ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC
——————o0o——————

ĐINH NGỌC PHÚC

ĐA THỨC HOÁN VỊ ĐƯỢC MODULO LŨY THỪA MỘT SỐ NGUYÊN TỐ

THÁI NGUYÊN, 08/2018

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

—————o0o—————

ĐINH NGỌC PHÚC

ĐA THỨC HOÁN VỊ ĐƯỢC MODULO LŨY THỪA MỘT SỐ NGUYÊN TỐ

CHUYÊN NGÀNH: PHƯƠNG PHÁP TOÁN SƠ CẤP
MÃ SỐ: 8460113

LUẬN VĂN THẠC SĨ TOÁN HỌC

GIÁO VIÊN HƯỚNG DẪN:
GS.TS. LÊ THỊ THANH NHÀN

THÁI NGUYÊN, 08/2018

Mục lục

LỜI CẢM ƠN

Trước hết, tôi xin gửi lời biết ơn chân thành đến GS. TS. Lê Thị Thanh Nhàn đã hướng dẫn tôi hoàn thành bản luận văn này. Khi bắt đầu nhận đề tài thực sự tôi cảm nhận đề tài mang nhiều nội dung mới mẻ. Hơn nữa với vốn kiến thức ít ỏi cùng với kinh nghiệm làm đề tài không nhiều nên tôi chưa thực sự tự tin để tiếp cận đề tài. Mặc dù rất bận rộn trong công việc nhưng Cô vẫn dành nhiều thời gian và tâm huyết trong việc hướng dẫn, động viên khuyến khích tôi trong suốt thời gian tôi thực hiện đề tài. Trong quá trình tiếp cận đề tài đến quá trình hoàn thiện luận văn Cô luôn tận tình chỉ bảo và tạo điều kiện tốt nhất nhất cho tôi hoàn thành luận văn. Cho đến bây giờ luận văn thạc sĩ của tôi đã được hoàn thành, xin cảm ơn Cô đã đôn đốc, nhắc nhở tôi.

Tôi xin trân trọng cảm ơn Ban Giám hiệu, Khoa Toán - Tin và Phòng Đào tạo của 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 thành luận văn này.

Tôi xin trân trọng cảm ơn Ban giám hiệu, các thầy cô giáo trường THPT Nguyễn Đăng Đạo -Bắc Ninh nơi tôi công tác đã tạo điều kiện giúp đỡ tôi hoàn thành công việc chuyên môn tại nhà trường để tôi hoàn thành chương trình học tập cao học.

Cuối cùng, tôi xin chân thành bày tỏ lòng biết ơn đến gia đình, bạn bè, những người không ngừng động viên, hỗ trợ tạo mọi điều kiện tốt nhất cho tôi trong suốt quá trình học tập và thực hiện luận văn.

Thái nguyên, ngày 10/08/2018

Tác giả

PHẦN MỞ ĐẦU

Trong Toán học, một đa thức một biến $f(x)$ với hệ số trên một vành giao hoán V được gọi là *đa thức hoán vị được trên* V (hay gọi là đa thức hoán vị trên V) nếu $f(x)$ tác động như một hoán vị trên V, nghĩa là ánh xạ cảm sinh $a \mapsto f(a)$ là một song ánh trên V. Chẳng hạn, khi $V = \mathbb{R}$ là trường số thực, thì đa thức $f(x) = x + 1$ là hoán vị được trên $\mathbb{R}$, tuy nhiên đa thức $g(x) = x^2$ thì không hoán vị được trên $\mathbb{R}$. Khi $V = \mathbb{Z}_2$, thì đa thức $f(x) = x+1$ là hoán vị được trên $\mathbb{Z}_2$ (do $f(0) = 1$ và $f(1) = 0$), còn đa thức $g(x) = x^2 + x + 1$ không hoán vị được (vì $g(0) = 1 = g(1)$).

Các nghiên cứu về tính hoán vị được của đa thức trên trường hữu hạn có nhiều ứng dụng trong Tổ hợp, Hình học, Khoa học máy tính và đóng vai trò quan trọng trong mã hóa, bảo mật, đặc biệt là trong các thuật toán phát hiện lỗi, thuật toán hiệu đính,... Đa thức hoán vị được, bắt đầu được nghiên cứu bởi Charles Hermite (1822-1901) cho trường hợp trường $\mathbb{Z}_p$, với p là một số nguyên tố. Tiếp đó, Leonard Eugene Dickson (1874-1954) là người đầu tiên mở rộng nghiên cứu tính hoán vị được của đa thức trên trường hữu hạn tùy ý. Nếu $\mathbb{F}$ là trường hữu hạn thì số phần tử của $\mathbb{F}$ là p^n với p là một số nguyên tố và n là một số nguyên dương. Vì thế nếu đa thức $f(x)$ hoán vị được trên trường $\mathbb{F}$ thì ta cũng nói $f(x)$ hoán vị được modulo p^n. Khi đó, chú ý rằng nếu F là một trường hữu hạn, thì đa thức $f(x) \in F[x]$ là hoán vị được trên F khi và chỉ khi ánh xạ cảm sinh $f : F \to F$ là đơn ánh, khi và chỉ khi ánh xạ này là toàn ánh. Vì thế, việc xét tính hoán vị được có phần được giảm nhẹ. Tuy nhiên, đặc trưng tính hoán vị được của đa thức trên một trường hữu hạn vẫn là bài toán khó, chưa có lời giải.

Đã có rất nhiều nhà toán học quan tâm và có một số công trình được công bố gần đây về tính hoán vị được của đa thức trên vành có p^n phần

tử, với p là một số nguyên tố và n là số nguyên dương. Gần đây trong một công trình của mình, hai tác giả Rajesh P Singh và Soumen Maity đã đưa ra một điều kiện cần và đủ để đa thức $f(x) = a_0 + a_1x + \ldots + a_dx^d$ với hệ số nguyên là hoán vị được trên vành $\mathbb{Z}_{p^n}$, với $p = 2, 3, 5$ thông qua các hệ số $a_0, a_1, \ldots, a_d$.

Mục đích của luận văn là trình bày lại các kết quả về tính hoán vị được của đa thức modulo lũy thừa một số nguyên tố, bao gồm tính hoán vị được trên một trường hữu hạn và tính hoán vị được trên vành $\mathbb{Z}_{p^n}$ với p là số nguyên tố.

Luận văn gồm hai chương. Chương 1 trình bày về đa thức bất khả quy, trường phân rã của một đa thức, cấu trúc của trường hữu hạn. Trong Chương 2, đầu tiên chúng tôi tập trung trình bày một số định nghĩa, kết quả ban đầu về tính hoán vị được của đa thức trên một trường hữu hạn. Tiếp theo chúng tôi trình bày lại các kết quả về tính hoán vị được của đa thức một biến với hệ số nguyên trên vành $\mathbb{Z}_{p^n}$, với $p = 2, 3, 5$ trong bài báo của hai tác giả Rajesh P Singh và Soumen Maity, kết quả chính được thể hiện trong các Định lý 2.2.7, Định lý 2.3.3 và Định lý 2.3.8.

Chương 1

Cấu trúc của trường hữu hạn

Mục đích của chương này là trình bày các tính chất cơ bản của trường phân rã và cấu trúc trường hữu hạn. Các kết quả trong Chương này được viết theo các tài liệu [1].

1.1 Đa thức bất khả quy

Trong suốt luận văn này chúng ta luôn xét đa thức với hệ số trên một trường $\mathbb{K}$. Trong trường hợp này, các đa thức hằng khác 0 đều khả nghịch. Do đó ta có thể định nghĩa đa thức bất khả quy như sau.

1.1.1 Định nghĩa. Đa thức $f(x)$ với hệ số trên một trường $\mathbb{K}$ 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.

Tiếp theo, chúng ta định nghĩa khái niệm đa thức bất khả quy của một phần tử đại số trên $\mathbb{K}$. Trước tiên ta nhắc lại một số khái niệm sau.

1.1.2 Định nghĩa. Cho $\mathbb{F}$ là một trường chứa $\mathbb{K}$. Một phần tử $a \in \mathbb{F}$ được gọi là *đại số* trên $\mathbb{K}$ nếu nó là nghiệm của một đa thức khác không với hệ số trên $\mathbb{K}$. Đa thức dạng chuẩn là đa thức có hệ số cao nhất là 1.

Mệnh đề tiếp theo đóng vai trò quan trọng để định nghĩa đa thức bất khả quy của một phần tử đại số.

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

Chứng minh. Vì a là phần tử đại số trên $\mathbb{F}$ nên tồn tại $f(x) \in \mathbb{K}[x]$ 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 $p(x) \in \mathbb{K}[x]$ 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 $\mathbb{K}[x]$ với bậc bé hơn và một trong hai đa thức này phải nhận a làm nghiệm, điều này là mâu thuẫn với cách chọn $p(x)$. Do đó $p(x)$ bất khả quy.

Tiếp theo, giả sử $g(x) \in \mathbb{K}[x]$ nhận a làm nghiệm. Nếu $g(x)$ không chia hết cho $p(x)$ thì vì $p(x)$ bất khả quy nên $\gcd(g(x), p(x)) = 1$. Khi đó, tồn tại $q(x), h(x) \in \mathbb{K}[x]$ 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 $q(x) \in \mathbb{K}[x]$ 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 $k(x) \in \mathbb{K}[x]$. Vì $q(x)$ bất khả quy nên $k(x) = c$ với $0 \neq c \in \mathbb{K}$. 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 $p(x) = q(x)$. □

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

1.1.5 Ví dụ. 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.

1.1.6 Mệnh đề. *Cho $\mathbb{F}$ là một trường chứa $\mathbb{K}$ và $a \in \mathbb{F}$ là phần tử đại số trên $\mathbb{K}$. Giả sử $g(x) \in \mathbb{K}[x]$ thỏa mãn $g(a) \neq 0$. Khi đó tồn tại $f(x) \in \mathbb{K}[x]$ sao cho trong trường $\mathbb{F}$ ta có $(g(a))^{-1} = f(a)$.*

Chứng minh. Theo Mệnh đề 1.1.3, tồn tại $p(x) \in \mathbb{K}[x]$ là đa thức bất khả quy của a. Do $g(a) \neq 0$ và $p(a) = 0$ nên $g(x)$ không chia hết cho $p(x)$. Do $p(x)$ bất khả quy nên $\gcd(p(x), g(x)) = 1$. Khi đó tồn tại các đa thức $f(x), t(x) \in \mathbb{K}[x]$ sao cho $1 = g(x).f(x) + p(x)t(x)$. Suy ra $1 = g(a)f(a)$. Do đó $(g(a))^{-1} = f(a)$. □

1.2 Trường phân rã của đa thức

Mục đích của tiết này là sử dụng tính chất của đa thức bất khả quy để chỉ ra sự tồn tại duy nhất của trường phân rã của một đa thức. Trong suốt tiết này, luôn giả thiết $\mathbb{K}$ là một trường. Nếu $\mathbb{E}$ là một trường chứa $\mathbb{K}$ thì ta viết $\mathbb{K} \subseteq \mathbb{E}$ hay $\mathbb{E}/\mathbb{K}$, khi đó ta gọi $\mathbb{E}/\mathbb{K}$ là một mở rộng trường. Rõ ràng $\mathbb{E}$ có cấu trúc tự nhiên như một $\mathbb{K}$-không gian véc tơ. Chiều của không gian này được gọi là bậc của mở rộng $\mathbb{E}/\mathbb{K}$ và kí hiệu là $[\mathbb{E} : \mathbb{K}]$. Nếu $[\mathbb{E} : \mathbb{K}] < \infty$ thì ta nói $\mathbb{E}/\mathbb{K}$ là mở rộng hữu hạn. Chú ý rằng nếu $\mathbb{E}/\mathbb{K}$ và $\mathbb{T}/\mathbb{E}$ là các mở rộng hữu hạn thì ta có công thức bậc $[\mathbb{T} : \mathbb{K}] = [\mathbb{T} : \mathbb{E}][\mathbb{E} : \mathbb{K}]$. Nếu mỗi phần tử của $\mathbb{E}$ đều đại số trên $\mathbb{K}$ thì ta nói $\mathbb{E}/\mathbb{K}$ là mở rộng đại số.

1.2.1 Chú ý. (i) Giả sử $\mathbb{E}/\mathbb{K}$ là một mở rộng trường. Nếu $\mathbb{E}/\mathbb{K}$ là mở rộng hữu hạn thì nó là mở rộng đại số. Thật vậy, giả sử $\dim_{\mathbb{K}} \mathbb{E} = t$ và $\alpha \in \mathbb{E}$. Vì hệ $\{1, \alpha, \ldots, \alpha^t\}$ gồm $t+1$ phần tử nên nó là hệ phụ thuộc tuyến tính. Do đó tồn tại $\alpha_0, \alpha_1, \ldots, \alpha_t \in \mathbb{K}$ với ít nhất một hệ số $\alpha_i \neq 0$ sao cho $\alpha_0 + \alpha_1\alpha + \cdots + \alpha_t\alpha^t = 0$. Như vậy, $\alpha_0 + \alpha_1 x + \cdots + \alpha_t x^t \in K[x]$ là đa thức khác 0 nhận α là nghiệm, vì thế α đại số trên $\mathbb{K}$.

(ii) Nếu $\mathbb{E}/\mathbb{K}$ là một mở rộng trường và $\alpha_1, \ldots, \alpha_n \in \mathbb{E}$ thì ta kí hiệu $\mathbb{K}(\alpha_1, \ldots, \alpha_n)$ ($\mathbb{K}[\alpha_1, \ldots, \alpha_n]$) là giao của tất cả các trường con (vành con) của $\mathbb{E}$ chứa $\mathbb{K}$ và chứa $\alpha_1, \ldots, \alpha_n$. Ta thấy rằng $\mathbb{K}(\alpha_1, \ldots, \alpha_n)$ là trường con bé nhất và $\mathbb{K}[\alpha_1, \ldots, \alpha_n]$ là vành con bé nhất của $\mathbb{E}$ chứa $\mathbb{K}$ và chứa các phần tử $\alpha_1, \ldots, \alpha_n$. Trường hợp $n = 1$, nếu $g(\alpha) \neq 0$ thì phần tử $(g(\alpha))^{-1} \in \mathbb{E}$ được kí hiệu là $\dfrac{1}{g(\alpha)}$. Khi đó

$$\mathbb{K}[\alpha] = \{g(\alpha) \mid g(x) \in \mathbb{K}[x]\},$$

$$\mathbb{K}(\alpha) = \left\{ \frac{g(\alpha)}{h(\alpha)} \mid g(x), h(x) \in \mathbb{K}[x], h(\alpha) \neq 0 \right\}$$

lần lượt là vành con bé nhất và trường con bé nhất của $\mathbb{E}$ chứa $\mathbb{K}$ và α.

1.2.2 Mệnh đề. *Cho $\mathbb{E}/\mathbb{K}$ là mở rộng trường và $\alpha \in \mathbb{E}$ là phần tử đại số trên $\mathbb{K}$. Giả sử $p(x) \in \mathbb{K}[x]$ là đa thức bất khả quy nhận α làm nghiệm. Khi đó $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$ và $[\mathbb{K}(\alpha) : \mathbb{K}] = \deg p(x)$. Hơn nữa, nếu $\deg p(x) = n$ thì $S = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ là một cơ sở của $\mathbb{K}$-không gian véc tơ $\mathbb{K}(\alpha)$.*

Chứng minh. Do α là đại số trên $\mathbb{K}$ nên theo Mệnh đề 1.1.6, mỗi phần tử khác 0 trong vành $\mathbb{K}[\alpha]$ đều khả nghịch. Suy ra $\mathbb{K}[\alpha]$ là một trường chứa $\mathbb{K}$ và α. Vì thế $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$. Cho $\beta \in \mathbb{K}(\alpha)$. Khi đó $\beta \in \mathbb{K}[\alpha]$. Vì thế $\beta = f(\alpha)$ với $f(x) \in \mathbb{K}[x]$. Theo Định lý chia với dư, tồn tại $q(x), r(x) \in \mathbb{K}[x]$ sao cho

$$f(x) = p(x)q(x) + r(x),$$

trong đó $r(x) = 0$ hoặc $\deg r(x) < \deg p(x)$. Giả sử

$$r(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1}.$$

Vì $p(\alpha) = 0$ nên

$$\beta = f(\alpha) = r(\alpha) = \alpha_0 + \alpha_1 \alpha + \cdots + \alpha_{n-1} \alpha^{n-1}.$$