Cơ sở đại số

Lý thuyết thông tin

Biên soạn: Phạm Văn Sự

Bộ môn Xử lý tín hiệu và Truyền thông
Khoa Kỹ thuật Điện tử I
Học viện Công nghệ Bưu chính Viễn thông

20/08/2011

Nhóm

Nhóm, nhóm giao hoán

Định nghĩa (Nhóm)

Một nhóm là một tập G chứa các phần tử và trên đó phép toán hai ngôi "$*$" được xác định thỏa mãn các tính chất sau:

1. *(Tính đóng):* $a, b \in G \Rightarrow a * b = c \in G$.
2. *(Tính kết hợp):* $\forall a, b, c \in G \Rightarrow (a * b) * c = a * (b * c)$.
3. *(Tồn tại phần tử đơn vị):* $\exists e \in G$ *sao cho* $a * e = e * a = a \ \forall a \in G$.
4. *(Tồn tại phần tử ngược):* $\forall a \in G \ \exists! a^{-1}$ *thỏa mãn* $a * a^{-1} = a^{-1} * a = e$.

Định nghĩa (Nhóm giao hoán)

Tập G được gọi là nhóm giao hoán nếu nó là một nhóm và có tính chất:

5. $\forall a, b \in G$ *thỏa mãn* $a * b = b * a$.

Nhóm

Cấp của nhóm, Xây dựng nhóm: Phép cộng đồng dư

Định nghĩa (Cấp của nhóm)

Cấp của một nhóm G, kí hiệu là $ord(G)$*, là số phần tử của nhóm:* $ord(G) = |G|$.

- **Chú ý**: Thường, chỉ riêng cấp của nhóm không đủ để xác định nhóm.

Định nghĩa (Phép toán cộng đồng dư m (modulo m))

$a + b \equiv c \quad modulo \quad m \quad (\equiv c \quad mod \quad m)$

Nhóm

Xây dựng nhóm: Phép cộng đồng dư (cont.)

- Phép cộng đồng dư m đối với một tập vô hạn các số nguyên tạo ra m lớp tương đương riêng biệt.
- Hai số nguyên a và b thuộc cùng một lớp tương đương đồng dư m nếu ta có thể viết $a = xm + b$ $(x \in Z)$.
- Một phần tử có thể được thay thế bởi bất cứ phần từ nào thuộc cùng nhóm tương đương mà không làm thay đổi các phép toán đồng dư m.
- Các lớp tương đương thường được gán nhãn đại diện là số nguyên dương nhỏ nhất trong lớp.

Định lý

Các lớp tương đương đồng dư m, $\{0, 1, 2, \ldots, m-1\}$*, tạo thành một nhóm giao hoán cấp m với phép cộng đồng dư m trong đó m là một số nguyên dương bất kỳ nào đó.*

Nhóm

Coset

Các lớp tương đương thu được từ việc mở rộng phép toán đồng dư với một nhóm con S nào đó của nhóm G được gọi là các Coset.

Định nghĩa (Các coset trái, phải)

Gọi S là một nhóm con của nhóm G với phép toán "$+$". Một coset trái của S trong G là một tập con của G mà các phần tử của chúng có thể biểu diễn bởi $x + S = \{x + s, s \in S\}$. Một coset phải của S trong G là một tập con của G mà các phần tử của chúng có thể biểu diễn bởi $S + x = \{s + x, s \in S\}$

- Nếu G là một nhóm giao hoán thì các coset trái trùng với các coset phải

Định lý

Các coset phân biệt nhau của một nhóm con S trong nhóm G không giao nhau.

- Một nhóm con S của một nhóm G định ra một phân hoạch của G thành các coset không giao nhau.

Nhóm

Xây dựng nhóm: Phép nhân đồng dư; Cấp của phần tử trong nhóm

Định nghĩa (Phép toán nhân đồng dư m (modulo m))

$a \times b \equiv c \quad modulo \quad m \quad (\equiv c \quad mod \quad m)$

- Phép nhân đồng dư m không thể dùng để tạo nhóm hữu hạn từ tập số nguyên nếu sử dụng đồng dư bất kỳ.

Định lý

Các phần tử $S = \{0, 1, 2, \ldots, p-1\}$, tạo thành một nhóm giao hoán cấp $p-1$ với phép nhân đồng dư p nếu và chỉ nếu p là một số nguyên tố.

Định nghĩa (Cấp của một phần tử của nhóm)

Gọi g là một phần tử của nhóm G với phép toán "$*$". Kí hiệu $g^2 = g * g$, $g^3 = g * g * g$, v.v... Cấp của g là số nguyên dương nhỏ nhất, kí hiệu là $ord(g)$, sao cho $g^{ord(g)}$ trở thành phần tử đơn vị.

Vành

Vành, vành giao hoán

Định nghĩa (Vành)

Một vành là một tập các phần tử R với hai phép toán "cộng" ("$+$") và phép toán "nhân" ("$\times$") thỏa mãn các tính chất sau:

1. *R là một nhóm giao hoán với phép cộng, phần tử đơn vị với phép cộng được kí hiệu là "0".*
2. *Phép "$\times$" có tính kết hợp: $(a \times b) \times c = a \times (b \times c)$ $\forall a, b, c \in R$.*
3. *Phép "$\times$" có tính phân phối với phép "$+$": $a \times (b + c) = a \times b + a \times c$.*

Định nghĩa (Vành giao hoán)

Một vành R là vành giao hoán nếu nó là một vành và thỏa mãn:

4. *Phép "$\times$" có tính chất giao hoán: $a \times b = b \times a$.*

Nhóm

Nhóm con

Định nghĩa (Nhóm con)

Gọi S là một tập con của G, nếu $\forall a, b \in S$ tồn tại $c = a * b^{-1}$ cũng thuộc S, thì S được gọi là nhóm con của G.

Định nghĩa (Nhóm con đúng nghĩa)

Một nhóm con S là một nhóm con theo đúng nghĩa của G nếu $S \subset G$ nhưng $S \neq G$.

Định lý

Nếu S là một nhóm con của nhóm G, thì $ord(S) | ord(G)$

- $a|b$ là biểu diễn a là một ước số của b

Trường
Định lý

Định lý
Tập các số nguyên $\{0, 1, 2, \ldots, p-1\}$, trong đó p là một số nguyên tố, tạo thành một trường Galois $GF(p)$ đối với các phép toán cộng và nhân đồng dư p.

- $GF(q)$ không phải luôn tồn tại với mọi q
  - q phải thỏa mãn $q = p^m$ (p là một số nguyên tố dương, m là một số nguyên dương)
- $GF(p^m)$ có thể được tạo dựng như một không gian véc-tơ trên trường cấp nguyên tố $GF(p)$.

Vành
Vành có phần tử đơn vị

Định nghĩa (Vành có phần tử đơn vị)
Một vành R có phần tử đơn vị là vành thỏa mãn:

5. *Phép toán "$\times$" có phần tử đơn vị. Phần tử đơn vị đối với phép "$\times$" này gọi là phần tử "1".*

- Nếu một vành R thỏa mãn cả điểm 4 và 5 thì được gọi là vành giao hoán có phần tử đơn vị.
- Vành đa thức là một trong các vành quan trọng trong nghiên cứu lý thuyết mã.

Không gian véc-tơ
Định nghĩa

Gọi **V** là một tập các véc-tơ, **F** là một trường các phần tử vô hướng.

Định nghĩa
***V** là một không gian véc-tơ trên trường **F** nếu thỏa mãn các tính chất sau:*

1. ***V** là một nhóm giao hoán với phép "$+$" véc-tơ.*
2. *Với bất kỳ phần tử $a \in \mathbf{F}$ và $\mathbf{v} \in \mathbf{v}$ ta có $a \times \mathbf{v} = \mathbf{u} \in \mathbf{V}$*
3. *Phép toán "$+$" và "$\times$" có tính chất phân phối:*
   - $a \times (\mathbf{v} + \mathbf{u}) = a \times \mathbf{v} + a \times \mathbf{u}$.
   - $(a + b) \times \mathbf{v} = a \times \mathbf{v} + b \times \mathbf{v}$.
4. *Tính chất kết hợp: $\forall a, b \in \mathbf{F}$ và $\forall \mathbf{v} \in \mathbf{V}$ ta có $(a \times b) \times \mathbf{v} = a \times (b \times \mathbf{v})$.*
5. *Phần tử đơn vị đối với phép nhân trong trường **F** có vai trò như phần tử đơn vị trong phép nhân của hằng số với một véc-tơ: $\forall \mathbf{v} \in \mathbf{V}$ ta có $1 \times \mathbf{v} = \mathbf{v}$.*

- **F** gọi là trường vô hướng trợ của không gian véc-tơ **V**.

Trường
Định nghĩa

Định nghĩa (Trường)
F là tập các đối tượng mà trên đó xác định hai phép toán "$+$" và "$\times$". F được gọi là một trường nếu và chỉ nếu:

1. *F là một nhóm giao hoán đối với phép "$+$", phần tử đơn vị đối với phép "$+$" gọi là "0".*
2. *$F - \{0\}$ (tập F đã được loại bỏ phần tử đơn vị của phép "$+$") là một nhóm giao hoán đối với phép "$\times$", phần tử đơn vị đối với phép "$\times$" được gọi là "1".*
3. *Phép "$+$" và phép "$\times$" có tính chất phân phối: $a \times (b + c) = a \times b + a \times c$.*

Định nghĩa (Trường hữu hạn)
Một trường F với bậc hữu hạn (số phần tử hữu hạn, $|F| < \infty$) được gọi là trường hữu hạn.
Một trường hữu hạn còn được gọi là một trường Galois. Một trường Galois cấp q được ký hiệu là $GF(q)$.

Không gian véc-tơ

Véc-tơ và các khái niệm

Véc-tơ $\mathbf{v}$ thuộc không gian véc-tơ $\mathbf{V}$ trên trường $\mathbf{F}$: $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$, trong đó $v_i \in \mathbf{F}$

Giả sử có các véc-tơ $\mathbf{v} = \{v_0, v_1, v_2, \ldots, v_{l-1}\}$, $\mathbf{u} = \{u_0, u_1, u_2, \ldots, u_{l-1}\}$ với các phần tử $v_i, u_i \in \mathbf{F}$.

- Phép cộng véc-tơ: $\mathbf{v} + \mathbf{u} = \{v_0 + u_0, v_1 + u_1, v_2 + u_2, \ldots, v_{l-1} + u_{l-1}\}$.
- Phép nhân véc-tơ với một số vô hướng: $a \times \mathbf{v} = \{a \times v_0, a \times v_1, a \times v_2, \ldots, a \times v_{l-1}\}$

Xét các véc-tơ $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_n \in \mathbf{V}$, và các hệ số a_1, a_2, ..., $a_n \in \mathbf{F}$, tổ hợp tuyến tính của $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_n$ được xác định là:

$$\mathbf{v} = \sum_i a_i \mathbf{v}_i = a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + \cdots + a_n \mathbf{v}_n$$

$\mathbf{v} \in \mathbf{V}$

Không gian véc-tơ

Véc-tơ và các khái niệm (cont.)

Tập các véc-tơ $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ được gọi là tập các véc-tơ độc lập tuyến tính nếu không có véc-tơ nào thuộc tập có thể biểu diễn bởi tổ hợp tuyến tính của các véc-tơ khác trong tập

Tập các véc-tơ $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ được gọi là tập các véc-tơ phụ thuộc tuyến tính nếu một hoặc một số véc-tơ có thể biểu diễn bởi tổ hợp tuyến tính của các véc-tơ khác trong tập

Không gian véc-tơ

Tập span và cơ sở của không gian véc-tơ

Định nghĩa

Một tập các véc-tơ $\mathbf{G} = \{\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{n-1}\}$ *là tập span của không gian véc-tơ* $\mathbf{V}$ *nếu các tổ hợp tuyến tính của các véc-tơ trong* $\mathbf{G}$ *chứa toàn bộ các véc-tơ trong* $\mathbf{V}$.

- Các véc-tơ trong một tập span của một không gian véc-tơ có thể phụ thuộc tuyến tính hoặc độc lập tuyến tính

Định nghĩa

Một tập span của không gian véc-tơ có số phần tử nhỏ nhất gọi là cơ sở của không gian con đó.

- Các véc-tơ trong cơ sở là độc lập tuyến tính.
- Một không gian con có thể có nhiều cơ sở, tuy nhiên các cơ sở phải có cùng số phần tử.

Không gian véc-tơ

Chiều của không gian véc-tơ

Định nghĩa

Nếu cơ sở của không gian véc-tơ có k phần tử, thì không gian véc-tơ $\mathbf{V}$ *được cho là có k chiều, kí hiệu* $\dim(\mathbf{V}) = k$

Định lý

Cho $\{\mathbf{v}_i\}$ *là một cơ sở của không gian véc-tơ* $\mathbf{V}$. *Khi đó với mọi véc-tơ* $\mathbf{v}$ *trong* $\mathbf{V}$ *tồn tại một biểu diễn:*

$$\mathbf{v} = a_0 \mathbf{v}_0 + a_1 \mathbf{v}_1 + \cdots + a_{k-1} \mathbf{v}_{k-1}$$

và biểu diễn này là duy nhất.

- $|\mathbf{V}| = |F|^k$

Trường Galois

Một số tính chất: Xác định trường, bậc của phần tử trong trường

- Trường Galois hoàn toàn xác định nếu biết cấp của trường.
  - $\Rightarrow$ Hai trường Galois có cùng kích thước luôn tương tự nhau về nhãn của các thành phần, bất kể cách thức mà trường được xây dựng.
- Nếu $\beta \in GF(q) \Rightarrow \beta^i \in GF(q)$.
  - $\Rightarrow$ Dãy $1, \beta, \beta^2, \beta^3, \beta^4, \ldots$ sẽ có sự lặp lại ở một thời điểm nào đó.

Định nghĩa (Bậc của một phần tử của trường Galois)

Với $\beta \in GF(p)$, bậc của β (kí hiệu: $ord(\beta)$) là số nguyên dương nhỏ nhất m sao cho $\beta^m = 1$.

- Tương tự định nghĩa bậc của phần tử trong nhóm.
  - Định nghĩa với phép nhân.

Định lý

Nếu $t = ord(\beta)$ với $\beta \in GF(q)$ thì $t|(q-1)$

Trường Galois

Một số tính chất: Mối quan hệ bậc, Hàm Euler

Định lý

Xét α và β là các phần tử trong $GF(q)$ sao cho $\beta = \alpha^i$. Nếu $ord(\alpha) = t$ thì $ord(\beta) = t/gcd(i,t)$

Định nghĩa (Hàm Euler)

Với một số nguyên t, số các số nguyên tố cùng nhau với t trong tập số $\{1, \ldots, t-1\}$ được xác định bởi hàm Euler như sau:

$$\Phi(t) = |\{1 \le i < t | gcd(i,t) = 1\}| = t \prod_{p|t} (1 - \frac{1}{p})$$

với p là các số nguyên tố là ước của t và nhỏ hơn t, $\Phi(1) = 1$, và $gcd(a,b)$ ước số chung lớn nhất của a và b.

- Tích trong hàm Euler được tính với tất cả các số nguyên tố dương $p < t$ và là ước số của t

Không gian véc-tơ

Không gian con và không gian đối ngẫu

Định nghĩa

Cho $\mathbf{v}_1$ và $\mathbf{v}_2$ là một cặp véc-tơ bất kỳ trong một tập con $\mathbf{S}$ của không gian véc-tơ $\mathbf{V}$ trên trường $\mathbf{F}$. $\mathbf{S}$ là một không gian con của $\mathbf{V}$ nếu và chỉ nếu bất cứ tổ hợp tuyến tính nào của $\mathbf{v}_1$ và $\mathbf{v}_2$ (tức là $a_1\mathbf{v}_1 + a_2\mathbf{v}_2$, với $a_1, a_2 \in \mathbf{F}$) cũng là một véc-tơ thuộc $\mathbf{S}$

Định nghĩa

Cho $\mathbf{S}$ là một không gian con có chiều k của $\mathbf{V}$. $\mathbf{S}^\perp$ là một tập tất cả các véc-tơ trong $\mathbf{V}$ sao cho $\forall \mathbf{u} \in \mathbf{S}$ và $\forall \mathbf{v} \in \mathbf{S}^\perp$ thì tích vô hướng $\mathbf{u}.\mathbf{v} = 0$. $\mathbf{S}^\perp$ được gọi là không gian đối ngẫu của $\mathbf{S}$

- Đôi khi, một không gian véc-tơ hoặc các tính chất của nó có thể dễ dàng được mô tả hơn bởi không gian đối ngẫu.
  - Có thể gặp khi nghiên cứu lớp mã khối tuyến tính
- Các không gian véc-tơ và không gian đối ngẫu của nó không tách rời (disjoint)
  - Cả hai không gian đều chứa phần tử $\mathbf{0}$

Không gian véc-tơ

Không gian con và không gian đối ngẫu (cont.)

Định lý

Không gian đối ngẫu $\mathbf{S}^\perp$ của một không gian con $\mathbf{S} \subseteq \mathbf{V}$ là một không gian con của $\mathbf{V}$

Định lý

$\mathbf{S}$ là không gian con của $\mathbf{V}$, và $\mathbf{S}^\perp$ là một không gian đối ngẫu của $\mathbf{S}$.

$$dim(\mathbf{S}) + dim(\mathbf{S}^\perp) = dim(\mathbf{V})$$

Định nghĩa (Số đặc trưng của một trường $GF(q)$)

Số đặc trưng (characteristic) của một trường $GF(q)$ là một số nguyên dương m nhỏ nhất mà tổng của m số "1" bằng không, ký hiệu: $m(1) = 0$.

Định lý

Số đặc trưng của một trường Galois luôn là một số nguyên tố.

Xét một trường $GF(q)$ có số đặc trưng p

- $GF(q)$ chứa một tập $Z_p = \{0, 1, 2(1), 3(1), \ldots, (p-1)(1)\}$.
  - Z_p phải là một trường đối với các phép cộng và nhân đồng dư p.
  - $p(\alpha) = 0 \ \forall \alpha \in GF(q)$

Định lý

Bậc q của một trường Galois $GF(q)$ phải là một số dạng lũy thừa của một số nguyên tố.

Tính chất của hàm Euler

- Nếu p là số nguyên tố thì $\Phi(p) = p - 1$.
- Nếu p_1 và p_2 là hai số nguyên tố phân biệt thì $\Phi(p_1 p_2) = \Phi(p_1)\Phi(p_2) = (p_1 - 1)(p_2 - 1)$
- Nếu p là một số nguyên tố thì $\Phi(p^m) = p^{(m-1)}(p-1)$.
- Nếu p_1 và p_2 là các số nguyên tố phân biệt thì $\Phi(p_1^m p_2^n) = p_1^{(m-1)} p_2^{(n-1)}(p_1 - 1)(p_2 - 1)$.

- Cho trước t là ước số của $q - 1$ thì số phần tử bậc t trong $GF(q)$ là $\Phi(t)$

Định lý (Cấu trúc nhân của các trường Galois)

Với một trường Galois $GF(q)$.

1. *Nếu t không phải là ước số của $q - 1$ thì trong $GF(q)$ không tồn tại phần tử nào có bậc là t.*
2. *Nếu t là ước số của $q - 1$ thì trong $GF(q)$ tồn tại $\Phi(t)$ phần tử có bậc là t.*

- $GF(q)$ có thể được biểu diễn bởi 0 và $q - 1$ lũy thừa liên tiếp của phần tử nguyên thủy $\alpha \in GF(q)$
- Phép nhân trong một trường Galois cấp là một số không nguyên tố có thể được thực hiện bằng cách biểu diễn các thành phần là số mũ của phần tử nguyên thủy α và cộng các số mũ đồng dư $q - 1$
- Trong $GF(q)$ có một trường con với cấp là một số nguyên tố, trường con này có phép cộng là phép cộng số nguyên đồng dư p
- Việc biểu diễn bởi các phần tử nguyên thủy có thể diễn tả cấu trúc cộng của toàn bộ trường.

Định nghĩa (Phần tử nguyên thủy)

Trong $GF(q)$, một phần tử có bậc $q - 1$ được gọi là phần tử nguyên thủy.

Hệ quả

Trong mọi trường $GF(q)$ tồn tại đúng $\Phi(q - 1)$ phần tử nguyên thủy

- Mọi trường $GF(q)$ có ít nhất một phần tử nguyên thủy α

Định lý

Mọi phần tử khác "0" trong $GF(q)$ có thể được biểu diễn bởi $(q - 1)$ lũy thừa liên tiếp của phần tử nguyên thủy (primitive) $\alpha \in GF(q)$

Các đa thức nguyên thủy và các trường Galois bậc p^m

Một số khái niệm và quy ước; Đa thức tối giản

- $GF(q)[x]$: tập tất cả các đa thức dạng $a_0 + a_1x + a_2x^2 + \cdots + x^n$.
  - Bậc bất kỳ, kí hiệu $deg()$.
  - Các hệ số là các phần tử của $GF(q)$.
  - $\Rightarrow$ $GF(q)[x]$ tạo thành một vành giao hoán có phần tử đơn vị.
  - Các phép toán cộng và nhân đa thức thực hiện một cách thông thường.
    - ⋆ Các phép toán với các hệ số đa thức được thực hiện trong trường mà các hệ số đó được lấy.

Định nghĩa (Đa thức tối giản - Irreducible Polynomial)

Một đa thức $f(x)$ được gọi là tối giản trong $GF(q)$ nếu $f(x)$ không thể phân tích thành tích của các đa thức bậc thấp hơn trong $GF(q)[x]$.

- Một đa thức có thể là tối giản trong vành đa thức này, nhưng có thể không tối giản trong vành đa thức khác.
- Mọi đa thức tối giản $f(x)$ bậc m trong vành $GF(p)[x]$ đều phải là thừa số của $x^{p^m-1} - 1$.

Các đa thức nguyên thủy và các trường Galois bậc p^m

Đa thức nguyên thủy

Định nghĩa (Đa thức nguyên thủy - Primitive polynomial)

Một đa thức tối giản $p(x) \in GF(p)[x]$ có bậc m được gọi là đa thức nguyên thủy nếu có một số nguyên dương nhỏ nhất $n = p^m - 1$ thỏa mãn $p(x)$ là một ước số của $x^n - 1$.

- Có $\Phi(2^n - 1)/n$ các đa thức nguyên thủy nhị phân bậc n.
- Một đa thức nguyên thủy $p(x) \in GF(p)[x]$ thì luôn là đa thức tối giản trong $GF(p)[x]$, điều ngược lại không chắc đúng.

Các đa thức nguyên thủy và các trường Galois bậc p^m

Đa thức nguyên thủy - Định lý về nghiệm

Định lý

Các nghiệm $\{\alpha_i\}$ của một đa thức nguyên thủy bậc m, $p(x) \in GF(p)[x]$, có cấp (order) $p^m - 1$.

- $\Rightarrow$ Nếu α có cấp $p^m - 1$ thì $p^m - 1$ lũy thừa liên tiếp của α sẽ tạo thành một nhóm nhân cấp $p^m - 1$
  - Phép nhân trong nhóm được thực hiện bằng cách cộng các lũy thừa của α đồng dư $p^m - 1$
  - $\Rightarrow$ Các biểu diễn lũy thừa có thể biểu diễn bởi dãy lũy thừa của α đồng dư đa thức nguyên thủy
- Các lũy thừa của α với bậc lớn hơn hoặc bằng m có thể biểu diễn dưới dạng một đa thức của α với bậc nhỏ hơn hoặc bằng $m - 1$.
- $ord(\alpha) = p^m - 1 \Rightarrow$ các lũy thừa của α phải có $p^m - 1$ đa thức khác không biểu diễn.
  - Các đa thức biểu diễn có dạng $b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{m-1}\alpha^{m-1}$, với $b_i \in GF(p)$
  - $\Rightarrow$ Có đúng $p^m - 1$ đa thức khác không phân biệt.

Các đa thức nguyên thủy và các trường Galois bậc p^m

Xây dựng trường mở rộng

- Tồn tại một ánh xạ $1 - 1$ giữa các lũy thừa phân biệt của α và các đa thức của nó với bậc $\leq m - 1$ với các hệ số $\in GF(p)$.
- $\Rightarrow$ $p^m - 1$ các đa thức đó và phần tử không tạo thành nhóm với phép cộng đa thức.
- $\Rightarrow$ $p^m - 1$ lũy thừa liên tiếp của α trở thành các phần từ khác không của trường $GF(p^m)$
- $\Rightarrow$ Các nghiệm của một đa thức nguyên thủy bậc m trong vành $GF(p)[x]$ là các phần tử nguyên thủy trong trường $GF(p^m)$.

- Một vành đa thức $GF(q)[x]$ với phép đồng dư $f(x)$ được ký hiệu là $GF(q)[x]/f(x)$

Định lý

Nếu $p(x)$ là một đa thức tối giản trong $GF(q)[x]$ thì $GF(q)[x]/p(x)$ là một trường.

- Vành $GF(p)[x]/(x^l - 1)$ chứa các lớp đa thức tương đương trong đó mỗi lớp có chứa một đa thức có bậc $\leq l$ hoặc phần tử 0
  - Mỗi lớp tương đương được gán nhãn là một đa thức có bậc nhỏ nhất trong lớp.
  - Vành $GF(p)[x]/(x^l - 1)$ có cấu trúc cao với các ideal cấu thành.
  - Vành $GF(p)[x]/(x^l - 1)$ có ứng dụng quan trọng trong xây dựng mã vòng (mã cyclic, mã xyclic).

Định nghĩa (Ideal)

Xét R là một vành. Một tập con không rỗng $I \subseteq R$ là một ideal nếu thỏa mãn:

1. *I là một nhóm đối với phép cộng trong R.*
2. $a \times r = b \in I$ $\forall a \in I$ và $\forall r \in R$.

Định nghĩa (Ideal chính - Principal Ideal)

Một ideal I trong vành R được gọi là Ideal chính nếu tồn tại một phần tử $g \in I$ sao cho mọi phần tử $c \in I$ có thể được biểu diễn là tích của $m \times g$ với một giá trị $m \in R$ nào đó.

- g được sử dụng để diễn tả tất cả các phần tử trong ideal chính.
- g thường được gọi là phần tử sinh (generator element).
- Ideal tạo bởi g được ký hiệu là $< g >$
- Các Ideal trong vành $GF(p)[x]/(x^l - 1)$ định ra các mã vòng tuyến tính.

Nhận xét

- Phép cộng trong $GF(p^m)$ được thực hiện bằng cách thay thế các lũy thừa bậc $\geq m$ bởi các đa thức và thực hiện phép cộng thông thường trong $GF(p)$.
- Phép nhân cũng được thực hiện một cách thông thường với chú ý kết quả thực hiện lấy modulo với $p(\alpha)$.
  - HOẶC $\alpha^a \times \alpha^b = \alpha^{(a+b) \bmod (p^m-1)}$
- **Chú ý**: Việc sử dụng nhãn là các số nguyên có thể dễ gây hiểu lầm vì chúng không đại diện các số nguyên trong trường hợp tổng quát.
- $GF(p^m)$ có thể coi như một không gian véc-tơ trên $GF(p)$
  - Phép cộng trong $GF(p^m)$ trở thành phép cộng véc-tơ trong $GF(p)$.
  - $GF(p^m) \supset GF(p)$: $GF(p^m)$- trường mở rộng của trường cấp nguyên tố p, $GF(p)$- trường con, trưởng cơ sở cấp nguyên tố.
  - $GF(p^m)$ có thể chứa nhiều trường con (subfield) khác ngoài $GF(p)$.
    - $GF(p^m)$ chứa tất cả các trường $GF(p^b)$, với b là ước số của m

Định lý

Một phần tử $\beta \in GF(q^m)$ thuộc trường con $GF(q)$ nếu và chỉ nếu $\beta^q = \beta$

- Một cách tổng quát, có thể biểu diễn $GF(q^m)$ như là một không gian con m-chiều trên $GF(q)$, trong đó $GF(q)$ là một trường con của $GF(q^m)$ có cấp là lũy thừa của một số nguyên tố.

Zech's logarithms

1. Kết hợp tất cả các phần tử có cùng lũy thừa bằng cách sử dụng phép cộng đồng dư của các lũy thừa (tức là phép cộng $GF(p)$)
2. Sắp xếp biểu thức kết quả $\alpha^a + \alpha^b + \cdots + \alpha^z$ theo thứ tự lũy thừa giảm dần.
3. Phân tích biểu thức kết quả thành dạng $(\ldots(((\alpha^{a-b} + 1)\alpha^{b-c} + 1)\alpha^{c-d} + 1)\ldots)\alpha^z$. Tổng thu được bây giờ có thể thực hiện được một chuỗi các phép cộng-một và các phép nhân trong trường Galois.

Định lý

I là một ideal trong $GF(q)[x]/(x^n - 1)$ thì những khẳng định sau là đúng:

1. *Tồn tại một đa thức monic (đa thức có hệ số bậc cao nhất bằng 1) $g(x) \in I$ với bậc tối thiểu.*
2. *I là một ideal chính với phần tử sinh $g(x)$.*
3. *$g(x)$ là ước của $x^n - 1$ trong $GF(q)[x]$.*

Kết thúc phần Kiến thức Đại số Cơ sở cho Lý thuyết mã