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

Mục lục 2

Lời cảm ơn **3**

Lời nói đầu **4**

1 Kiến thức chuẩn bị **6**

1.1 Kiến thức chuẩn bị về nhóm 6

1.2 Kiến thức chuẩn bị về vành 10

1.3 Kiến thức chuẩn bị về trường 14

1.4 Kiến thức chuẩn bị về đa thức 17

2 Đa thức hoán vị được **20**

2.1 Khái niệm đa thức hoán vị được 20

2.2 Một số lớp đa thức hoán vị được trên một trường 26

2.3 Đa thức hoán vị được modulo 2^k 30

Kết luận 39

Tài liệu tham khảo 40

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 $\overline{a}, \overline{b} \in \mathbb{Z}_n$.

c) Cho R là một vành. Kí hiệu

$$R[x] = \{a_0 + a_1x + \ldots + a_nx^n \mid n \in \mathbb{N}, a_i \in R, \forall i\}$$

là tập các đa thức một biến x với hệ số trong R. Khi đó $R[x]$ là một vành giao hoán với phép cộng và nhân các đa thức: $\sum a_ix^i + \sum b_ix^i = \sum(a_i + b_i)x^i$ và $\sum a_ix^i \ \sum b_ix^i = \sum c_kx^k$ với $c_k = \sum_{i+j=k} a_ib_j$. Ta gọi $R[x]$ là *vành đa thức một biến x trên R*. Rõ ràng R giao hoán nếu và chỉ nếu $R[x]$ là giao hoán.

1.2.3 Định nghĩa. Cho V là một vành. Một tập con S của V được gọi là *vành con* của V nếu $-1 \in S$ và $x + y, xy \in S$ với mọi $x, y \in S$.

Dễ thấy rằng tập con S của vành V là vành con của V nếu và chỉ nếu phép cộng và phép nhân đóng kín trong S và S làm thành một vành cùng với hai phép toán này.

1.2.4 Định nghĩa. Cho V là vành và I là tập con của V. Ta nói rằng I là *iđêan* của V nếu I là nhóm con của nhóm cộng V và $xa, ax \in I$ với mọi $a \in I, x \in V$.

Cho V là một vành. Dễ thấy rằng $\{0\}$ là iđêan bé nhất của V và V là iđêan lớn nhất của V. Idêan $\{0\}$ được kí hiệu là 0. Các iđêan của V khác V được gọi là các iđêan *thực sự*.

1.2.5 Định nghĩa. Cho V là vành và I là iđêan của V. Xét tập $V/I = \{x + I \mid x \in V\}$ - tập các lớp ghép của V theo nhóm con I. Rõ ràng hai phần tử $x + I, y + I \in V/I$ là bằng nhau nếu và chỉ nếu $x - y \in I$. Trong tập V/I, ta định nghĩa quy tắc cộng $(x+I)+(y+I) = (x+y)+I$ và quy tắc nhân $(x + I)(y + I) = xy + I$. Ta có thể kiểm tra rằng quy tắc cộng và nhân ở trên không phụ thuộc vào việc chọn đại diện của các phần tử, tức là nếu $x' + I = x + I$ và $y' + I = y + I$ thì $x + y + I = x' + y' + I$ và $xy + I = x'y' + I$. Vì thế các quy tắc cộng và nhân này là hai phép

toán trên V/I. Hơn nữa, tập V/I cùng với phép cộng và nhân xác định như trên là một vành giao hoán, có đơn vị là $1 + I$ và phần tử không là $0 + I$. Vành V/I vừa xây dựng ở trên được gọi là *vành thương của V theo iđêan I*.

Chú ý rằng vành thương của vành $\mathbb{Z}$ theo iđêan $m\mathbb{Z}$ chính là vành $\mathbb{Z}_m$ các số nguyên modulo m.

1.2.6 Định nghĩa. Một *đồng cấu vành* là một ánh xạ f từ vành V đến vành S sao cho

(i) $f(a + a') = f(a) + f(a')$ với mọi $a, a' \in V$.

(ii) $f(aa') = f(a)f(a')$ với mọi $a, a' \in V$.

(iii) $f(1) = 1$.

Đồng cấu f được gọi là *đơn cấu* (*toàn cấu, đẳng cấu*) nếu f là đơn ánh (toàn ánh, song ánh). Vành V được gọi là *đẳng cấu* với vành S nếu tồn tại một đẳng cấu giữa chúng. Một đồng cấu (đơn cấu, toàn cấu, đẳng cấu) từ vành S đến S được gọi là một *tự đồng cấu (tự đơn cấu, tự toàn cấu, tự đẳng cấu).*

Mệnh đề sau đây cho ta tính chất của vành con và iđêan khi tác động qua một đồng cấu vành.

1.2.7 Mệnh đề. *Cho $f : V \longrightarrow S$ là đồng cấu vành, B là vành con của V và J là iđêan của S. Các phát biểu sau là đúng.*

(i) $f(B)$ là vành con của S.

(ii) $f^{-1}(J)$ là iđêan của V.

Chứng minh. (i). Cho $s, r \in f(B)$. Khi đó $s = f(b)$ và $r = f(c)$ với $b, c \in B$. Vì $b + c, bc \in B$ nên $s + r = f(b) + f(c) = f(b + c) \in f(B)$ và $sr = f(b)f(c) = f(bc) \in f(B)$. Vì $-1 \in B$ nên

$$-1 = -f(1) = f(-1) \in f(B).$$

Vậy $f(B)$ là vành con của S.
(ii). Do $f(0) = 0 \in J$ nên $0 \in f^{-1}(J)$. Cho $a, b \in f^{-1}(J)$. Khi đó $f(a), f(b) \in J$. Suy ra $f(a-b) = f(a) - f(b) \in J$. Do đó ta có $a - b \in f^{-1}(J)$. Vì thế $f^{-1}(J)$ là nhóm con của nhóm cộng V. Cuối cùng, cho $a \in f^{-1}(J)$ và $x \in V$. Khi đó $f(a) \in J$. Suy ra $f(ax) = f(a)f(x) \in J$, tức là $ax \in f^{-1}(J)$. Tương tự, $xa \in f^{-1}(J)$. Vậy $f^{-1}(J)$ là iđêan của V. □

1.2.8 Định nghĩa. Cho $f : V \longrightarrow S$ là một đồng cấu vành. Vì V là vành con của V nên $f(V)$ là vành con của S. Vành con $f(V)$ được gọi là *ảnh* của f và được kí hiệu bởi Im f. Đặt $\operatorname{Ker} f = \{a \in V \mid f(a) = 0\}$. Khi đó $\operatorname{Ker} f = f^{-1}(0)$. Vì 0 là iđêan của S nên theo Mệnh đề 1.2.7, $\operatorname{Ker} f$ là iđêan của V. Ta gọi $\operatorname{Ker} f$ là *hạt nhân của* f.

1.2.9 Mệnh đề. *Cho $f : V \longrightarrow S$ là đồng cấu vành. Khi đó f là đơn cấu nếu và chỉ nếu* $\operatorname{Ker} f = 0$. *Trong trường hợp này, V đẳng cấu với vành con Im f của S.*

Chứng minh. Giả sử f là đơn cấu. Rõ ràng $0 \in \operatorname{Ker} f$. Cho $a \in \operatorname{Ker} f$. Khi đó $f(a) = 0 = f(0)$. Suy ra $a = 0$. Vì thế $\operatorname{Ker} f = 0$. Giả sử $\operatorname{Ker} f = 0$. Cho $a, b \in V$ sao cho $f(a) = f(b)$. Khi đó $f(a-b) = 0$. Suy ra $a - b \in \operatorname{Ker} f = 0$. Vì thế $a - b = 0$ hay $a = b$. Vậy f là đơn cấu. □

1.2.10 Định lý. *(Định lí đồng cấu vành). Cho $f : V \longrightarrow S$ là đồng cấu vành. Khi đó* $V/\operatorname{Ker} f \cong$ *Im f.*

1.2.11 Định nghĩa. Cho V là vành. Giả sử tồn tại số nguyên $n \neq 0$ sao cho $n1 = 0$. Khi đó $(-n)1 = 0$. Trong hai số n và $-n$ ắt phải có một số nguyên dương. Trong trường hợp này, ta gọi *đặc số của V* là số nguyên dương n nhỏ nhất sao cho $n1 = 0$. Nếu $n1 = 0$ chỉ xảy ra khi $n = 0$ thì ta nói V *có đặc số* 0.

Dễ thấy rằng vành $\mathbb{Z}$ các số nguyên, vành $\mathbb{Q}$ các số hữu tỷ, vành $\mathbb{R}$ các số thực, vành $\mathbb{C}$ các số phức đều có đặc số 0. Vành $\mathbb{Z}_m$ các số nguyên modulo m có đặc số m.

1.2.12 Mệnh đề. *Cho V là một vành. Các phát biểu sau là đúng.*
(i) Nếu V có đặc số 0 thì V chứa một vành con đẳng cấu với vành $\mathbb{Z}$.
(ii) Nếu V có đặc số m thì V chứa một vành con đẳng cấu với $\mathbb{Z}_m$.

Chứng minh. Xét ánh xạ $f : \mathbb{Z} \longrightarrow V$ xác định bởi $f(n) = n1$ với mọi $n \in \mathbb{Z}$. Dễ thấy rằng f là đồng cấu vành. Giả sử V có đặc số 0. Khi đó $f(n) = 0$ khi và chỉ khi $n = 0$. Vì thế f là đơn cấu. Do đó $\mathbb{Z} \cong \text{Im } f$. Vì thế Im f là vành con của V đẳng cấu với $\mathbb{Z}$. Giả sử V có đặc số m. Khi đó $\text{Ker } f = m\mathbb{Z}$. Theo Định lí 1.2.10, $\mathbb{Z}/m\mathbb{Z} \cong \text{Im } f$. Vì thế Im f là vành con của V đẳng cấu với $\mathbb{Z}_m$. □

1.3 Kiến thức chuẩn bị về trường

1.3.1 Định nghĩa. Một phần tử a của vành giao hoán R được gọi là *khả nghịch* nếu tồn tại $b \in R$ sao cho $ab = 1$. *Trường* là một vành giao hoán, khác 0 và mọi phần tử khác 0 đều khả nghịch.

Chú ý rằng vành $\mathbb{Z}_6$ không là trường vì $\overline{2} \in \mathbb{Z}_6$ không khả nghịch. Vành $\mathbb{Z}$ không là trường vì $2 \in \mathbb{Z}$ không khả nghịch. Các vành $\mathbb{Q}$, $\mathbb{R}$ và $\mathbb{C}$ đều là trường.

1.3.2 Bổ đề. *Đặc số của trường là 0 hoặc là số nguyên tố.*

Chứng minh. Giả sử T là trường có đặc số $n \neq 0$. Vì $1 \neq 0$ nên $n > 1$. Nếu n không nguyên tố thì $n = ab$ với $1 < a, b < n$. Vì n là số nguyên dương bé nhất thoả mãn $n1 = 0$ nên $a1, b1 \neq 0$. Do đó tồn tại các phần tử $x, y \in T$ sao cho $x(a1) = 1 = y(b1)$. Vì thế ta có

$$0 = (n1)xy = x(a1)y(b1) = 1.1 = 1.$$

Điều này là vô lí. □

1.3.3 Bổ đề. *Vành $\mathbb{Z}_n$ là trường khi và chỉ khi n là số nguyên tố.*

Chứng minh. Cho $\mathbb{Z}_n$ là trường. Vì $\mathbb{Z}_n$ có đặc số n nên theo Bổ đề 1.3.2, n là số nguyên tố. Cho n là số nguyên tố. Khi đó $n > 1$. Vì thế $\mathbb{Z}_n \neq 0$. Cho $\overline{0} \neq \overline{a} \in \mathbb{Z}_n$. Khi đó a không là bội của n. Vì n nguyên tố nên a và n nguyên tố cùng nhau, tức là tồn tại $x, y \in \mathbb{Z}$ sao cho $1 = ax + ny$. Suy ra $\overline{1} = \overline{a}\ \overline{x}$, tức là $\overline{a}$ khả nghịch. Vậy $\mathbb{Z}_n$ là trường. □

1.3.4 Định nghĩa. Một tập con A của trường T được gọi là một *trường con* nếu phép cộng và nhân là đóng kín trong A và A làm thành một trường cùng với hai phép toán này.

Giả sử T là một trường có đặc số $m > 0$. Theo Bổ đề 1.3.2, m phải là số nguyên tố. Theo Mệnh đề 1.2.12, T chứa một trường con đẳng cấu với trường $\mathbb{Z}_m$.

Trong phần cuối của mục này, chúng ta nghiên cứu số phần tử của một trường hữu hạn. Trước hết ta cần nhắc lại một số khái niệm và tính chất của không gian véc tơ.

1.3.5 Định nghĩa. Cho K là một trường. Một tập V có trang bị một phép cộng và một ánh xạ $K \times V \longrightarrow V$ (gọi là phép nhân với vô hướng) được gọi là *một không gian véc tơ* trên trường K hay một K-không gian vec tơ nếu $(V, +)$ là một nhóm giao hoán và tích vô hướng thoả mãn các tính chất sau đây: với mọi $x, y \in K$ và mọi $\alpha, \beta \in V$ ta có

(i) Phân phối: $(x + y).\alpha = x.\alpha + y.\alpha$ và $x.(\alpha + \beta) = x.\alpha + x.\beta$;

(ii) Kết hợp: $x(y\alpha) = (x.y).\alpha$;

(iii) Unita: $1\alpha = \alpha$.

1.3.6 Định nghĩa. Giả sử V là một K-không gian véc tơ.

(i) Một hệ véc tơ $\{v_i\}_{i \in I}$ trong V được gọi là một *hệ sinh* của V nếu mọi phần tử $x \in V$ đều có thể biểu thị tuyến tính theo hệ đó, tức là

tồn tại hữu hạn phần tử $v_{i1}, \ldots, v_{ik}$ của hệ $\{v_i\}_{i\in I}$ và hữu hạn phần tử $a_{i1}, \ldots, a_{ik}$ của K sao cho $x = \sum_{j=1}^{k} a_{ij}v_{ij}$. Nếu V có một hệ sinh gồm hữu hạn phần tử thì V được gọi là *K-không gian hữu hạn sinh.*

(ii) Một hệ véc tơ $\{v_i\}_{i\in I}$ trong V được gọi là một *hệ độc lập tuyến tính* nếu từ mỗi ràng buộc tuyến tính của hệ $\sum_{j=1}^{k} a_{ij}v_{ij} = 0$ ta đều có $a_{ij} = 0$ với mọi $j = 1, \ldots, k$.

(iii) Một hệ véc tơ trong V được gọi là một *cơ sở* của V nếu nó là một hệ sinh và độc lập tuyến tính.

Chú ý rằng một hệ véc tơ của V là một cơ sở của V nếu và chỉ nếu mỗi véc tơ của V đều có thể biểu thị tuyến tính một cách duy nhất qua hệ đó. Ta có thể chỉ ra rằng mỗi K-không gian véc tơ $V \neq 0$ đều có ít nhất một cơ sở và các cơ sở của V đều có cùng lực lượng. Lực lượng chung này được gọi là *số chiều* của V và kí hiệu là $\dim_K V$. Đặc biệt, nếu V có một cơ sở gồm n phần tử thì các cơ sở khác của V cũng có n phần tử và ta có $\dim_K V = n$.

1.3.7 Mệnh đề. *Cho T là trường hữu hạn có n phần tử. Khi đó T có đặc số p nguyên tố và n là lũy thừa nào đó của p.*

Chứng minh. Theo Bổ đề 1.3.2, đặc số của T là 0 hoặc là số nguyên tố. Nếu T có đặc số 0 thì theo Mệnh đề 1.2.12, T chứa một vành con đẳng cấu với $\mathbb{Z}$, do đó T có vô hạn phần tử, vô lí. Vì thế T có đặc số $p > 0$. Theo Bổ đề 1.3.2, p là số nguyên tố. Theo Mệnh đề 1.2.12, T chứa một vành con đẳng cấu với $\mathbb{Z}_p$. Chú ý rằng $\mathbb{Z}_p$ là trường theo Bổ đề 1.3.3. Vì thế ta dễ dàng kiểm tra rằng T có cấu trúc tự nhiên là một không gian véc tơ trên trường $\mathbb{Z}_p$. Do T có hữu hạn phần tử nên không gian này có chiều hữu hạn. Giả sử $\dim_{\mathbb{Z}_p} T = k$. Khi đó số phần tử của T là $n = p^k$. □

1.4 Kiến thức chuẩn bị về đa thức

Trong mục này ta giả thiết K là một trường. Nhắc lại rằng một *đa thức* một biến x với hệ số trong K là một biểu thức dạng $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ trong đó $a_i \in K$. Nếu $a_n \neq 0$ thì a_n được gọi là *hệ số cao nhất* của $f(x)$ và số tự nhiên n được gọi là *bậc* của $f(x)$. Ta kí hiệu bậc của $f(x)$ là $\deg f(x)$. Kí hiệu $K[x]$ là tập các đa thức một biến x với hệ số trong K. Giả sử $f(x) = \sum a_i x^i$ và $g(x) = \sum b_i x^i$, ta định nghĩa $f(x) + g(x) = \sum (a_i + b_i)x^i$ và $f(x)g(x) = \sum c_k x^k$, trong đó $c_k = \sum_{i+j=k} a_i b_j$. Khi đó $K[x]$ là một vành, gọi là vành đa thức một biến x với hệ số trong K.

1.4.1 Chú ý. Với $f(x), g(x) \in K[x]$ ta luôn có

$$\deg(f(x) + g(x)) \leqslant \max\{\deg f(x), \deg g(x)\}$$
$$\deg(f(x).g(x)) = \deg f(x) + \deg g(x).$$

Tiếp theo là định lí phép chia với dư cho đa thức một biến.

1.4.2 Định lý. *Cho $f(x), g(x) \in K[x]$ với $g(x) \neq 0$. Khi đó tồn tại duy nhất một cặp đa thức $q(x), r(x) \in K[x]$ sao cho*

$$f(x) = g(x)q(x) + r(x), \text{ với } r(x) = 0 \text{ hoặc } \deg r(x) < \deg g(x).$$

Chứng minh. Chứng minh tính duy nhất. Giả sử

$$f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x),$$

trong đó $r(x), r_1(x)$ bằng 0 hoặc có bậc nhỏ hơn bậc của $g(x)$. Khi đó

$$g(x)(q(x) - q_1(x)) = r_1(x) - r(x).$$

Nếu $r_1(x) = r(x)$ thì $g(x)(q(x) - q_1(x)) = 0$. Vì $g(x) \neq 0$ và K là trường nên $q(x) - q_1(x) = 0$, tức là $q(x) = q_1(x)$. Nếu $r(x) \neq r_1(x)$ thì

$$\deg(r - r_1) = \deg\big(g(q - q_1)\big) = \deg g + \deg(q - q_1).$$

Chú ý rằng

$$\deg(r - r_1) \leqslant \max\{\deg r, \deg r_1\} < \deg g \leqslant \deg g + \deg(q - q_1).$$

Điều này mâu thuẫn với đẳng thức trên.

Ta chứng minh sự tồn tại của $q(x)$ và $r(x)$. Nếu $\deg f(x) < \deg g(x)$ thì ta chọn $q(x) = 0$ và $r(x) = f(x)$. Giả sử $\deg f(x) \geqslant \deg g(x)$. Cho $f(x) = a_m x^m + \ldots + a_0$ và $g(x) = b_n x^n + \ldots + b_0$ với $a_m, b_n \neq 0$ và $n \leqslant m$. Chọn $h(x) = \dfrac{a_m}{b_n} x^{m-n}$. Đặt $f_1(x) = f(x) - g(x)h(x)$. Khi đó $f_1(x) = 0$ hoặc $f_1(x)$ có bậc thực sự bé hơn bậc của $f(x)$. Trong trường hợp $f_1(x) = 0$, ta tìm được dư của phép chia $f(x)$ cho $g(x)$ là $r(x) = 0$ và thương là $q(x) = h(x)$. Nếu $f_1(x) \neq 0$ thì ta tiếp tục làm tương tự với $f_1(x)$ và ta được đa thức $f_2(x)$. Cứ tiếp tục quá trình trên ta được dãy đa thức $f_1(x), f_2(x), \ldots$, nếu chúng đều khác 0 thì chúng có bậc giảm dần. Vì thế sau hữu hạn bước ta được một đa thức có bậc bé hơn bậc của $g(x)$ và đó chính là đa thức dư $r(x)$. Nếu một đa thức của dãy bằng 0 thì dư $r(x) = 0$. Cụ thể, ta có

$$\begin{aligned}
f_1(x) &= f(x) - g(x)h(x) \\
f_2(x) &= f_1(x) - g(x)h_1(x) \\
&\cdots\cdots\cdots \\
f_k(x) &= f_{k-1}(x) - g(x)h_{k-1}(x)
\end{aligned}$$

với $f_k(x) = 0$ hoặc $\deg f_k(x) < \deg g(x)$. Cộng vế với vế các đẳng thức đó lại, ta được

$$f(x) = g(x)(h(x) + h_1(x) + ... + h_{k-1}(x)) + f_k(x).$$

Từ đó ta có $q(x) = h(x) + h_1(x) + \ldots + h_{k-1}(x)$ và $r(x) = f_k(x)$. □

Trong định lý trên, nếu $r(x) \neq 0$ thì $q(x)$ được gọi là *thương hụt* và $r(x)$ được gọi là *dư* của phép chia $f(x)$ cho $g(x)$. Nếu $r(x) = 0$ thì ta nói rằng $f(x)$ *chia hết cho* $g(x)$ hay $g(x)$ là *ước* của $f(x)$.

1.4.3 Hệ quả. *Cho K là một trường và $a \in K$. Khi đó dư của phép chia $f(x) \in K[x]$ cho $x - a$ là $f(a)$.*

Chứng minh. Chia $f(x)$ cho $x - a$, dư hoặc bằng 0 hoặc là một đa thức bậc 0 vì bậc của $(x - a)$ bằng 1. Vì vậy, dư là một phần tử $r \in K$. Ta có $f(x) = (x-a)q(x)+r$. Thay $x = a$ vào đẳng thức ta được $r = f(a)$. □

Một phần tử $a \in K$ được gọi là *nghiệm* của $f(x) \in K[x]$ nếu $f(a) = 0$. Từ Hệ quả 1.4.3 ta có ngay kết quả sau.

1.4.4 Hệ quả. *Cho K là một trường và $a \in K$. Khi đó a 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 $f(x) = (x - a)g(x)$.*

Từ Hệ quả 1.4.4 ta có ngay kết quả sau.

1.4.5 Hệ quả. *Cho $f(x) \in K[x]$ là đa thức khác 0 và $a_1, a_2, \ldots, a_r \in K$ là các nghiệm phân biệt của $f(x)$. Khi đó* $\deg f(x) \geqslant r$.

Chương 2

Đa thức hoán vị được

2.1 Khái niệm đa thức hoán vị được

2.1.1 Định nghĩa. (i) Cho R là một vành giao hoán có hữu hạn phần tử. Cho $f(x) \in R[x]$. Ta nói rằng $f(x)$ là *đa thức hoán vị được* trên R nếu ánh xạ $\varphi : R \to R$ cho bởi $\varphi(a) = f(a)$ là một song ánh.

(ii) Giả sử $f(x)$ là đa thức với hệ số nguyên. Với n là một số nguyên dương cho trước, xét $f(x)$ như đa thức trong $\mathbb{Z}_n[x]$. Ta nói $f(x)$ là *hoán vị được modulo* n nếu nó là đa thức hoán vị được trên $\mathbb{Z}_n$.

Dưới đây là một số ví dụ về đa thức hoán vị được.

2.1.2 Ví dụ. Xét $R = \mathbb{Z}_2$ - trường các số nguyên modulo 2. Cho $f(x) = 1 + 5x + 2x^2 + 3x^3$ và $g(x) = 1 + x + 4x^2$. Trong $\mathbb{Z}_2[x]$, đa thức $f(x)$ có dạng $f(x) = 1 + x + x^3$ và đa thức $g(x)$ có dạng $g(x) = 1 + x$. Ta có $f(0) = 1$ và $f(1) = 1$. Vì thế ánh xạ $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_2$ cho bởi $\varphi(a) = f(a)$ không phải là song ánh. Ta có $g(0) = 1$ và $g(1) = 0$. Vì thế ánh xạ $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_2$ cho bởi $\varphi(a) = g(a)$ là một song ánh. Do đó $f(x)$ là đa thức không hoán vị được modulo 2 và $g(x)$ là đa thức hoán vị được modulo 2.

2.1.3 Ví dụ. Xét $R = \mathbb{Z}_4$ - vành các số nguyên modulo 4. Cho $f(x) = 2 + 3x + 2x^2$ và $g(x) = 3 + 2x + x^2$. Ta có $f(0) = 2, f(1) = 3, f(2) = 0$ và $f(3) = 1$. Vì thế ánh xạ $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_4$ cho bởi $\varphi(a) = f(a)$ là song

ánh. Ta có $g(0) = 3, g(1) = 2, g(2) = 3$ và $g(3) = 2$. Vì thế ánh xạ $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_4$ cho bởi $\varphi(a) = g(a)$ không là một song ánh. Do đó $f(x)$ là đa thức hoán vị được modulo 4 và $g(x)$ là đa thức không hoán vị được modulo 4.

Một bài toán rất tự nhiên đặt ra là: Cho trước đa thức $f(x) = a_0 + a_1x + \ldots + a_nx^n$. Với điều kiện nào của các hệ số $a_0, \ldots, a_n$, đa thức $f(x)$ là hoán vị được. Vì những ứng dụng của đa thức hoán vị được, có rất nhiều người quan tâm đến bài toán này. Tuy nhiên, cho đến nay, bài toán này mới chỉ được giải quyết cho một số trường hợp đặc biệt. Bài toán tổng quát vẫn đang là một vấn đề mở thách thức các nhà toán học trên thế giới.

Phần còn lại của mục này là trình bày tính hoán vị được cho các đa thức bậc không quá 2 và đa thức dạng x^n. Trước hết chúng ta đưa ra tiêu chuẩn hoán vị được của các đa thức bậc không quá 1.

2.1.4 Mệnh đề. *Các phát biểu sau là đúng.*

(i) Trên một vành nhiều hơn 1 *phần tử, mọi đa thức bậc không đều không hoán vị được.*

(ii) Trên một trường T hữu hạn, mọi đa thức bậc nhất là hoán vị được.

Chứng minh. (i) Giả sử $f(x) = a$ là đa thức bậc 0 trên vành R có nhiều hơn 1 phần tử. Khi đó $f(b) = a$ với mọi $b \in R$. Do đó ánh xạ $\varphi : R \longrightarrow R$ xác định bởi $\varphi(b) = f(b)$ không là toàn ánh. Vì thế $f(x)$ không hoán vị được.

(ii) Giả sử $f(x) = a + bx \in T[x]$ là đa thức bậc nhất. Khi đó $b \neq 0$. Vì T là trường nên tồn tại phần tử $b^{-1} \in T$ là nghịch đảo của b. Do đó với mỗi $c \in T$, phương trình $a + bx = c$ luôn có nghiệm là $x = b^{-1}(c - a) \in T$. Điều này chứng tỏ ánh xạ $\varphi : T \to T$ cho bởi $\varphi(\alpha) = f(\alpha) = a + b\alpha$ là

một toàn ánh. Do T là hữu hạn nên φ là song ánh. Vậy $f(x)$ là hoán vị được trên T. □

Phần tiếp theo, chúng ta sẽ đưa ra tiêu chuẩn hoán vị được cho những đa thức dạng $f(x) = x^n$. Trước hết, ta cần hai bổ đề hỗ trợ sau. Nhắc lại rằng hàm Euler φ được định nghĩa trên tập các số nguyên dương như sau: $\varphi(1) = 1$ và $\varphi(n)$ là số các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n.

2.1.5 Bổ đề. *Cho G là một nhóm có cấp n. Khi đó G là nhóm xyclic nếu và chỉ nếu với mỗi ước d của n tồn tại nhiều nhất một nhóm con xyclic cấp d.*

Chứng minh. Giả sử $G = (a)$ là xyclic. Cho d là ước của n. Đặt $b = a^{n/d}$. Ta có $b^d = a^n = e$. Nếu $b^k = e$ thì $a^{nk/d} = e$. Do đó nk/d là bội của n. Suy ra k là bội của d. Theo Bổ đề 1.1.5, b có cấp d. Đặt $H = (b)$. Khi đó H là nhóm xyclic cấp d. Giả sử H' cũng là một nhóm con xyclic cấp d của G. Viết $H' = (c)$ và biểu diễn $c = a^t$. Do H' có cấp d nên $c^d = e$. Suy ra $a^{td} = e$. Vì thế td là bội của n và do đó t là bội của n/d. Vì thế $c = a^t \in H$. Suy ra $H' \subseteq H$. Do H và H' cùng có số phần tử là d nên $H = H'$. Vậy G có duy nhất một nhóm con xyclic cấp d.

Ngược lại, giả sử mỗi ước d của n có nhiều nhất một nhóm con xyclic cấp d của G. Ta xét quan hệ trên G như sau: $x \sim y$ nếu và chỉ nếu $(x) = (y)$. Dễ thấy $\sim$ là quan hệ tương đương trên G. Với mỗi $x \in G$, kí hiệu $cl(x)$ là lớp tương đương của x. Khi đó ta có

$$cl(x) = \{y \in G \mid (x) = (y)\} = \{y \in G \mid y \text{ là phần tử sinh của } (x)\}.$$

Giả sử x có cấp d_x. Theo Định lí Lagrange, d_x là ước của n. Theo Hệ quả 1.1.6, phần tử $y = x^k$ là phần tử sinh của nhóm xyclic (x) nếu và chỉ nếu $(k, d_x) = 1$. Vì thế $cl(x)$ có đúng $\varphi(d_x)$ phần tử với φ là hàm Euler.

Gọi $cl(x_1), \ldots, cl(x_t)$ là tất cả lớp tương đương. Khi đó $G = \bigcup_{i=1,\ldots,t} cl(x_i)$ và $cl(x_i) \cap cl(x_j) = \varnothing$ với mọi $i \neq j$. Do đó ta có

$$n = \varphi(d_{x_1}) + \ldots + \varphi(d_{x_t}).$$

Chú ý rằng $d_{x_1}, \ldots, d_{x_t}$ đều là ước của n. Theo giả thiết, mỗi ước d của n chỉ có đúng một nhóm con xyclic cấp d nên các nhóm $(x_1), \ldots, (x_t)$ phải có cấp đôi một khác nhau. Do đó $d_{x_1}, \ldots, d_{x_t}$ là các số tự nhiên đôi một khác nhau. Bây giờ ta xét nhóm $\mathbb{Z}_n$. Khi đó với mỗi ước d của n, tồn tại duy nhất một nhóm con xyclic cấp d của $\mathbb{Z}_n$. Do đó ta có $n = \sum_{d|n} \varphi(d)$. Vì thế $n = \varphi(d_{x_1}) + \ldots + \varphi(d_{x_t}) \leqslant \sum_{d|n} \varphi(d) = n$. Vì thế $d_{x_1}, \ldots, d_{x_t}$ là tất cả các là ước của n. Đặc biệt, trong các ước $d_{x_i}, i = 1, \ldots, t$, ắt có một ước bằng n. Do đó tồn tại phần tử $x_i \in G$ có cấp $d_{x_i} = n$. Vì vậy $G = (x_i)$ là xyclic. □

Nhắc lại rằng nếu T là một trường thì mỗi đa thức một biến bậc n với hệ số trong T có nhiều nhất n nghiệm trong T.

2.1.6 Bổ đề. *Cho T là trường hữu hạn. Đặt $T^* = T\backslash\{0\}$. Khi đó T^* là nhóm xyclic với phép nhân.*

Chứng minh. Giả sử T có q phần tử. Khi đó T^* có $q - 1$ phần tử.

Trước hết ta chứng minh T^* là nhóm với phép nhân. Cho $a, b \in T^*$. Khi đó $a, b \neq 0$. Do đó tồn tại $c, d \in T$ sao cho $ac = 1 = bd$. Suy ra $(ab)(sd) = 1 \neq 0$. Vì thế $ab \neq 0$, tức là $ab \in T^*$. Do đó phép nhân đóng kín trong T^*. Rõ ràng phép nhân trong T^* có tính chất kết hợp. Do $1 \neq 0$ nên $1 \in T^*$. Cho $a \in T^*$. Khi đó $a \neq 0$. Vì thế a có nghịch đảo $a^{-1} \in T$. Rõ ràng $a^{-1} \neq 0$. Suy ra $a^{-1} \in T^*$. Vì thế mỗi phần tử trong T^* đều khả nghịch. Vậy, T^* là một nhóm nhân với cấp là $q - 1$.

Tiếp theo ta chứng minh T^* là nhóm xyclic. Giả sử d là một ước của $q - 1$. Theo Bổ đề 2.1.5, để chứng minh T^* là xyclic, ta chỉ cần chứng

minh T^* có nhiều nhất một nhóm con xyclic cấp d. Giả sử $H = (a)$ và $H' = (b)$ là hai nhóm con xyclic cấp d khác nhau của G. Khi đó $a^d = 1$ và $b^d = 1$. Vì thế các phần tử của H và H' đều là nghiệm của đa thức $x^d - 1 \in T[x]$. Vì H và H' khác nhau nên $H \cup H'$ có ít nhất $d+1$ phần tử. Điều này chứng tỏ đa thức bậc d có ít nhất $d+1$ nghiệm. Điều này là vô lí. □

Bây giờ chúng ta trình bày tiêu chuẩn hoán vị được của đa thức x^n.

2.1.7 Định lý. *Trên một trường có q phần tử, đa thức $f(x) = x^n$ là hoán vị được nếu và chỉ nếu $q-1$ và n là nguyên tố cùng nhau.*

Chứng minh. Giả sử $q-1$ và n là nguyên tố cùng nhau. Khi đó tồn tại các số nguyên r, s sao cho $1 = r(q-1) + sn$. Giả sử T là trường có q phần tử. Với mỗi $0 \neq c \in T$, ta có $c = c^1 = c^{r(q-1)}(c^s)^n$. Ta khẳng định $c^{r(q-1)} = 1$. Thật vậy, đặt $T^* = T\backslash\{0\}$. Khi đó T^* là một nhóm nhân với cấp là $q-1$ và nhóm nhân này là xyclic. Theo Hệ quả 1.1.9 ta có $c^{q-1} = 1$. Suy ra $c^{r(q-1)} = 1$. Khẳng định được chứng minh. Do đó $c = (c^s)^n = f(c^s)$. Khi $c = 0$ thì ta luôn có $c = (c)^n = f(c)$. Suy ra ánh xạ $\varphi : T \to T$ cho bởi $\varphi(a) = a^n$ là toàn ánh. Vì T là tập hữu hạn nên φ là song ánh. Do đó đa thức $f(x) = x^n$ là hoán vị được.

Giả sử x^n là hoán vị được trên trường T có q phần tử. Ta chứng minh $q-1$ và n nguyên tố cùng nhau. Gọi d là ước chúng lớn nhất của $q-1$ và n. Theo Bổ đề 2.1.6, T^* là nhóm xyclic cấp $q-1$ với phép nhân. Giả sử $T^* = (a)$. Vì T^* có cấp $q-1$ nên $a^{q-1} = 1$ theo Hệ quả 1.1.9. Do đó $(a^{q-1})^{n/d} = 1$. Vì thế $(a^{(q-1)/d})^n = 1 = 1^n$. Đặt $f(x) = x^n$. Khi đó ta có $f(a^{(q-1)/d}) = f(1)$. Do $f(x)$ hoán vị được theo giả thiết nên ta có $a^{(q-1)/d} = 1$. Do a có cấp $q-1$ nên theo Bổ đề 1.1.5, $(q-1)/d$ là bội của $q-1$. Vì thế $d = 1$. □

Sử dụng Định lí 2.1.7, ta có thể đặc trưng tính hoán vị được của các

đa thức bậc 2 như sau.

2.1.8 Mệnh đề. *Đa thức $f(x) = ax^2 + bx + c$ với $a \neq 0$ là hoán vị được trên một trường hữu hạn T nếu và chỉ nếu $b = 0$ và T có đặc số 2.*

Chứng minh. Giả sử $b = 0$ và T có đặc số 2. Khi đó $f(x) = ax^2 + c$. Giả sử T có q phần tử. Do T có đặc số 2 nên theo Mệnh đề 1.3.7, tồn tại số tự nhiên k sao cho $q = 2^k$. Do đó $q - 1$ là số lẻ. Vì thế $q - 1$ nguyên tố cùng nhau với 2. Theo Định lí 2.1.7, đa thức x^2 là hoán vị được trên T. Giả sử $f(r) = f(s)$ với $r, s \in T$. Khi đó $ar^2 + c = as^2 + c$. Suy ra $ar^2 = as^2$. Do $a \neq 0$ và T là trường nên a khả nghịch. Nhân hai vế với nghịch đảo của a ta được $r^2 = s^2$. Vì đa thức x^2 là hoán vị được trên T nên $r = s$. Vậy $f(x)$ là hoán vị được trên T.

Ngược lại, giả sử $f(x)$ là hoán vị được trên T. Trước hết ta chứng minh $b = 0$. Giả sử $b \neq 0$ và ta cần tìm mâu thuẫn. Do $a \neq 0$ nên tồn tại phần tử $a^{-1} \in T$ sao cho $aa^{-1} = 1$. Vì thế ta có

$$f(-a^{-1}b) = a(-a^{-1}b)^2 + b(-a^{-1}b) + c = a^{-1}b^2 - a^{-1}b^2 + c = c.$$

Rõ ràng $f(0) = c$. Do $f(x)$ là hoán vị được trên T nên $0 = a^{-1}b$. Vì $b \neq 0$ nên tồn tại $b^{-1} \in T$ sao cho $bb^{-1} = 1$. Nhân cả hai vế của đẳng thức $0 = a^{-1}b$ với ab^{-1} ta được $0 = 1$, điều này là vô lí. Vậy $b = 0$.

Tiếp theo ta chứng minh đặc số của T là 2. Do T là trường nên T có đặc số 0 hoặc đặc số p nguyên tố. Nếu T có đặc số 0 thì với mọi số tự nhiên $n < m$ ta có $(m - n)1 \neq 0$, tức là $n.1 \neq m.1$. Vì thế T chứa một tập con $\{n.1 \mid n \in \mathbb{Z}\}$ gồm vô hạn phần tử, điều này là vô lí. Vì thế T có đặc số p nguyên tố. Ta cần chứng minh $p = 2$. Nếu $p \neq 2$ thì p là số nguyên tố lẻ. Do số phần tử của T là một lũy thừa của p nên q là số lẻ. Vì thế $q - 1$ là số chẵn. Vì thế $q - 1$ và 2 không nguyên tố cùng nhau. Theo Định lí 2.1.7, đa thức x^2 không hoán vị được trên T. Vì thế tồn tại hai phần tử $r \neq s$ trong T sao cho $r^2 = s^2$. Suy ra $ar^2 + c = as^2 + c$,

tức là $f(r) = f(s)$, trong khi đó $r \neq s$. Do đó $f(x)$ không hoán vị được trên T, vô lí. □

2.2 Một số lớp đa thức hoán vị được trên một trường

Mục này dành để trình bày tiêu chuẩn hoán vị được trên một trường của một số lớp đa thức. Trước hết, chúng ta trình bày một mở rộng của Mệnh đề 2.1.8.

2.2.1 Định lý. *Cho T là trường có q phần tử. Giả sử k, j là các số nguyên dương sao cho $k > j \geqslant 1$ và $\gcd(k-j, q-1) = 1$. Khi đó đa thức $f(x) = ax^k + bx^j + c$ với $a \neq 0$ là hoán vị được trên T nếu và chỉ nếu $b = 0$ và $\gcd(k, q-1) = 1$.*

Chứng minh. Giả sử $f(x)$ hoán vị được trên T. Trước hết ta chứng minh $b = 0$. Giả sử $b \neq 0$ và ta cần tìm mâu thuẫn. Đặt $g(x) = x^k + a^{-1}bx^j$. Ta khẳng định $g(x)$ hoán vị được trên T. Cho $r, s \in T$ sao cho $g(r) = g(s)$. Khi đó $ag(r) + c = ag(s) + c$. Suy ra $f(r) = f(s)$. Do $f(x)$ hoán vị được trên T nên $r = s$. Vì thế $g(x)$ hoán vị được. Ta có $g(x) = x^j(x^{k-j} + a^{-1}b)$. Vì $j \geqslant 1$ nên $g(0) = 0$. Theo giả thiết, $\gcd(k-j, q-1) = 1$. Do đó tồn tại các số nguyên m, n sao cho $1 = m(k-j) + n(q-1)$. Đặt $d = -a^{-1}b$. Do $b \neq 0$ và $a \neq 0$ nên $d \in T^*$. Ta có

$$d = d^1 = (d^m)^{k-j}(d^{q-1})^n.$$

Do T^* là nhóm cấp $q-1$ với phép nhân và $d \in T^*$ nên $d^{q-1} = 1$. Vì thế $d = (d^m)^{k-j}$. Suy ra

$$g(d^m) = (d^m)^j((d^m)^{k-j} - d) = (d^m)^j((d^m)^{k-j} - (d^m)^{k-j}) = 0.$$

Do $d \neq 0$ nên $d^m \neq 0$. Như vậy, $g(0) = g(d^m)$, trong khi đó $d^m \neq 0$. Điều này chứng tỏ $g(x)$ không hoán vị được trên T, vô lí. Vậy $b = 0$.

Tiếp theo, ta chứng minh $\gcd(k, q-1) = 1$. Do $b = 0$ nên $f(x) = ax^k + c$. Đặt $h(x) = x^k$. Cho $h(r) = h(s)$ với $r, s \in T$. Khi đó $r^k = s^k$. Suy ra $ar^k + c = as^k + c$, tức là $f(r) = f(s)$. Do $f(x)$ hoán vị được trên T nên $r = s$. Vì thế $h(x)$ là hoán vị được trên T. Theo Định lí 2.1.7, $\gcd(k, q-1) = 1$.

Ngược lại, giả sử $b = 0$ và $\gcd(k, q-1) = 1$. Ta cần chứng minh $f(x)$ hoán vị được trên T. Vì $b = 0$ nên $f(x) = ax^k + c$. Do $\gcd(k, q-1) = 1$ nên theo Định lí 2.1.7, đa thức x^k là hoán vị được trên T. Giả sử $f(r) = f(s)$. Khi đó $ar^k + c = as^k + c$. Suy ra $r^k = s^k$. Do x^k hoán vị được trên T nên $r = s$. Vậy $f(x)$ là hoán vị được trên T. □

Hệ quả sau đây cho ta một lớp các đa thức hoán vị được.

2.2.2 Hệ quả. *Cho T là trường có q phần tử. Giả sử $q-1$ không là bội của $3, 5, 7$. Khi đó đa thức $x^8 + bx^t$, với t là một số lẻ nhỏ hơn 8, là đa thức hoán vị được trên T nếu và chỉ nếu $b = 0$ và T có đặc số 2.*

Chứng minh. Xét đa thức $f(x) = x^k + ax^t$ với $k = 8$. Vì t lẻ và $t < 8$ nên $k - t = 8 - t \in \{7, 5, 3, 1\}$. Theo giả thiết, $q-1$ không là bội của $3, 5, 7$. Do đó $\gcd(k-t, q-1) = 1$. Theo Định lí 2.2.1, đa thức $f(x)$ là hoán vị được trên T nếu và chỉ nếu $a = 0$ và $\gcd(k, q-1) = \gcd(8, q-1) = 1$. Chú ý rằng $\gcd(8, q-1) = 1$ nếu và chỉ nếu q là số chẵn. Gọi p là đặc số của T. Khi đó p là số nguyên tố và q là một lũy thừa của p. Vì thế q là số chẵn nếu và chỉ nếu T có đặc số nguyên tố chẵn, tức là đặc số của T bằng 2. Vậy, $f(x)$ là hoán vị được trên T nếu và chỉ nếu $a = 0$ và T có đặc số 2. □

2.2.3 Hệ quả. *Cho T là trường có q phần tử. Cho $f(x) = ax^k + bx^j + c$ là một đa thức trên T, trong đó $a \neq 0$, $k > j \geqslant 1$ và $-ba^{-1}$ là một lũy thừa bậc $k - j$ của một phần tử trong T. Khi đó $f(x)$ là hoán vị được trên T nếu và chỉ nếu $b = 0$ và $\gcd(k, q-1) = 1$.*

Chứng minh. Giả sử $f(x)$ hoán vị được trên T. Theo giả thiết, tồn tại phần tử $r \in T$ sao cho $-ba^{-1} = r^{k-j}$. Đặt $g(x) = x^k + ba^{-1}x^j$. Ta khẳng định $g(x)$ là hoán vị được trên T. Thật vậy, giả sử $g(s) = g(s')$ với $s, s' \in T$. Khi đó $ag(s) + c = ag(s') + c$. Do đó $f(s) = f(s')$. Vì $f(x)$ hoán vị được trên T nên $s = s'$. Do đó $g(x)$ hoán vị được trên T.

Ta có

$$g(x) = x^j(x^{k-j} - (-a^{-1}b)) = x^j(x^{k-j} - r^{k-j}).$$

Do $j \geqslant 1$ nên $g(0) = 0$. Rõ ràng $g(r) = 0$. Vì $g(x)$ hoán vị được nên $r = 0$. Suy ra $-a^{-1}b = 0$. Vì $a \neq 0$ nên $b = 0$. Do đó $g(x) = x^k$. Vì $g(x)$ hoán vị được nên theo Định lí 2.1.7 ta có $\gcd(k, q-1) = 1$.

Ngược lại, giả sử $b = 0$ và $\gcd(k, q-1) = 1$. Khi đó $f(x) = ax^k + c$. Do $\gcd(k, q-1) = 1$ nên theo Định lí 2.1.7 ta suy ra x^k là hoán vị được trên T. Giả sử $f(r) = f(s)$ với $r, s \in T$. Khi đó $ar^k + c = as^k + c$. Suy ra $r^k = s^k$. Do $g(x)$ hoán vị được trên T nên $r = s$. Vì thế $f(x)$ là hoán vị được trên T. □

Trong phần cuối của mục này, chúng ta trình bày một số ví dụ về đa thức hoán vị được.

2.2.4 Ví dụ. Các phát biểu sau là đúng:

(i) Đa thức $x^8 - 2x^3$ hoán vị được trên trường $\mathbb{Z}_{11}$.

(ii) Đa thức $x^8 + 4x$ hoán vị được trên trường $\mathbb{Z}_{29}$.

Chứng minh. Trong Hệ quả 2.2.2, với giả thiết T là trường có q phần tử với $q-1$ không là bội của $3, 5, 7$ thì đa thức $f(x) = x^8 + bx^t$, trong đó t lẻ nhỏ hơn 8, là hoán vị được trên T nếu và chỉ nếu $b = 0$ và T có đặc số 2. Ví dụ 2.2.4 chỉ ra rằng giả thiết $q-1$ không là bội của $3, 5, 7$ là không thể bỏ đi được. Mặc dù đa thức $x^8 - 2x^3$ trong mệnh đề (i) có hệ số $b = -2 \neq 0$ và đặc số của trường $T = \mathbb{Z}_{11}$ là $11 \neq 2$, nhưng đa

thức này vẫn hoán vị được trên T vì $q-1=10$ là một bội của 5. Thật vậy, xét đa thức $f(x)=x^8-2x^3$ ta có $f(0)=0, f(1)=10, f(2)=9, f(3)=6, f(4)=2, f(5)=7, f(6)=1, f(7)=5, f(8)=4, f(9)=8$ và $f(10)=3$. Vì thế ánh xạ $\varphi:\mathbb{Z}_{11}\to\mathbb{Z}_{11}$ cho bởi $\varphi(a)=f(a)$ là song ánh. Do đó $f(x)$ là đa thức hoán vị được modulo 11. Tương tự như vậy, mặc dù đa thức x^8+4x trong mệnh đề (ii) có hệ số $b=4\neq 0$ và đặc số của trường $T=\mathbb{Z}_{29}$ là $29\neq 2$, nhưng nó vẫn hoán vị được trên $\mathbb{Z}_{29}$. Sở dĩ như vậy vì $q-1=28$ là một bội của 7. Thật vậy, xét đa thức $f(x)=x^8+4x$ ta có $f(0)=0, f(1)=5, f(2)=3, f(3)=19, f(4)=12, f(5)=15, f(6)=18, f(7)=6, f(8)=23, f(9)=27, f(10)=7, f(11)=2, f(12)=20, f(13)=10, f(14)=21, f(15)=25, f(16)=22, f(17)=11, f(18)=1, f(19)=14, f(20)=13, f(21)=17, f(22)=8, f(23)=28, f(24)=4, f(25)=9, f(26)=24, f(27)=16$ và $f(28)=26$. Vì thế ánh xạ $\varphi:\mathbb{Z}_{29}\to\mathbb{Z}_{29}$ cho bởi $\varphi(a)=f(a)$ là song ánh. Do đó $f(x)$ là đa thức hoán vị được modulo 29 □

2.2.5 Ví dụ. Xét đa thức $f(x)=x^8-3x$. Khi đó

(i) $f(x)$ không hoán vị được trên trường $\mathbb{Z}_5$;

(ii) $f(x)$ không hoán vị được trên trường $\mathbb{Z}_{11}$;

(iii) $f(x)$ không hoán vị được trên trường $\mathbb{Z}_{13}$.

Chứng minh. Ở ví dụ (i) đa thức $f(x)=x^8-3x$ có $q-1=4$ không là bội của $3,5,7$ nhưng $b=-3\neq 0$ và đặc số của trường $T=\mathbb{Z}_5$ là $5\neq 2$. Đồng thời đa thức $f(x)$ có $f(0)=0, f(1)=3, f(2)=0, f(3)=2$ và $f(4)=4$. Vì thế ánh xạ $\varphi:\mathbb{Z}_5\to\mathbb{Z}_5$ cho bởi $\varphi(a)=f(a)$ không là song ánh. Do đó $f(x)$ là đa thức không hoán vị được modulo 5. Ở ví dụ (ii) đa thức $f(x)=x^8-3x$ có $q-1=10$ là bội của 5 và có $b=-3\neq 0$ và đặc số của trường $T=\mathbb{Z}_{11}$ là $11\neq 2$. Đồng thời đa thức $f(x)$ có $f(0)=0, f(1)=9, f(2)=8, f(3)=7, f(4)=8, f(5v)=0, f(6)=8, f(7)=10, f(8)=3, f(9)=9$ và $f(10)=4$. Vì thế ánh xạ $\varphi:\mathbb{Z}_{11}\to\mathbb{Z}_{11}$ cho

bởi $\varphi(a) = f(a)$ không là song ánh ($f(2) = f(4) = f(6) = 8$). Do đó $f(x)$ là đa thức không hoán vị được modulo 11. Tương tự như vậy, ở ví dụ (iii) đa thức $f(x) = x^8 - 3x$ có $q-1 = 12$ là bội của 3 và có $b = -3 \neq 0$ và đặc số của trường $T = \mathbb{Z}_{13}$ là $13 \neq 2$. Đồng thời đa thức $f(x)$ có $f(0) = f(3) = 0, f(1) = f(6) = 11, f(2) = f(8) = 3, f(4) = f(12) = 4$ và $f(9) = f(11) = 2$ Vì thế ánh xạ $\varphi : \mathbb{Z}_{13} \to \mathbb{Z}_{13}$ cho bởi $\varphi(a) = f(a)$ không là song ánh. Do đó $f(x)$ là đa thức không hoán vị được modulo 13 □

2.3 Đa thức hoán vị được modulo 2^k

Mục đích của mục này là trình bày tiêu chuẩn hoán vị được của đa thức với hệ số nguyên theo modulo 2^k trong bài báo của Ronald Rivest [R]. Từ nay đến hết luận văn, ta luôn giả thiết $f(x)$ là đa thức với hệ số nguyên. Nhắc lại rằng $f(x)$ được gọi là hoán vị được modulo n nếu ánh xạ $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ cho bởi $\varphi(\overline{a}) = f(\overline{a})$ là một song ánh.

2.3.1 Chú ý. Giả sử X là một tập hữu hạn. Khi đó một ánh xạ $\varphi : X \longrightarrow X$ là song ánh nếu và chỉ nếu nó là đơn ánh, nếu và chỉ nếu nó là toàn ánh. Do đó, đa thức $f(x)$ hoán vị được modulo n nếu và chỉ nếu ánh xạ $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ cho bởi $\varphi(\overline{a}) = f(\overline{a})$ là đơn ánh, nếu và chỉ nếu $f(a) \equiv f(b) \pmod{n}$ kéo theo $a \equiv b \pmod{n}$ với mọi $a, b \in \mathbb{Z}$.

2.3.2 Ví dụ. Cho $f(x) = 3+7x+8x^2+3x^3+4x^4$ và $g(x) = 2+2x+2x^2$. Ta xét tính hoán vị được của $f(x)$ và $g(x)$ theo modulo 2^3. Trong $\mathbb{Z}_8[x]$, đa thức $f(x)$ có dạng $f(x) = 3 + 7x + 3x^3 + 4x^4$. Ta có $f(0) = 3, f(1) = 1, f(2) = 4, f(3) = 7, f(4) = 6, f(5) = 2, f(6) = 0$ và $f(7) = 5$. Vì thế ánh xạ $\varphi_f : \mathbb{Z}_8 \to \mathbb{Z}_8$ cho bởi $\varphi_f(a) = f(a)$ là song ánh. Ta có $g(0) = 2, g(1) = 6, g(2) = 6, g(3) = 2, g(4) = 2, g(5) = 6, g(6) = 6$ và $g(7) = 2$. Vì thế ánh xạ $\varphi_g : \mathbb{Z}_8 \to \mathbb{Z}_8$ cho bởi $\varphi_g(a) = g(a)$ không

là song ánh. Vậy, $f(x)$ hoán vị được modulo 2^3 và $g(x)$ không hoán vị được modulo 2^3.

Trước hết chúng ta trình bày một tiêu chuẩn để đa thức $f(x)$ là hoán vị được modulo 2.

2.3.3 Bổ đề. *Đa thức $f(x) = a_0 + a_1x + \ldots + a_dx^d$ với hệ số nguyên là hoán vị được modulo 2 nếu và chỉ nếu $a_1 + \ldots + a_d$ là lẻ.*

Chứng minh. Ta luôn có $f(0) = a_0 \in \mathbb{Z}_2$. Ta xét hai trường hợp.

a) Giả sử a_0 chẵn. Khi đó $f(0) = 0 \in \mathbb{Z}_2$. Vì thế, $f(x)$ là hoán vị được modulo 2 nếu và chỉ nếu $f(1) = 1 \in \mathbb{Z}_2$. Ta có $f(1) = a_0 + a_1 + \ldots + a_d$. Vì a_0 chẵn nên $f(1) = 1 \in \mathbb{Z}_2$ nếu và chỉ nếu $a_1 + \ldots + a_d$ là lẻ. Do đó $f(x)$ là hoán vị được modulo 2 nếu và chỉ nếu $a_1 + \ldots + a_d$ là lẻ.

b) Giả sử a_0 lẻ. Khi đó $f(0) = 1 \in \mathbb{Z}_2$. Vì thế, $f(x)$ là hoán vị được modulo 2 nếu và chỉ nếu $f(1) = 0 \in \mathbb{Z}_2$. Ta có $f(1) = a_0 + a_1 + \ldots + a_d$. Vì a_0 lẻ nên $f(1) = 0 \in \mathbb{Z}_2$ nếu và chỉ nếu $a_1 + \ldots + a_d$ là lẻ. Do đó $f(x)$ là hoán vị được modulo 2 nếu và chỉ nếu $a_1 + \ldots + a_d$ là lẻ. □

2.3.4 Bổ đề. *Cho $f(x) = a_0 + a_1x + \ldots + a_dx^d$ là đa thức với hệ số nguyên. Cho $n = 2m$ với m là một số nguyên chẵn. Giả sử $f(x)$ là hoán vị được modulo n. Khi đó a_1 là số lẻ.*

Chứng minh. Ta có $\overline{0} \neq \overline{m} \in \mathbb{Z}_n$. Vì $f(x)$ hoán vị được modulo n nên $f(\overline{0}) \neq f(\overline{m}) \in \mathbb{Z}_n$. Ta có

$$f(m) = a_0 + a_1m + \left(a_2m^2 + \ldots + a_dm^d\right).$$

Do m là số chẵn nên m^2 chia hết cho n. Do đó

$$f(m) \equiv a_0 + a_1m \pmod{n}.$$

Giả sử a_1 là chẵn. Vì m chẵn nên $a_1m \equiv 0 \pmod{n}$. Do đó $f(m) \equiv a_0 \pmod{n}$. Rõ ràng $f(0) \equiv 0 \pmod{n}$. Vì thế $f(\overline{m}) = f(\overline{0}) \in \mathbb{Z}_n$, trong

khi đó $\overline{0} \neq \overline{m} \in \mathbb{Z}_n$. Vì thế $f(x)$ không hoán vị được modulo n, vô lí. Vậy, a_1 là số lẻ. □

2.3.5 Ví dụ. Cho $f(x) = 2x + 4x^2 + 6x^3$. Ta xét tính hoán vị được của $f(x)$ theo modulo $n = 8$. Rõ ràng $n = 2.m$, với $m = 4$ là số chẵn. Ta có $a_1 = 2$ là số chẵn. Vì thế, theo Bổ đề 2.3.4, đa thức $f(x)$ không hoán vị được modulo 8. Điều này cũng có thể thấy dễ dàng từ định nghĩa đa thức hoán vị được. Trong $\mathbb{Z}_8$ ta có $f(0) = 0, f(1) = 4, f(2) = 4, f(3) = 4, f(4) = 0, f(5) = 4, f(6) = 4$ và $f(7) = 4$. Vì thế ánh xạ $\varphi_g : \mathbb{Z}_8 \to \mathbb{Z}_8$ cho bởi $\varphi_f(a) = f(a)$ không là song ánh.

2.3.6 Bổ đề. *Cho $f(x) = a_0 + a_1x + \ldots + a_dx^d$ là đa thức với hệ số nguyên. Cho $n = 2^k$ với $k > 0$ và cho $m = 2^{k-1} = n/2$. Nếu $f(x)$ hoán vị được modun n thì nó hoán vị được modulo m.*

Chứng minh. Giả sử $f(x)$ hoán vị được modulo n. Với mỗi $a \in \mathbb{Z}$ ta có

$$\begin{aligned} f(a+m) &= a_0 + a_1(x+m) + \ldots + a_d(x+m)^d \\ &= a_0 + a_1a + \ldots + a_da^d + mt, \text{ với } t \text{ là một số nguyên nào đó} \\ &\equiv a_0 + a_1a + \ldots + a_da^d \pmod{m} \\ &\equiv f(a) \pmod{m}. \end{aligned}$$

Giả sử $f(x)$ không hoán vị được modulo m. Khi đó có hai giá trị $\overline{r} \neq \overline{s} \in \mathbb{Z}_m$ sao cho $f(\overline{r}) = f(\overline{s}) \in \mathbb{Z}_m$. Suy ra $r \not\equiv s \pmod{m}$ và $f(r) \equiv f(s) \pmod{m}$. Vì vậy, theo tính chất vừa chứng minh ở trên ta có

$$f(r) \equiv f(r+m) \equiv f(s) \equiv f(s+m) \pmod{m}.$$

Do đó, tồn tại các số nguyên t_1, t_2 sao cho $f(r) - f(r+m) = mt_1$ và $f(r) - f(s) = mt_2$. Vì $(r+m) - r$ không là bội của $n = 2m$ nên ta có $\overline{r+m} \neq \overline{r} \in \mathbb{Z}_n$. Do $f(x)$ hoán vị được modulo n nên $f(r+m) \not\equiv f(r) \pmod{n}$. Do đó t_1 lẻ. Theo giả thiết, $r \not\equiv s \pmod{m}$. Vì thế

$r \not\equiv s \pmod n$. Vì $f(x)$ hoán vị được modulo n nên $f(r) \not\equiv f(s) \pmod n$. Vì thế t_2 là lẻ. Suy ra $t_2 - t_1$ chẵn. Do đó

$$\begin{aligned} f(r+m) - f(s) &= \big(f(r) - f(s)\big) - \big(f(r) - f(r+m)\big) \\ &= m(t_2 - t_1) \equiv 0 \pmod n. \end{aligned}$$

Do $f(x)$ hoán vị được modulo n nên $r + m - s \equiv 0 \pmod n$. Do m là ước của n nên $r + m - s \equiv 0 \pmod m$. Vì thế $r - s \equiv 0 \pmod m$. Điều này là vô lí với cách chọn của r và s. □

Nhìn chung, bài toán kiểm tra (theo định nghĩa) tính không hoán vị được của $f(x)$ modulo 2^k khi k lớn là rất khó. Vì thế, trong nhiều trường hợp ta có thể sử dụng Bổ đề 2.3.6 để giải quyết bài toán này. Dưới đây là một ví dụ minh họa.

2.3.7 Ví dụ. Cho đa thức $f(x) = 1 + 2x + x^2$. Khi đó $f(x)$ không hoán vị được modulo 128.

Chứng minh. Trong vành $\mathbb{Z}_8$ ta có

$$f(0) = 1, f(1) = 4, f(2) = 1, f(3) = 0, f(4) = 1, f(5) = 4, f(6) = 1.$$

Đặc biệt, ta có $\overline{0} \neq \overline{2} \in \mathbb{Z}_8$, nhưng $f(\overline{0}) = f(\overline{2}) = \overline{1} \in \mathbb{Z}_8$. Vì thế ánh xạ $\varphi_f : \mathbb{Z}_8 \to \mathbb{Z}_8$ cho bởi $\varphi_f(\overline{a}) = f(\overline{a})$ không là song ánh. Vì thế $f(x)$ không hoán vị được modulo 8. Theo Bổ đề 2.3.6, $f(x)$ không hoán vị được modulo 16. Tiếp tục áp dụng Bổ đề 2.3.6, ta suy ra $f(x)$ không hoán vị được modulo 2^k với mọi $k \geqslant 3$. Đặc biệt, vì 128 là lũy thừa của 2 nên $f(x)$ không hoán vị được modulo 128. □

2.3.8 Bổ đề. *Cho $f(x) = a_0 + a_1x + \ldots + a_dx^d$ là đa thức với hệ số nguyên. Cho $n = 2m$. Giả sử $f(x)$ hoán vị được modulo n. Khi đó $f(a + m) \equiv f(a) + m \pmod m$ với mọi số nguyên a.*

Chứng minh. Cho $a \in \mathbb{Z}$. Theo chứng minh Bổ đề 2.3.6, tồn tại số nguyên t sao cho $f(a+m) - f(a) = mt$. Vì $n = 2m$ nên $(a+m) - a$ không là bội của n, tức là $\overline{a+m} \neq \overline{a} \in \mathbb{Z}_n$. Do $f(x)$ hoán vị được modulo n nên $f(\overline{a+m}) \neq f(\overline{a}) \in \mathbb{Z}_n$. Do đó $f(a) \not\equiv f(a+m) \pmod{n}$. Vì thế mt không là bội của n. Suy ra t là số lẻ. Vì thế

$$\begin{aligned} f(a+m) = f(a) + mt &\equiv f(a) + m \pmod{2m} \\ &\equiv f(a) + m \pmod{n}. \end{aligned}$$

□

2.3.9 Bổ đề. *Cho $f(x) = a_0 + a_1x + \ldots + a_dx^d$ là đa thức với hệ số nguyên. Cho $n = 2m$ với m là một số chẵn. Giả sử $f(x)$ hoán vị được modulo m. Khi đó $f(x)$ hoán vị được modulo n nếu và chỉ nếu a_1 là số lẻ và $a_3 + a_5 + a_7 + \ldots$ là số chẵn.*

Chứng minh. Do m là số chẵn nên m^2 chia hết cho $n = 2m$. Do đó với mỗi $i = 2, \ldots, d$ và với mỗi số nguyên a ta có

$$\begin{aligned} (a+m)^i &= a^i + ima^{i-1} + tm^2 \text{ với số nguyên } t \text{ nào đó} \\ &\equiv a^i + ima^{i-1} \pmod{n}. \end{aligned}$$

Vì $i \geqslant 2$ nên $i - 1 \geqslant 1$. Do đó nếu có ít nhất một trong 3 số i, a, a_i là chẵn thì a_iima^{i-1} là bội của n. Trong trường này ta có

$$a_i(a+m)^i \equiv a_ia^i \pmod{n}.$$

Còn nếu cả 3 số i, a, a_i đều là số lẻ thì $a_i(ima^{i-1}) \equiv m \pmod{n}$ và do đó ta có

$$a_i(a+m)^i \equiv a_ia^i + m \pmod{n}.$$

Bây giờ ta xét hai trường hợp.

Trường hợp 1: a là số chẵn. Theo trên ta có

$$\begin{aligned} f(a+m) &\equiv a_0 + a_1(a+m) + (a_2a^2 + \ldots + a_da^d) \\ &\equiv f(a) + a_1m \pmod{n}. \end{aligned}$$

Trường hợp 2: a là số lẻ. Theo trên ta có

$$\begin{aligned} f(a+m) &\equiv a_0 + a_1(a+m) + \left(a_2a^2 + a_4a^4 + \ldots\right) \\ &\quad + (a_3a^3 + m) + (a_5a^5 + m) + \ldots \\ &\equiv f(a) + (a_1 + a_3 + a_5 + \ldots)m \pmod{n}. \end{aligned}$$

Bây giờ ta chứng minh bổ đề. Giả sử $f(x)$ hoán vị được modulo n. Theo Bổ đề 2.3.4, hệ số a_1 là lẻ. Chú ý rằng $\overline{a+m} \neq \overline{a} \pmod{n}$ với mọi số nguyên a. Vì thế $f(a+m) \not\equiv f(a) \pmod{n}$ với mọi số nguyên a. Chọn a là một số lẻ (chẳng hạn $a = 1$). Theo Trường hợp 2 ta có

$$f(a+m) - f(a) \equiv (a_1 + a_3 + a_5 + \ldots)m \pmod{n}.$$

Do đó ta có $(a_1 + a_3 + a_5 + \ldots)m \not\equiv 0 \pmod{n}$. Suy ra $a_1 + a_3 + a_5 + \ldots$ phải là số lẻ. Vì a_1 lẻ nên $a_3 + a_5 + a_7 + \ldots$ là số chẵn.

Ngược lại, giả sử a_1 là số lẻ và $a_3 + a_5 + a_7 + \ldots$ là số chẵn. Giả sử phản chứng rằng $f(x)$ không hoán vị được modulo n. Khi đó tồn tại $\overline{a} \neq \overline{b} \in \mathbb{Z}_n$ sao cho $f(\overline{a}) = f(\overline{b}) \in \mathbb{Z}_n$. Do đó có hai số nguyên $a \not\equiv b \pmod{n}$ sao cho $f(a) \equiv f(b) \pmod{n}$. Vì m là ước của n nên $f(a) \equiv f(b) \pmod{m}$. Theo giả thiết, $f(x)$ hoán vị được modulo m, vì thế $a \equiv b \pmod{m}$. Do $a \not\equiv b \pmod{n}$ và $n = 2m$ nên $a - b = mt$ với t là một số lẻ. Vì thế có một số nguyên t' sao cho $b = a - mt = a + m - 2t'm \equiv a + m \pmod{n}$. Suy ra $\overline{b} = \overline{a+m} \in \mathbb{Z}_n$. Vì $f(a) \equiv f(b) \pmod{m}$ nên ta có

$$f(a) \equiv f(a+m) \pmod{n}.$$

Nếu a là số chẵn thì theo Trường hợp 1 ta có

$$f(a+m) \equiv f(a) + a_1m \pmod{n}.$$

Do đó $a_1 m$ là bội của n. Suy ra a_1 chẵn, điều này mâu thuẫn với giả thiết a_1 lẻ. Do đó a là số lẻ. Theo Trường hợp 2 ta có

$$f(a+m) \equiv f(a) + (a_1 + a_3 + a_5 + \ldots)m \pmod{n}.$$

Do đó $(a_1 + a_3 + a_5 + \ldots)m$ là bội của n. Suy ra $a_1 + a_3 + a_5 + \ldots$ là chẵn. Theo giả thiết a_1 là số lẻ. Vì thế $a_3 + a_5 + \ldots$ là số lẻ, điều này là mâu thuẫn với giả thiết $a_3 + a_5 + \ldots$ chẵn. Vậy $f(x)$ hoán vị được modulo n. □

Định lí sau đây là kết quả chính của mục này, và là một trong 3 kết quả chính của luận văn.

2.3.10 Định lý. *Cho $f(x) = a_0 + a_1 x + \ldots + a_d x^d$ là một đa thức với hệ số nguyên. Cho $n = 2^k$ với $k \geqslant 2$. Khi đó $f(x)$ hoán vị được modulo n nếu và chỉ nếu a_1 là số lẻ, $a_2 + a_4 + a_6 + \ldots$ là số chẵn và $a_3 + a_5 + a_7 + \ldots$ là số chẵn.*

Chứng minh. Giả sử $f(x)$ hoán vị được modulo n. Đặt $m_1 = 2^{k-1}$. Khi đó $n = 2m_1$. Do $k \geqslant 2$ nên m_1 là số chẵn. Do đó theo Bổ đề 2.3.4, hệ số a_1 là số lẻ. Do $f(x)$ hoán vị được modulo $n = 2m_1$ nên theo Bổ đề 2.3.6, đa thức $f(x)$ hoán vị được modulo m_1. Vì thế, áp dụng Bổ đề 2.3.9, ta có $a_3 + a_5 + a_7 + \ldots$ là số chẵn.

Tiếp theo, ta khẳng định bằng quy nạp theo $i = 1, \ldots, k-1$ rằng $f(x)$ là hoán vị được modulo 2^{k-i}. Với $i = 1$, ta đã chứng minh ở phần trên rằng $f(x)$ hoán vị được modulo $m_1 = 2^{k-1}$, do đó khẳng định đúng với $i = 1$. Giả sử kết quả đã đúng cho $i-1$ với $i \leqslant k-1$, tức là $f(x)$ hoán vị được modulo 2^{k-i+1}. Đặt $m_i = 2^{k-i}$ và $m_{i-1} = 2^{k-i+1}$. Khi đó $m_{i-1} = 2m_i$. Do $f(x)$ hoán vị được modulo m_{i-1} nên theo Bổ đề 2.3.6, $f(x)$ hoán vị được modulo $m_i = 2^{k-i}$. Khẳng định được chứng minh. Với $i = k-1$, từ khẳng định trên ta suy ra $f(x)$ hoán vị được modulo

2. Do đó theo Bổ đề 2.3.3 ta có $a_1 + a_2 + a_3 + \ldots + a_d$ là số lẻ. Vì a_1 lẻ nên

$$(a_2 + a_4 + a_6 + \ldots) + (a_3 + a_5 + a_7 + \ldots)$$

là số chẵn. Do $a_3 + a_5 + a_7 + \ldots$ là số chẵn nên $a_2 + a_4 + a_6 + \ldots$ là số chẵn.

Ngược lại, giả sử a_1 là số lẻ, $a_2 + a_4 + a_6 + \ldots$ là số chẵn và $a_3 + a_5 + a_7 + \ldots$ là số chẵn. Ta cần chứng minh $f(x)$ hoán vị được modulo $n = 2^k$. Ta chứng minh điều này bằng quy nạp theo k. Cho $k = 1$. Vì a_1 là số lẻ, $a_2 + a_4 + a_6 + \ldots$ là số chẵn và $a_3 + a_5 + a_7 + \ldots$ là số chẵn nên $a_1 + a_2 + a_3 + \ldots + a_d$ là số lẻ. Do đó, theo Bổ đề 2.3.3 ta suy ra $f(x)$ hoán vị được modulo $2 = 2^1$. Vậy, kết quả đúng cho trường hợp $k = 1$.

Cho $k > 1$ và giả thiết kết quả đã đúng cho trường hợp $k - 1$, tức là $f(x)$ hoán vị được modulo 2^{k-1} trong trường hợp a_1 là số lẻ, $a_2 + a_4 + a_6 + \ldots$ là số chẵn và $a_3 + a_5 + a_7 + \ldots$ là số chẵn. Đặt $m = 2^{k-1}$. Khi đó $n = 2m$. Do $k > 1$ nên m là số chẵn. Vì a_1 là số lẻ, $a_3 + a_5 + a_7 + \ldots$ là số chẵn và $f(x)$ hoán vị được modulo m nên theo Bổ đề 2.3.9 ta suy ra $f(x)$ hoán vị được modulo n. □

Phần cuối của mục này trình bày một số ví dụ về đa thức hoán vị được modulo 2^k.

2.3.11 Ví dụ. Các đa thức sau là hoán vị được modulo 2^k

(i) $ax + bx^2$ với mọi số lẻ a và mọi số chẵn b.

(ii) $x + x^2 + x^4$.

(iii) $1 + x + x^2 + \ldots + x^d$, trong đó $d \equiv 1 \pmod 4$.

Chứng minh. (i) Ta có $a_1 = a$ lẻ, $a_2 = b$ chẵn. Theo Định lí 2.3.10, $ax + bx^2$ hoán vị được modulo 2^k.

(ii) Ta có $a_1 = 1$ lẻ, $a_2 + a_4 = 2$ chẵn. Theo Định lí 2.3.10, $x + x^2 + x^4$ hoán vị được modulo 2^k.

(iii) Từ giả thiết ta suy ra d là số lẻ. Ta có $a_1 = 1$ lẻ, $a_2 + a_4 + \ldots + a_{d-1} = (d-1)/2$ và $a_3 + a_5 + \ldots + a_d = (d-1)/2$. Do $d \equiv 1 \pmod 4$ nên $d - 1$ là bội của 4. Vì thế $(d-1)/2$ là số chẵn. Theo Theo Định lí 2.3.10, $1 + x + x^2 + \ldots + x^d$ hoán vị được modulo 2^k. □

Kết luận

Luận văn trình bày một số kết quả về đa thức hoán vị được trong hai bài báo:

1. R. Rivest, Permutation polynomials modulo 2^w, *Finite fields and their applications*, **7** (2001), 287-292.

2. R. A. Mollin and C. Small, On permutation polynomials over finite fields, *Inter. J. Math. and Math. Sciences*, **10** (1987), 535-544.

Nội dung chính của luận văn là:

• Trình bày một số kiến thức chuẩn bị về nhóm, vành, trường, đa thức phục vụ chứng minh các kết quả chính ở Chương 2.

• Đưa ra tiêu chuẩn để đa thức dạng x^n là hoán vị được trên một trường hữu hạn (Định lí 2.1.7). Từ đó suy ra tiêu chuẩn hoán vị được của đa thức bậc không quá hai.

• Chứng minh một điều kiện cần và đủ cho các đa thức dạng $x^k + bx^j + c$, trong đó $k > j \geqslant 1$ là hoán vị được trên một trường hữu hạn (Định lí 2.2.1). Từ đó thu được tính chất hoán vị được của một số đa thức đặc biệt.

• Giải quyết trọn vẹn bài toán về tính hoán vị được modulo n cho các đa thức với hệ số nguyên trong trường hợp n là lũy thừa của 2 (Định lí 2.3.10).

Tài liệu tham khảo

[C] Nguyễn Tự Cường, *Đại số hiện đại, tập 1*, NXB ĐHQGHN, 2001.

[HT] Bùi Huy Hiền và Phan Doãn Thoại, *Bài tập Đại số và số học,* Tập 2, NXB Giáo dục, 1986.

[La] Ngô Thúc Lanh, *Đại số và số học,* Tập 2, NXB Giáo dục, 1986.

[LN] R. Lidl and H. Niedereiter, *Finite Fields*, Addison - Wesley, 1983

[LM1] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field? *The American Math, Monthly*, **3** (1988), 243-246

[LM2] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field? **II**. *The American Math, Monthly*, **1** (1993), 71-74

[MS] R. A. Mollin and C. Small, On permutation polynomials over finite fields, *Inter. J. Math. and Math. Sciences*, **10** (1986), 535-544.

[Riv] R. Rivest, Permutation polynomials modulo 2^w, *Finite fields and their applications*, **7** (1999), 287-292.