a+b)^p = a^p + b^p$. Bằng quy nạp theo n, biến đổi $(a+b)^{p^n} = ((a+b)^{p^{n-1}})^p$ suy ra $(a+b)^{p^n} = a^{p^n} + b^{p^n}$. Để chứng minh $(a-b)^{p^n} = a^{p^n} - b^{p^n}$, ta biến đổi

$$(a-b)^{p^n} = (a+(-b))^{p^n} = a^{p^n} + (-b)^{p^n}.$$

Nếu p lẻ thì ta có $(-1)^{p^n} = -1$, nếu p chẵn thì $p = 2$ và $(-1)^{p^n} = 1 = -1$. □

Cho p là số nguyên tố, và $1 \leq n \in \mathbb{Z}$. Đặt $q = p^n$. Khi đó ta có định lý sau.

Định lý 1.1.6. *Nhóm nhân $\mathbb{F}^*_q$ của trường hữu hạn $\mathbb{F}$ là xyclic cấp $q-1$.*

Để chứng minh Định lý 1.1.6 ta cần các bổ đề sau đây.

Bổ đề 1.1.7. *Nếu $1 \leq m \in \mathbb{Z}$, thì $m = \sum_{d|m} \varphi(d)$, trong đó $\varphi(d)$ là kí hiệu cho hàm Euler.*

Chứng minh. Nếu d chia hết m, thì ta kí hiệu C_d là nhóm con duy nhất của $\mathbb{Z}_m$ có cấp d, và kí hiệu Φ_d là tập tất cả các phần tử sinh của C_d. Vì mỗi phần tử bất kì của $\mathbb{Z}_m$ đều sinh ra một trong các nhóm C_d nào đó, nên nhóm $\mathbb{Z}_m$ là hợp rời của các tập Φ_d; từ đó ta có

$$m = |Z_m| = \sum_{d|m} |\Phi_d| = \sum_{d|m} \varphi(d).$$

□

Bổ đề 1.1.8. *Cho H là một nhóm hữu hạn cấp n. Giả sử rằng, với mỗi ước d của n, tập các phần tử $x \in H$ sao cho $x^d = 1$ có nhiều nhất là d phần tử. Khi đó H là nhóm xyclic.*

Chứng minh. Cho d là một ước của m. Nếu tồn tại $x \in H$ có cấp d, thì nhóm con $(x) = \{1, x, \ldots, x^{d-1}\}$ là nhóm xyclic cấp d; mặt khác theo giả thiết, có không quá d phần tử $y \in H$ thỏa mãn $y^d = 1$. Vì thế mọi $y \in H$ sao cho $y^d = 1$ đều thuộc vào (x). Đặc biệt, mọi phần tử của H có cấp d đều sinh ra (x) và có tất cả $\varphi(d)$ phần tử cấp d. Vì thế số phần tử của H có cấp d hoặc là 0 hoặc $\varphi(d)$.

Lưu ý rằng với trường hợp nhóm H hữu hạn bất kì có cấp n, ta cũng luôn có

$$H = \bigcup_{d'|m, \exists x' \in H \text{ có cấp } d'} \Phi(d')$$

trong đó $\Phi(d')$ là kí hiệu cho tập tất cả các phần tử của H có cấp d'. Do đó

$$m = |H| = \sum_{d'|m, \exists x' \in H \text{ có cấp } d'} |\Phi(d')| = \sum_{d'|m, \exists x' \in H \text{ có cấp } d'} \varphi(d').$$

Nếu tồn tại $d|m$ mà không có phần tử nào của H có cấp d thì công thức trên cho thấy

$$m \leq \sum_{d'|n,\ d' \neq d} \varphi(d') < \sum_{d'|n} \varphi(d')$$

trong khi đó $\sum_{d'|m} \varphi(d') = m$ theo Bổ đề 1.1.7. Từ đó suy ra mâu thuẫn. Vậy mọi ước d của n đều có phần tử của H có cấp d. Đặc biệt, có một phần tử $x \in H$ có cấp m, và do đó H trùng với nhóm xyclic (x). □

Chứng minh Định lý 1.1.6. Định lý này được suy ra từ Bổ đề 1.1.8 áp dụng cho $H = \mathbb{F}_q^*$ và $m = q - 1$. Thật vậy với mọi $d|(q-1)$, ta có phương trình $x^d - 1 = 0$ có bậc d và có hệ số trên một trường $\mathbb{F}_p$, nên nó có nhiều nhất là d nghiệm trong $\mathbb{F}_q$. □

Chú ý 1.1.9. Từ chứng minh trên cho thấy một kết quả tổng quát hơn đó là mọi nhóm con hữu hạn của nhóm nhân của một trường đều là xyclic.

Định lý 1.1.10. *Cho $\mathbb{F}_q$ là trường hữu hạn và đa thức $f \in \mathbb{F}_q[x]$ bất khả quy trên $\mathbb{F}_q$, $\deg f = n$. Khi đó trường phân rã của f trên $\mathbb{F}_q$ là $\mathbb{F}_{q^n}$. Hơn*