ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

VƯƠNG THỊ YẾN

ĐA THỨC HOÁN VỊ ĐƯỢC

LUẬN VĂN THẠC SỸ TOÁN HỌC

Chuyên ngành : PHƯƠNG PHÁP TOÁN SƠ CẤP
Mã số : 60 46 40

Giáo viên hướng dẫn:
PGS.TS. LÊ THỊ THANH NHÀN

THÁI NGUYÊN, 2012

Mục lục

Lời cảm ơn

Đề tài được thực hiện tại trường Đại học Khoa học - Đại học Thái Nguyên dưới sự hướng dẫn của PGS.TS Lê Thị Thanh Nhàn. Tôi xin bày tỏ lòng biết ơn sâu sắc, chân thành nhất đối với Cô. Bởi sự giúp đỡ, chỉ bảo, khuyến khích ân cần của Cô đã góp phần rất lớn cho sự thành công của luận văn này.

Tôi cũng xin được bày tỏ lòng cảm ơn chân thành nhất tới Ban lãnh đạo, Phòng Đào tạo - Khoa học và Quan hệ quốc tế, Khoa Toán - Tin Trường Đại học khoa học - Đại học Thái Nguyên đã tạo điều kiện thuận lợi để tôi và các bạn học viên cao học Khóa 4 (2010 - 2012) được học tập, nghiên cứu.

Tôi cũng xin cảm ơn các Thầy, Cô là GS.TSKH Hà Huy Khoái, GS.TSKH Nguyễn Văn Mậu,... là những nhà toán học hàng đầu Việt Nam đã giảng dạy các chuyên đề cho lớp chúng tôi.

Cuối cùng, tôi xin được gửi lời cảm ơn tới gia đình, bạn bè, những người thân đã luôn ở bên, động viên, giúp đỡ để tôi có thể hoàn thành luận văn.

Lời nói đầu

Ta đã biết rằng một đa thức $f(x)$ trên một vành hữu hạn R được gọi là *hoán vị được* nếu đa thức đó *hoán vị được* các phần tử của vành R, tức là ánh xạ $\varphi : R \to R$ cho bởi $\varphi(a) = f(a)$ phải là một song ánh.

Trong cuốn "Finite fields" xuất bản lần đầu tiên năm 1983, Lidl và Niedereiter [LN] đã nghiên cứu các tiêu chuẩn của đa thức hoán vị được, các dạng đặc biệt của đa thức hoán vị được, nhóm các đa thức hoán vị được, trường hợp ngoại lệ của đa thức hoán vị được và đa thức hoán vị được ở một số dạng bất định. Lidl và Mullen [LM1,2] cũng đã nghiên đa thức hoán vị được trên trường hữu hạn. Năm 1986, R. A. Mollin và C. Small [MS] đã đưa ra tiêu chuẩn đa thức hoán vị được dạng x^n. Năm 1999, R. Rivest [Riv] đưa ra tiêu chuẩn đa thức hoán vị được modulo 2^k.

Trong đề tài này chúng tôi trình bày lại các kết quả trong hai bài báo của R.A.Mollin và C.Small [MS] và của R.Rivest [Riv] về đặc trưng tính hoán vị được của đa thức dạng x^n và đa thức dạng $x^k + bx^j + c$ với $(k > j \geqslant 1)$ trên một trường hữu hạn, đồng thời xét tính hoán vị được của đa thức dạng $P(x) = a_0 + a_1x + ... + a_nx^n$ với $n = 2^k$ trên vành $\mathbb{Z}_{2^k}$.

Luận văn gồm 2 chương. Chương 1 trình bày kiến thức chuẩn bị về nhóm, vành, trường và đa thức nhằm phục vụ cho việc chứng minh các kết quả ở chương sau. Trong phần đầu của Chương 2 trình bày khái niệm đa thức hoán vị được và một số ví dụ đơn giản. Phần thứ 2 của Chương 2 giành để chứng minh tiêu chuẩn hoán vị được trên một trường hữu hạn của một số lớp đa thức dạng x^n (Định lý 2.1.7) và đa thức dạng $x^k + bx^j + c$ với $k > j \geqslant 1$ (Định lý 2.2.1). Phần cuối của Chương 2 nhằm trình bày một điều kiện cần và đủ để một đa thức với hệ số nguyên

hoán vị được theo modulo 2^k, tức là hoán vị được trên vành $\mathbb{Z}_{2^k}$ (Định lý 2.3.10).

Chương 1

Kiến thức chuẩn bị

Chương này trình bày khái niệm và những kết quả chuẩn bị về nhóm, vành, trường và đa thức phục vụ cho chứng minh các kết quả của chương sau.

1.1 Kiến thức chuẩn bị về nhóm

1.1.1 Định nghĩa. *Nhóm* là một tập G cùng với một phép toán (kí hiệu theo lối nhân) thoả mãn các điều kiện
(i) Phép toán có tính kết hợp: $a(bc) = (ab)c$, $\forall a, b, c \in G$.
(ii) G có đơn vị: $\exists e \in G$ sao cho $ex = xe = x$, $\forall x \in G$.
(iii) Mọi phần tử của G đều khả nghịch: Với mỗi $x \in G$, tồn tại $x^{-1} \in G$ sao cho $xx^{-1} = x^{-1}x = e$.

Một nhóm G được gọi là *nhóm giao hoán* (hay *nhóm Abel*) nếu phép toán là giao hoán. Nếu G có hữu hạn phần tử thì số phần tử của G được gọi là *cấp của* G. Nếu G có vô hạn phần tử thì ta nói G *có cấp vô hạn.*

Sau đây là một số ví dụ về nhóm: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ là các nhóm giao hoán cấp vô hạn với phép cộng thông thường. Với mỗi số nguyên $m \geqslant 1$, tập

$$\mathbb{Z}_m = \{\overline{a} \mid a \in \mathbb{Z}, \overline{a} = \overline{b} \text{ nếu và chỉ nếu } a - b \text{ chia hết cho } m\}$$

các số nguyên modulo m với phép cộng $\overline{a} + \overline{b} = \overline{a + b}$ là một nhóm giao

hoán cấp m. Tập

$$\mathbb{Z}_m^* = \{\overline{a} \in \mathbb{Z}_m \mid (a, m) = 1\}$$

các số nguyên modulo m nguyên tố cùng nhau với m với phép nhân $\overline{a}\ \overline{b} = \overline{ab}$ là một nhóm giao hoán cấp $\varphi(m)$, trong đó φ là hàm Euler, tức là $\varphi(1) = 1$ và khi $m > 1$ thì $\varphi(m)$ là số các số tự nhiên nhỏ hơn m và nguyên tố cùng nhau với m.

1.1.2 Định nghĩa. Một nhóm G được gọi là *xyclic* nếu tồn tại $a \in G$ sao cho mỗi phần tử của G đều là một luỹ thừa của a. Trong trường hợp này ta viết $G = (a)$ và ta gọi G là nhóm xyclic *sinh bởi* a. Phần tử a được gọi là một *phần tử sinh* của G.

1.1.3 Bổ đề. *Nhóm con của nhóm xyclic là xyclic.*

Chứng minh. Giả sử $G = (a)$ là nhóm xyclic. Cho H là nhóm con của G. Nếu $H = \{e\}$ thì H là nhóm xyclic sinh bởi e. Giả sử $H \neq \{e\}$. Chọn $e \neq x \in H$. Viết $x = a^k$. Do $x \neq e$ nên $k \neq 0$. Vì H là nhóm con nên $a^{-k} \in H$. Trong hai số k và $-k$ ắt phải có một số nguyên dương. Vì thế H chứa những lũy thừa nguyên dương của a. Gọi r là số nguyên dương bé nhất sao cho $a^r \in H$. Rõ ràng $H \supseteq (a^r)$. Cho $y \in H$. Viết $y = a^t$ với $t = rq + s$, trong đó $0 \leqslant s < r$. Ta có $y = a^t = (a^r)^q a^s$. Do đó $a^s = y(a^r)^{-q} \in H$. Từ cách chọn của r ta suy ra $s = 0$. Do đó $y = a^t = (a^r)^q \in (a^r)$. Vậy $H = (a^r)$ là nhóm xyclic. □

1.1.4 Định nghĩa. Tập con H của một nhóm G được gọi là *nhóm con* của G nếu $e \in H$, $a^{-1} \in H$ và $ab \in H$ với mọi $a, b \in H$.

Cho G là một nhóm. Khi đó $\{e\}$ là nhóm con bé nhất của G và G là nhóm con lớn nhất của G. Cho $a \in G$. Đặt $(a) = \{a^n \mid n \in \mathbb{Z}\}$. Khi đó (a) là nhóm con của G, được gọi là *nhóm con xyclic sinh bởi* a. Cấp của nhóm con (a) được gọi là *cấp của phần tử* a.

1.1.5 Bổ đề. *Cho G là một nhóm và a là một phần tử của G. Các phát biểu sau là tương đương*

(i) a có cấp n.

(ii) n là số nguyên dương bé nhất sao cho $a^n = e$.

(iii) $a^n = e$ và nếu $a^k = e$ thì k là bội của n với mọi $k \in \mathbb{Z}$.

Chứng minh. (i)⇒(ii). Trước hết ta khẳng định tồn tại một số nguyên dương k sao cho $a^k = e$. Giả sử ngược lại, với mọi cặp số tự nhiên $k < k'$ ta có $a^{k'-k} \neq e$. Suy ra $a^k \neq a^{k'}$. Điều này chứng tỏ (a) có cấp vô hạn, vô lí với giả thiết (i). Do đó, tồn tại những số nguyên dương k sao cho $a^k = e$. Gọi r là số nguyên dương bé nhất có tính chất $a^r = e$. Ta thấy rằng các phần tử $e, a, a^2, \ldots, a^{r-1}$ là đôi một khác nhau. Thật vậy, nếu $a^i = a^j$ với $0 \leqslant i \leqslant j < r$ thì $a^{j-i} = e$ và $0 \leqslant j - i < r$, do đó theo cách chọn của r ta có $i = j$. Bây giờ ta chứng minh $G = \{e, a, a^2, \ldots, a^{r-1}\}$. Rõ ràng $G \supseteq \{e, a, a^2, \ldots, a^{r-1}\}$. Cho $b \in G$. Khi đó $b = a^k$ với $k \in \mathbb{Z}$. Viết $k = rq + s$ trong đó $q, s \in \mathbb{Z}$ và $0 \leqslant s \leqslant r - 1$. Ta có

$$b = a^k = a^{rq+s} = (a^r)^q a^s = a^s \in \{e, a, a^2, \ldots, a^{r-1}\}.$$

Vì thế $G = \{e, a, a^2, \ldots, a^{r-1}\}$ là nhóm cấp r. Suy ra $r = n$ và (ii) được chứng minh.

(ii)⇒(iii). Giả sử $a^k = e$. Viết $k = nq + r$ với $0 \leqslant r < n$. Vì $a^n = e$ nên $e = a^k = a^{nq}a^r = a^r$. Theo cách chọn n ta phải có $r = 0$, suy ra k chia hết cho n.

(iii)⇒(i). Gọi r là số nguyên dương bé nhất sao cho $a^r = e$. Theo (iii), r là bội của n. Do đó n là số nguyên dương bé nhất thỏa mãn $a^n = e$. Tương tự như chứng minh (i)→(ii) ta suy ra cấp của a là n. □

1.1.6 Hệ quả. *Cho $G = (a)$ là nhóm xyclic cấp n. Khi đó phần tử $b = a^k$ là phần tử sinh của G nếu và chỉ nếu $(k, n) = 1$.*

Chứng minh. Giả sử $b = a^k$ là phần tử sinh của G. Khi đó b có cấp n. Đặt $d = (k, n)$. Ta có $b^{n/d} = (a^n)^{k/d} = e$. Theo Bổ đề 1.1.5, n/d là bội của n. Vì thế $d = 1$.

Ngược lại, giả sử $(k, n) = 1$. Ta có $b^n = (a^n)^k = e$. Giả sử $b^t = e$. Khi đó $a^{kt} = e$. Theo Bổ đề 1.1.5, kt là bội của n. Do $(k, n) = 1$ nên t là bội của n. Theo Bổ đề 1.1.5, b có cấp n. Vậy $G = (b)$. □

1.1.7 Định nghĩa. Cho G là nhóm và H là nhóm con của G. Với mỗi $a \in G$, kí hiệu $Ha = \{ha \mid h \in H\}$. Ta gọi Ha là một *lớp ghép trái* hay *lớp kề trái* của H trong G ứng với phần tử a. Tập các lớp ghép trái của H trong G được kí hiệu là G/H. Khi H chỉ có hữu hạn lớp ghép trái thì số các lớp ghép trái của H được gọi là *chỉ số của H trong G* và được kí hiệu là $(G : H)$. Trong trường hợp này, chỉ số của H chính là số phần tử của G/H. Đặc biệt, cấp của G chính là $(G : e)$, chỉ số của nhóm con tầm thường $\{e\}$.

Với H là nhóm con của nhóm G và $a, b \in G$, ta dễ dàng kiểm tra được $Ha = Hb$ nếu và chỉ nếu $ab^{-1} \in H$.

1.1.8 Định lý. *(***Lagrange***). Trong một nhóm hữu hạn, cấp và chỉ số của một nhóm con là ước của cấp của toàn nhóm.*

Chứng minh. Giả sử G là nhóm có cấp n và H là nhóm con của G có cấp m. Với mỗi $a \in G$ ta có $a = ea \in Ha$. Vì thế, mỗi phần tử của G đều thuộc một lớp ghép trái của H. Giả sử $Ha \cap Hb \neq \varnothing$. Khi đó tồn tại $h, h' \in H$ sao cho $ha = h'b$. Suy ra $a = h^{-1}h'b$. Cho $xa \in Ha$, trong đó $x \in H$. Khi đó $xa = (xh^{-1}h')b \in Hb$. Suy ra $Ha \subseteq Hb$. Tương tự, $Hb \subseteq Ha$ và do đó $Ha = Hb$. Vậy hai lớp ghép trái bất kì của H nếu khác nhau thì phải rời nhau. Với mỗi $a \in G$, rõ ràng ánh xạ $f : H \longrightarrow Ha$ xác định bởi $f(h) = ha$ là một song ánh. Vì thế mỗi lớp ghép trái của H đều có đúng m phần tử. Gọi chỉ số của H là s. Từ các lập luận trên ta suy ra $n = sm$. Vì thế s và m đều là ước của n. □

1.1.9 Hệ quả. *Cho G là nhóm cấp n và $a \in G$. Khi đó cấp của a là ước của n. Hơn nữa, $a^n = e$.*

Chứng minh. Gọi cấp của a là r. Khi đó nhóm con xyclic (a) có cấp r. Theo Định lí Lagrange, r là ước của n. Theo Bổ đề 1.1.5 ta có $a^r = e$. Suy ra $a^n = e$. □

1.1.10 Hệ quả. *Mọi nhóm cấp nguyên tố đều là nhóm xyclic.*

Chứng minh. Giả sử G là nhóm cấp p nguyên tố. Lấy $a \in G$, $a \neq e$. Theo Định lí Lagrange, a có cấp là ước của p. Vì p nguyên tố nên cấp của a là 1 hoặc là p. Do $a \neq e$ nên cấp của a lớn hơn 1. Vậy cấp của a là p, tức G là nhóm xyclic sinh bởi a. □

1.2 Kiến thức chuẩn bị về vành

1.2.1 Định nghĩa. *Vành* là một tập V được trang bị hai phép toán cộng và nhân thỏa mãn các điều kiện sau đây:
(i) *V là một nhóm giao hoán với phép cộng*;
(ii) *V là một vị nhóm với phép nhân*: Phép nhân có tính chất kết hợp và tồn tại phần tử $1 \in V$ (gọi là phần tử đơn vị) sao cho $1x = x1 = x$ với mọi $x \in V$;
(iii)*Phép nhân phân phối đối với phép cộng.*

Nếu phép nhân là giao hoán thì V được gọi là *vành giao hoán*. Sau đây là một số ví dụ thường gặp về vành:

1.2.2 Ví dụ. a) Rõ ràng $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ là những vành giao hoán với phép cộng và nhân thông thường;

b) Với mỗi số tự nhiên $n > 0$, tập $\mathbb{Z}_n$ các số nguyên modulo n làm thành một vành giao hoán với phép cộng và phép nhân cho bởi: $\overline{a} + \overline{b} = \overline{a+b}$ và $\overline{a}\ \overline{b} = \overline{ab}$ với mọi $\overline{a}, \overline{b} \in \mathbb{Z}_n$.