



## 第六章 有限域

信息与软件工程学院

电子科技大学

# 内容安排

- 6.1 域和扩域
- 6.2 有限域的结构
- 6.3 不可约多项式的根，迹和范数
- 6.4 有限域上元素的表示
- 6.5 有限域中的算法



## 6.1 域和扩域

- 定义6.1.1 一个有限域 $F$ 是指只含有限个元素的域， $F$ 的阶是指 $F$ 中元素的个数。有限域又称为Galois域。若域 $F$ 的阶为 $n$ ，则可将 $F$ 记为 $F_n$ 或 $GF(n)$ 。

定义6.1.2 设 $F$ 是域， $K$ 是 $F$ 的子集。如果 $K$ 在 $F$ 的运算下也构成一个域，则称 $K$ 为 $F$ 的子域，称 $F$ 为 $K$ 的扩域。特别地，如果 $K \neq F$ ，则称 $K$ 为 $F$ 的真子域。一个域如果不包含真子域，则称该域为素域。

例6.1.1 有理数域和阶为素数 $p$ 的有限域 $Z_p$ 都是素域。



# 素域的结构

- 定理6.1.1 特征为素数 $p$ 的域 $F$ 的素子域同构于 $\mathbb{Z}_p$ ；特征为0的域 $F$ 的素子域同构于有理数域。

证明：设 $P$ 是 $F$ 的素子域，则 $0, 1 \in P$ 。

当 $F$ 的特征为素数 $p$ 时，因为 $\{0, 1\} \subset P$ ，所以 $\{m \cdot 1 \mid m \in \mathbb{Z}\} \subset P$ 。构造映射

$$\phi: \mathbb{Z} \rightarrow P: m \mapsto m \cdot 1.$$

容易验证 $\phi$ 是一个环同态映射，且 $\ker \phi = \langle p \rangle$ 。所以 $\mathbb{Z}_p = \mathbb{Z} / \langle p \rangle = \mathbb{Z} / \ker \phi \cong \phi(\mathbb{Z}) \subset P$ 。又由于 $\mathbb{Z}_p$ 是域， $P$ 又没有真子域，因此 $\mathbb{Z}_p \cong \phi(\mathbb{Z}) = P$ 。

## ○ 证明（续）

当  $F$  的特征为  $0$  时，因为  $\{0,1\} \subset P$ ，所以  
 $\{(m \cdot 1)(n \cdot 1)^{-1} \mid m, n \in Z\} \subset P$ 。构造映射

$$\phi: Q \rightarrow P: m/n \mapsto (m \cdot 1)(n \cdot 1)^{-1}$$

容易验证  $\phi$  是一个环的单同态映射。所以  
 $Q \cong \phi(Q) \subset P$ 。又由于  $Q$  是域， $P$  又没有真子域，  
因此  $Q \cong \phi(Q) = P$ 。定理得证。



# 扩域、单扩域

- **定义6.1.3** 设 $F$ 是一个域， $E$ 是 $F$ 的扩域， $S \subseteq E$ ，将 $E$ 中既包含 $F$ 又包含 $S$ 的最小子域记为 $F(S)$ ，称之为由 $S$ 生成的 $F$ 的扩域。 $F(S)$ ： $E$ 中全体既包含 $F$ 又包含 $S$ 的子域的交集。

➤ 域  $F(S)$  也称为由域  $F$  添加  $S$  的元素所生成的扩域。

若  $S$  有限 且  $S = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ ，我们记  $F(S) = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ 。如果  $S$  仅含一个元  $\alpha$ ，则称  $F(\alpha)$  为  $F$  的**单扩域**。



# 扩域、单扩域

➤  $F(S)$  中的元素形如  $\frac{f(\alpha_1, \alpha_2, \dots, \alpha_n)}{g(\alpha_1, \alpha_2, \dots, \alpha_n)}$ ，其中  $f(\alpha_1, \alpha_2, \dots, \alpha_n), g(\alpha_1, \alpha_2, \dots, \alpha_n) \in F[\alpha_1, \alpha_2, \dots, \alpha_n]$ ，且  $g(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0$ 。其中， $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$  是  $S$  的有任意有限子集。

多元多项式：

$$f(x_1, x_2, \dots, x_n) = \sum_{i_1, i_2, \dots, i_n} a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

问题：记  $\mathbf{Q}(\sqrt{2})$  为  $\sqrt{2}$  生成的  $\mathbf{Q}$  的扩域。那么， $\mathbf{Q}(\sqrt{2})$  如何表示？



# 代数元

- 定义6.1.4 设 $K$ 是 $F$ 的一个子域,  $\alpha \in F$ , 如果  $\alpha$  是 $K$ 上的一个非零多项式的根, 则称  $\alpha$  为 $K$ 上的代数元。不是代数元的元素称为超越元。如果  $F$  的一个扩张中所有的元素都是  $F$  上的代数元, 则称该扩张为代数扩张。

问题: 1.  $\mathbb{Q}$  是  $\mathbb{R}$  的子域,  $\sqrt{2}$  是  $\mathbb{Q}$  的代数元还是超越元?  
2. 有没有  $\mathbb{Q}$  的超越元?





# 代数元

**定义 6.1.5** 设  $K$  是  $F$  的一个子域,  $\alpha \in F$ , 是  $K$  上的一个代数元, 则  $K[x]$  中满足  $f(\alpha) = 0$  的**次数最小**的多项式

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

称为  $\alpha$  在域  $K$  上的**极小多项式**, 该多项式的次数称为**代数元次数**

**例 6.1.2** 虚单位根  $i$  在实数域上的极小多项式为  $x^2 + 1$ ,

$\sqrt{2}$  在有理数域上的极小多项式为  $x^2 - 2$ 。



# 极小多项式的性质

**定理 6.1.2** 设  $K$  是  $F$  的一个子域,  $\alpha \in F$  是  $K$  上的一个代数元, 则  $\alpha$  的极小多项式  $f(x)$  满足如下性质:

(1)  $f(x)$  是不可约多项式;

(2) 令  $I = \{g(x) \in K[x] \mid g(\alpha) = 0\}$ , 则  $I$  是  $K[x]$  的理想, 且

$I = \langle f(x) \rangle$ 。



证明: (1) 不妨设  $f(x) = f_1(x)f_2(x)$ , 其中

$1 \leq \deg(f_1(x)), \deg(f_2(x)) < \deg(f(x))$ , 则有

$$f_1(\alpha)f_2(\alpha) = f(\alpha) = 0, \text{ 因而有 } f_1(\alpha) = 0 \text{ 或 } f_2(\alpha) = 0.$$

这与  $f(x)$  是  $\alpha$  的极小多项式矛盾。因此,  $f(x)$  是不可约多项式。

(2) 很显然, 对于任意多项式  $h(x), g(x) \in I$ , 有  $h(\alpha) - g(\alpha) = 0$ , 即有  $h(x) - g(x) \in I$  且对于任意多项式  $q(x) \in F[x]$ , 有  $q(\alpha)h(\alpha) = 0$ , 即有  $q(x)h(x) \in I$ 。所以  $I$  是  $K[x]$  的理想。根据  $f(x)$  的极小性, 不难验证  $I = \langle f(x) \rangle$ 。



# 向量空间（线性空间）

- **定义6.1.6** 设 $F$ 为域， $V$ 为交换加群，集合 $F \times V = \{ (a, v) \mid a \in F, v \in V \}$ 到 $V$ 有一个**映射**： $(a, v) \rightarrow av \in V$ 。假定**映射**满足下列条件，对任意 $a, b \in F, u, v \in V$ 有
  - (1)  $a(u + v) = au + av$
  - (2)  $(a + b)v = av + bv$
  - (3)  $a(bv) = (ab)v$
  - (4)  $1v = v$
- 则 $V$ 称为域 $F$ 上的**向量空间**。

例如： $\mathbb{R}^2$ （复数域 $\mathbb{C}$ ）为 $\mathbb{R}$ 上的向量空间。



# 向量空间（线性空间）

若存在  $v_1, v_2, \dots, v_n \in V$  使得对于任意  $v \in V$  都可唯一表示为  $v = a_1 v_1 + a_2 v_2 + \dots + a_n v_n$ ，其中  $a_i \in F$ ， $1 \leq i \leq n$ ，则称  $V$  为有限维向量空间， $v_1, v_2, \dots, v_n \in V$  称为  $V$  的一组基， $n$  是  $V$  的维数。



# 扩张次数

- 定义6.1.7 若 $E$ 是 $F$ 的扩域，则 $E$ 是 $F$ 上的向量空间。如果 $E$ 作为 $F$ 上的向量空间是有限维的，则称 $E$ 为域 $F$ 的有限扩域， $E$ 作为 $F$ 上的向量空间的维数称为扩张次数，记为 $[E:F]$ 。

问题： $\mathbb{R}^n$ 为 $n$ 维向量空间，则有 $[\mathbb{R}^n:\mathbb{R}] = n$ ；  
那有没有无限扩域的例子？

定理6.1.3 设 $E$ 是 $F$ 的有限扩域， $K$ 是 $E$ 的有限扩域，则有：

$$[K:F] = [K:E][E:F]$$

证明要点：利用基向量的线性无关性。



## 定理6.1.3的证明

**证明：** 假设  $[K : E] = m$  与  $[E : F] = n$  ,  $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$  是  $E$  在  $F$  上的一组基,  $\{\beta_1, \beta_2, \dots, \beta_m\}$  是  $K$  在  $E$  上的一组基, 于是  $K$  的任一元素  $\alpha$  可表示成为

$$\alpha = \sum_{i=1}^m \gamma_i \beta_i, \quad \gamma_i \in E, \quad \text{其中 } \beta_i = \sum_{j=1}^n r_{ij} \alpha_j, \quad r_{ji} \in F,$$

于是有

$$\alpha = \sum_{i=1}^m \gamma_i \beta_i = \sum_{i=1}^m \left( \sum_{j=1}^n r_{ij} \alpha_j \right) \beta_i = \sum_{i=1}^m \sum_{j=1}^n r_{ij} \alpha_j \beta_i.$$

这说明  $\{\alpha_j \beta_i \mid j = 1, 2, \dots, n; i = 1, 2, \dots, m\}$  可生成向量空间  $K$ 。



## 定理6.1.3的证明 (续)

下证,  $\{\alpha_j\beta_i \mid j=1,2,\cdots,n; i=1,2,\cdots,m\}$  是  $K$  在  $F$  上的一组基。

假设存在  $s_{ji} \in F, j=1,2,\cdots,n; i=1,2,\cdots,m$ , 使得

$$\sum_{i=1}^m \sum_{j=1}^n s_{ji} \alpha_j \beta_i = 0,$$

则

$$\sum_{i=1}^m \left( \sum_{j=1}^n s_{ji} \alpha_j \right) \beta_i = 0.$$





## 定理6.1.3的证明 (续)

由于  $\{\beta_1, \beta_2, \dots, \beta_m\}$  是  $\mathbf{K}$  在  $\mathbf{E}$  上的一组基, 所以有

$$\sum_{j=1}^m s_{ji} \alpha_j = 0, 1 \leq i \leq n,$$

又  $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$  是  $\mathbf{E}$  在  $\mathbf{F}$  上的一组基, 所以有

$$s_{ji} = 0, j = 1, 2, \dots, n; i = 1, 2, \dots, m.$$

于是,  $K$  作为  $F$  上的向量空间的维数为  $[K : F] = mn = [K : E][E : F]$ 。



# 代数扩张

○ 定理6.1.4 每个有限扩张都是代数扩张。

证明：设  $E$  是  $F$  的扩域， $[E:F] = n$ ，则对于任意  $\alpha \in E$ ， $n+1$  个元素  $1, \alpha, \alpha^2, \dots, \alpha^n$  一定线性相关。所以存在不全为零的元素

$a_i \in F, i = 0, 1, 2, \dots, n$ ，使得  $\sum_{i=0}^n a_i \alpha^i = 0$ 。因此， $\alpha$  满足多项式

$f(x) = \sum_{i=0}^n a_i x^i$ ，即  $\alpha$  是代数元。



# 代数扩张 (续)

**定理 6.1.5** 设  $\alpha$  是域  $F$  上代数元, 其极小多项式为  $p(x)$ ,  $\deg(p(x)) = n$ , 则

(1)  $F(\alpha) \cong F[x] / \langle p(x) \rangle$ ;

(2)  $[F(\alpha) : F] = n$ , 且  $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$  是  $F[\alpha]$  在  $F$  上的一组基。

**证明:** (1) 定义  $\phi : F[x] \rightarrow F(\alpha)$  如下:

$$\phi\left(\sum_{i=0}^k a_i x^i\right) = \sum_{i=0}^k a_i \alpha^i .$$

容易验证  $\phi$  是环同态映射, 且  $\ker \phi = \langle p(x) \rangle$ 。由同态基本定理可得

$$\phi(F[x]) \cong F[x] / \langle p(x) \rangle .$$



## 定理6.1.5 证明 (续)

因此,  $\phi(F[x]) \subseteq F(\alpha)$  是子域。又因为  $\phi(x) = \alpha \in \phi(F[x])$ , 所以有

$F(\alpha) \subseteq \phi(F[x])$ 。综上所述有  $F(\alpha) = \phi(F[x])$ , 从而有

$$F(\alpha) \cong F[x] / \langle p(x) \rangle.$$

(2) 由于  $F(\alpha) = \phi(F[x])$ , 所以对于任意  $\beta \in F(\alpha)$ , 存在  $f(x) \in F[x]$  使得  $f(\alpha) = \beta$ 。因为  $p(\alpha) = 0$ ,  $\deg(p(x)) = n$ , 根据带余除法可以找到次数小于  $n$  的  $f(x) \in F[x]$ , 满足  $f(\alpha) = \beta$ , 所以  $\beta$  可以表示成

$1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  的组合。



## 定理6.1.5 证明 (续)

下证  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  线性无关。若有  $a_i \in F, i = 0, 1, \dots, n-1$  使得

$$a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0,$$

则可得  $\alpha$  满足多项式  $f(x) = a_{n-1}x^{n-1} + \dots + a_1x + a_0$ ，但是  $\alpha$  的极小多项式的次数为  $n$ ，所以只有  $f(x) = 0$ ，从而有  $a_{n-1} = \dots = a_1 = a_0 = 0$ 。因此， $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  线性无关，即有  $[F(\alpha):F] = n$ ，且  $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$  是  $F[\alpha]$  在  $F$  上的一组基。

域的单代数扩张实际上是添加了一个不可约多项式的根的扩张。



# 分裂域

**定义 6.1.8** 设  $f(x) \in F[x]$  是一个  $n$  次多项式,  $E$  是  $F$  的一个扩域, 若

(1)  $f(x)$  在  $E$  上能够分解成一次因式的乘积, 即

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

其中,  $\alpha_i \in E, i = 1, \cdots, n, a \in F$ 。

(2)  $E = F(\alpha_1, \cdots, \alpha_n)$ ,

则称  $E$  是  $f(x)$  在  $F$  上的一个分裂域。

**例 6.1.3**  $x^2+1$  是实数域上的一个不可约多项式, 则复数域就是  $x^2+1$  在实数域上的一个分裂域。



## 分裂域 (续)

- 定理6.1.6 域 $F$ 上任意一个次数大于等于1的多项式在 $F$ 上都有分裂域。

证明：对  $f(x)$  的次数作归纳法。当  $\deg(f(x))=1$  时，  
 $f(x)=a(x-\alpha), \alpha \in F$ ，显然  $F$  本身是  $f(x)$  的一个分裂域。假设  
当  $\deg(f(x)) < n (n > 1)$  时， $f(x)$  有一个分裂域。当  $\deg(f(x)) = n$  时  
任取  $f(x)$  的一个不可约因式  $p(x)$ ，则存在一个单代数扩张  
 $E_1 = F(\alpha_1)$ ， $p(\alpha_1) = 0$ ，于是  $p(x)$  在  $E_1$  上可分解出一个一次因式，  
因而  $f(x)$  在  $E_1$  上至少可分解出一个一次因式。



## 分裂域 (续)

不妨设  $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r)f_1(x)$ ,  $f_1(x) \in E_1[x]$ ,  $\alpha_i \in E_1$ ,  $i = 1, \dots, r$ ,

$r \geq 1$ 。此时  $\deg(f_1(x)) < n$ 。若  $f_1(x)$  是常数, 则  $E_1$  就是  $f(x)$  的一个分裂域。若

$\deg(f_1(x)) \geq 1$ , 则根据归纳假设,  $f_1(x)$  在  $E_1$  有一个分裂域, 设为  $E$ 。于是

$$f_1(x) = c(x - \alpha_{r+1})(x - \alpha_{r+2}) \cdots (x - \alpha_n), \quad \alpha_i \in E_1, \quad i = r+1, \dots, n,$$

$$\begin{aligned} E &= E_1(\alpha_{r+1}, \dots, \alpha_n) = F(\alpha_1)(\alpha_{r+1}, \dots, \alpha_n) \\ &= F(\alpha_1, \dots, \alpha_r)(\alpha_{r+1}, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_n) \end{aligned}$$

所以  $E$  就是  $f(x)$  在  $F$  上的一个分裂域。

**定理 6.1.7** 设  $f(x) \in F[x]$ , 则  $f(x)$  在  $F$  上的任何两个分裂域是同构的。





## 6.2 有限域的结构

- 有限域的三条结构定理

- 定理6.2.1** 设 $F$ 是一个特征为素数 $p$ 的有限域，则 $F$ 中的元素个数为 $p^n$ ， $n$ 是一个正整数。
- 定理6.2.2**（**存在性**）对于任何素数 $p$ 和任意正整数 $n$ ，总存在一个有限域恰好含有 $p^n$ 个元素。
- 定理6.2.3**（**惟一性**）任意两个 $q=p^n$ 元域都同构，即 $p^n$ 元域在同构意义下是惟一的。



## 有限域中元素的个数

- 定理6.2.1 设 $F$ 是一个特征为素数 $p$ 的有限域，则 $F$ 中的元素个数为 $p^n$ ， $n$ 是一个正整数。

**证明：**由于 $F$ 的特征为 $p$ ，所以 $F$ 的素域与 $GF(p)$ 同构。又由于 $F$ 是一个有限域，因此 $F$ 是 $GF(p)$ 上的有限维向量空间，设其维数为 $n$ ，且 $\alpha_1, \alpha_2, \dots, \alpha_n$ 是 $F$ 在 $GF(p)$ 上的一组基，则

$$F = \{a_1\alpha_1 + a_2\alpha_2 + \dots + a_n\alpha_n \mid a_i \in GF(p), i = 1, 2, \dots, n\}$$

所以 $F$ 中的元素个数为 $p^n$ 。



## 有限域的存在性

- 定理6.2.2（存在性）对于任何素数 $p$ 和任意正整数 $n$ ，总存在一个有限域恰好含有 $p^n$ 个元素。

证明：考虑  $GF(p)$  上的多项式  $f(x) = x^q - x$ ，其中  $q = p^n$ 。  $f(x)$  的形式导数为

$$f'(x) = qx^{q-1} - 1 = -1,$$

因此  $f(x)$  和  $f'(x)$  互素，从而  $f(x)$  没有重根，即  $f(x)$  在其分裂域上有  $q$  个不同的根。

取  $F$  为  $f(x)$  在  $GF(p)$  上的分裂域。令  $S$  是  $F$  中多项式  $f(x)$  的所有根组成的集合容易验证  $S$  是  $F$  的子域，又  $f(x)$  在  $S$  中可分解成一次因式的乘积，所以  $S = F$ 。因此， $F$  是一个有  $q = p^n$  个元素的有限域。



## 有限域的唯一性

- 定理6.2.3 (唯一性) 任意两个 $q=p^n$ 元域都同构, 即 $p^n$ 元域在同构意义下是惟一的。

证明:  $F$  是具有  $q = p^n$  个元素的有限域, 则  $F$  的特征为  $p$ ,

且以  $GF(p)$  为其子域。所以  $F$  是  $GF(p)$  上的多项式  $x^q - x$  的

分裂域, 根据定理 6.1.7, 多项式的分裂域是同构的。因此,  $p^n$

元域都同构于  $GF(p)$  上的多项式  $x^q - x$  的分裂域。



## 有限域的乘法群

**定理 6.2.4** 设  $F_q$  是  $q$  元域，则其乘法群  $F_q^*$  是一个循环群。

**证明：**  $F_q^*$  的阶是  $q-1$ ，要证明  $F_q^*$  是一个循环群，只需要找到  $F_q^*$  中的一个  $q-1$  阶元素。

设  $q \geq 3$ ， $q-1 = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$  是  $q-1$  的标准分解。

对于任意  $i, 1 \leq i \leq t$ ，多项式  $x^{(q-1)/p_i} - 1$  最多有  $(q-1)/p_i$  个根，而  $(q-1)/p_i < q-1$ ，所以存在非零元  $a_i \in F_q^*$ ，使得  $a_i^{(q-1)/p_i} \neq 1$ 。令

$b_i = a_i^{(q-1)/p_i^{e_i}}$ ，则

$$b_i^{p_i^{e_i}} = 1$$



又  $b_i^{p_i^{e_i}-1} = a_i^{(q-1)/p_i} \neq 1$ , 所以  $b_i$  的阶为  $p_i^{e_i}$ 。令

$$b = b_1 b_2 \cdots b_t,$$

则  $b^{q-1} = 1$ 。因此,  $b$  的阶  $m$  是  $q-1$  的因子。若  $m$  是  $q-1$  的真因子, 则必然存在某个  $i$ , 使得  $m \mid (q-1)/p_i$ 。故

$$1 = b^{(q-1)/p_i} = b_1^{(q-1)/p_i} b_2^{(q-1)/p_i} \cdots b_t^{(q-1)/p_i}。$$

当  $j \neq i$  时, 有  $p_j^{e_j} \mid (q-1)/p_i$ , 从而  $b_j^{(q-1)/p_i} = 1$ , 所以有  $b_i^{(q-1)/p_i} = 1$ , 矛盾。所以

$m = q-1$ , 即  $b$  是  $q-1$  阶元。



# 本原元

○ 定义6.2.1  $F_q^*$  中的生成元成为  $F_q$  的本原元。

根据定理3.5.1,  $F_q$  中的本原元有  $\varphi(q-1)$  个。

例 6.2.1  $x^2 + x + 1$  是  $F_2$  上的不可约多项式, 设  $\alpha$  是  $x^2 + x + 1$  的根, 则

$$F_2(\alpha) = \{0, 1, \alpha, \alpha + 1\}$$

又  $\alpha^2 = \alpha + 1$ ,  $\alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha = 1$ , 所以  $\alpha$  是  $F_2(\alpha)$  的本原元。



# 本原多项式

**定义 6.2.2** 设  $K$  是  $F$  的一个子域,  $\alpha$  是  $F$  的本原元, 则  $\alpha$  在域  $K$  上的极小多项式称为本原多项式。

## $F_2$ 上的本原多项式

|                             |                                 |
|-----------------------------|---------------------------------|
| $x^2 + x + 1$               | $x^{11} + x^2 + 1$              |
| $x^3 + x + 1$               | $x^{12} + x^6 + x^4 + x + 1$    |
| $x^4 + x + 1$               | $x^{13} + x^4 + x^3 + x + 1$    |
| $x^5 + x^2 + 1$             | $x^{14} + x^{10} + x^6 + x + 1$ |
| $x^6 + x + 1$               | $x^{15} + x + 1$                |
| $x^7 + x^3 + 1$             | $x^{16} + x^{12} + x^3 + x + 1$ |
| $x^8 + x^4 + x^3 + x^2 + 1$ | $x^{17} + x^3 + 1$              |
| $x^9 + x^4 + 1$             | $x^{18} + x^7 + 1$              |
| $x^{10} + x^3 + 1$          | $x^{19} + x^5 + x^2 + x + 1$    |
|                             | $x^{20} + x^3 + 1$              |



## 有限域的子域

**定理 6.2.5** 设  $q = p^n$ ，其中  $p$  是素数， $n$  是正整数，则有限域  $F_q$  的任意一个子域含有  $p^m$  个元素，其中  $m \mid n$ ；反之，对于任意正整数  $m$ ，若  $m \mid n$ ，则  $F_q$  含有惟一一个子域包含  $p^m$  个元素。

**例 6.2.2**  $F_{2^{30}}$  域的子域完全由 30 的因子决定。30 的因子有 1, 2, 3, 5, 6, 10, 15, 30。因此  $F_{2^{30}}$  的子域有

$$F_2, F_{2^2}, F_{2^3}, F_{2^5}, F_{2^6}, F_{2^{10}}, F_{2^{15}}, F_{2^{30}}。$$



## 有限域的子域（续）

### ○ 定理6.2.5的证明：

证明：若  $K$  是  $F_q$  的一个子域，则  $K$  含有  $t = p^m$  个元素， $m \leq n$ 。又  $F_q$  是  $K$  的扩域，设  $[F_q : K] = s$ ，则  $q = t^s$  即  $p^n = p^{ms}$ ，所以  $m \mid n$ 。

反之，若  $m \mid n$ ，有  $p^m - 1 \mid p^n - 1$ ，进而  $x^{p^m} - x \mid x^{p^n} - x$ 。因此， $x^{p^m} - x$  在  $F_p$  上的分裂域是  $F_q$  的一个子域，且含有  $p^m$  个元素。假设  $F_q$  有两个的含有  $p^m$  个元素的子域，则这两个子域的元素都是  $x^{p^m} - x$  的根，而  $x^{p^m} - x$  只有  $p^m$  个不同的根，因此，这两个域一定相同。




## 6.3 不可约多项式的根，迹和范数

**定理 6.3.1** 设  $f(x) \in F_q[x]$  是一个不可约多项式， $\alpha$  是  $f(x)$  在  $F_q$  的某一扩域中的根，则对于  $F_q[x]$  中的多项式  $h(x)$ ，有  $h(\alpha) = 0$  当且仅当  $f(x) \mid h(x)$

**证明：** 设  $a \in F_q$  是  $f(x)$  的首项系数，令  $p(x) = a^{-1}f(x)$ 。

显然， $p(x)$  的首项系数为 1，且  $p(\alpha) = 0$ ，所以  $p(x)$  是  $\alpha$  的极小多项式。因此， $h(\alpha) = 0$  当且仅当  $p(x) \mid h(x)$  当且仅当  $f(x) \mid h(x)$ 。



**定理 6.3.2**  $f(x) \in F_q[x]$  是  $m$  次不可约多项式，则

$f(x) \mid x^{q^n} - x$  当且仅当  $m \mid n$ 。

**证明：**假设  $f(x) \mid x^{q^n} - x$ 。 $\alpha$  是  $f(x)$  在某一个分裂域中的根，则  $\alpha^{q^n} = \alpha$ ，所以  $\alpha \in F_{q^n}$ ，因此有  $F_q(\alpha) \subseteq F_{q^n}$ 。又由于  $[F_q(\alpha):F_q] = m$ ， $[F_{q^n}:F_q] = n$ ，根据定理 6.1.3 有  $m \mid n$ 。

反之，若  $m \mid n$ ，则  $F_{q^m}$  是  $F_{q^n}$  的子域。若  $\alpha$  是  $f(x)$  在某一个分裂域中的根，则有  $[F_q(\alpha):F_q] = m$ ，所以  $F_q(\alpha) = F_{q^m}$ 。因此  $\alpha \in F_{q^n}$ ，从而有  $\alpha^{q^n} = \alpha$ ，即  $\alpha$  是多项式  $x^{q^n} - x$  的根，根据定理 6.3.1，有  $f(x) \mid x^{q^n} - x$ 。



## 不可约多项式的根

**定理 6.3.3**  $f(x) \in F_q[x]$  是  $m$  次不可约多项式, 则  $f(x)$  有根  $\alpha \in F_{q^m}$ , 更进一步有,  $f(x)$  的所有根恰好为  $F_{q^m}$  中的  $m$  个元素  $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$ 。

**证明要点:** 由于  $m$  次多项式最多有  $m$  个根, 所以我们只需证明  $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$  是  $f(x)$  的根, 并且两两不同即可。



## 定理6.3.3的证明

假设  $\alpha$  是  $f(x)$  在某一个分裂域中的根, 则  $[F_q(\alpha):F_q]=m$ , 所以  $F_q(\alpha)=F_{q^m}$

$\alpha \in F_{q^m}$ 。考虑  $\alpha^q$ 。设  $f(x)=a_mx^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0$ , 其中  $a_i \in F_q$ ,

则

$$\begin{aligned}f(\alpha^q) &= a_m(\alpha^q)^m + a_{m-1}(\alpha^q)^{m-1} + \cdots + a_1(\alpha^q) + a_0 \\&= (a_m\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0)^q \\&= 0\end{aligned}$$

同理, 可依次证明  $\alpha^{q^2}, \cdots, \alpha^{q^{m-1}}$  都是  $f(x)$  的根。



## 定理6.3.3的证明 (续)

下证  $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$  两两不同。假设  $\alpha^{q^j} = \alpha^{q^k}$ ，其中  $0 \leq j < k \leq m-1$ ，则

$$(\alpha^{q^j})^{q^{m-k}} = (\alpha^{q^k})^{q^{m-k}}$$

因此有  $\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha$ ，从而由定理 6.3.1 可知， $f(x) \mid x^{q^{m-k+j}} - x$ 。

再由定理 6.3.2 可知  $m \mid m-k+j$ ，而  $m-k+j < m$ ，矛盾。所以

$\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$  两两不同。



# 共轭元与特征多项式

**定义 6.3.1** 设  $F_{q^m}$  是  $F_q$  的扩域,  $\alpha \in F_{q^m}$ , 称  $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$  为  $\alpha$  相对于  $F_q$  的**共轭元**。

**定义 6.3.2** 对于  $\alpha \in F_{q^m}$ , 定义多项式

$$f(x) = (x - \alpha)(x - \alpha^q) \cdots (x - \alpha^{q^{m-1}})$$

为  $\alpha$  在  $F_q$  上的**特征多项式**。





## 特征多项式

当  $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$  两两不同时,  $\deg(f(x)) = m$ , 此时  $\alpha$  的特征多项式与极小多项式  $p(x)$  相同。当  $\alpha$  仅有  $d$  个两两不同的共轭元  $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{d-1}}$  时,  $\alpha$  所有的共轭元正好是这  $d$  个共轭元重复  $m/d$  次。此时  $f(x) = (p(x))^{m/d}$ 。由此可知,  $\alpha$  在  $F_q$  上的特征多项式  $f(x) \in F_q[x]$ , 将其展开可得

$$f(x) = x^m - (\alpha + \alpha^q + \dots + \alpha^{q^{m-1}})x^{m-1} + \dots + (-1)^m \alpha \alpha^q \dots \alpha^{q^{m-1}}。$$



## 迹

**定义 6.3.3** 设  $\alpha \in E = F_{q^m}$  ,  $F = F_q$  , 定义  $\alpha$  的迹如下:

$$Tr_{E/F}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} ,$$

可简记为  $Tr(\alpha)$  。

**定理 6.3.4** 设  $E = F_{q^m}$  ,  $F = F_q$  ,  $\alpha, \beta \in E$  ,  $c \in F$  , 则迹函数  $Tr$

满足:

- (1)  $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$  ;
- (2)  $Tr(c\alpha) = cTr(\alpha)$  ;
- (3)  $Tr(c) = mc$  ;
- (4)  $Tr(\alpha^q) = Tr(\alpha)$  。



## 迹的应用

**例 6.3.1** 试证明有限域  $F_{2^n}$  上方程  $x^2 + x + \beta = 0$  有解的充要条件是  $Tr(\beta) = 0$ 。

**证明：**必要性。假设方程  $x^2 + x + \beta = 0$  有解，设为  $x_0$ ，则

$$\begin{aligned} Tr(0) &= Tr(x_0^2 + x_0 + \beta) \\ &= Tr(x_0^2) + Tr(x_0) + Tr(\beta) \\ &= Tr(x_0) + Tr(x_0) + Tr(\beta) \\ &= Tr(\beta) \end{aligned}$$

即  $Tr(\beta) = Tr(0) = 0$ 。



## 迹的应用（续）

充分性。设  $Tr(\beta) = 0$ ，分两种情况证明。

当  $n$  是奇数时，定义函数  $\tau: F_{2^n} \rightarrow F_{2^n}$  为

$$\tau(\beta) = \sum_{j=0}^{(n-1)/2} \beta^{2^{2j}}$$

则有

$$\begin{aligned}\tau(\beta)^2 + \tau(\beta) + \beta &= \sum_{j=0}^{(n-1)/2} \beta^{2^{2j+1}} + \sum_{j=0}^{(n-1)/2} \beta^{2^{2j}} + \beta \\ &= Tr(\beta) + \beta + \beta \\ &= Tr(\beta) \\ &= 0\end{aligned}$$

即当  $Tr(\beta) = 0$  时， $\tau(\beta)$  是方程  $x^2 + x + \beta = 0$  的一个根。可以验证  $\tau(\beta) + 1$  是方程  $x^2 + x + \beta = 0$  的另一个根。



## 迹的应用（续）

当  $n$  是偶数时，首先需要找到一个元素  $\delta \in F_{2^n}$ ， $\delta \neq 1$ ， $Tr(\delta) = 1$ 。找到这样的  $\delta$  后，

令

$$x_0 = \sum_{i=0}^{n-2} \left( \sum_{j=i+1}^{n-1} \delta^{2^j} \right) \beta^{2^i},$$

则当  $Tr(\beta) = 0$  时， $x_0$  和  $x_0 + 1$  就是方程  $x^2 + x + \beta = 0$  的两个根。因为

$$\begin{aligned} x_0^2 + x_0 &= \sum_{i=1}^{n-1} \left( \sum_{j=i+1}^{n-1} \delta^{2^j} \right) \beta^{2^i} + \sum_{i=0}^{n-2} \left( \sum_{j=i+1}^{n-1} \delta^{2^j} \right) \beta^{2^i} \\ &= \delta(\beta^{2^{n-1}} + \beta^{2^{n-2}} + \cdots + \beta^2) + (\delta^{2^{n-1}} + \delta^{2^{n-2}} + \cdots + \delta^2)\beta \\ &= \delta(Tr(\beta) + \beta) + (Tr(\delta) + \delta)\beta \\ &= \delta Tr(\beta) + \beta \end{aligned}$$

因此， $x_0$  是方程  $x^2 + x + \beta = 0$  的一个根。容易验证  $x_0 + 1$  也是方程  $x^2 + x + \beta = 0$  的根。

# 范数

**定义 6.3.3** 设  $\alpha \in E = F_{q^m}$ ,  $F = F_q$ , 定义  $\alpha$  的范数如下:

$$N_{E/F}(\alpha) = \alpha \alpha^q \cdots \alpha^{q^{m-1}},$$

可简记为  $N(\alpha)$ 。

**定理 6.3.5** 设  $E = F_{q^m}$ ,  $F = F_q$ ,  $\alpha, \beta \in E$ ,  $c \in F$ , 则范数函数  $N$  满足:

(1)  $N(\alpha\beta) = N(\alpha)N(\beta)$ ;

(2)  $N(c) = c^m$ ;

(4)  $N(\alpha^q) = N(\alpha)$ 。



## 6.4 有限域上元素的表示

### ○有限域上元素的三种表示方法：

- 多项式表示法
- 本原元表示法
- 伴随矩阵表示法



## 多项式表示法

设  $p$  是素数,  $q = p^n$ 。根据推论 5.3.1 可知, 只要找到  $F_p$  上一个  $n$  次不可约多项式  $f(x)$ , 就有

$$F_q = F_p[x] / \langle f(x) \rangle,$$

取  $f(x)$  的一个根  $\alpha$ , 根据定理 6.1.5,  $F_p(\alpha) \cong F_q$ , 且  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  是  $F_p[\alpha]$  在  $F_p$  上的一组基。因此,  $F_q$  中的元素可以表示成  $F_p$  上  $\alpha$  的次数小于  $n$  的多项式, 其上的加法为多项式的加法, 而乘法为模多项式  $f(\alpha)$  的乘法。





## 多项式表示法（续）

○ 例6.4.1 给出有限域 $F_9$ 的元素表示，并给出 $F_9$ 的乘法表。

解：  $F_9$  可以看成是  $F_3$  通过添加一个二次不可约多项式的根  $\alpha$  得到的 2 次扩张。

$f(x) = x^2 + 1$  是  $F_3$  上一个不可约多项式，设  $\alpha$  是  $f(x)$  的一个根，即

$f(\alpha) = \alpha^2 + 1 = 0$ ，则  $1, \alpha$  是  $F_9$  在  $F_3$  上的一组基，从而，  $F_9$  中的元素可以表示成  $F_3$  上  $\alpha$  的次数小于 2 的多项式，即

$$F_9 = \{0, 1, 2, \alpha, 1 + \alpha, 2 + \alpha, 2\alpha, 1 + 2\alpha, 2 + 2\alpha\}$$



## 多项式表示法 (续)

乘法表如下:

| *           | 0 | 1           | 2           | $\alpha$    | $1+\alpha$  | $2+\alpha$  | $2\alpha$   | $1+2\alpha$ | $2+2\alpha$ |
|-------------|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| 0           | 0 | 0           | 0           | 0           | 0           | 0           | 0           | 0           | 0           |
| 1           | 0 | 1           | 2           | $\alpha$    | $1+\alpha$  | $2+\alpha$  | $2\alpha$   | $1+2\alpha$ | $2+2\alpha$ |
| 2           | 0 | 2           | 1           | $2\alpha$   | $2+2\alpha$ | $1+2\alpha$ | $\alpha$    | $2+\alpha$  | $1+\alpha$  |
| $\alpha$    | 0 | $\alpha$    | $2\alpha$   | 2           | $2+\alpha$  | $2+2\alpha$ | 1           | $1+\alpha$  | $1+2\alpha$ |
| $1+\alpha$  | 0 | $1+\alpha$  | $2+2\alpha$ | $2+\alpha$  | $2\alpha$   | 1           | $1+2\alpha$ | 2           | $\alpha$    |
| $2+\alpha$  | 0 | $2+\alpha$  | $1+2\alpha$ | $2+2\alpha$ | 1           | $\alpha$    | $1+\alpha$  | $2\alpha$   | 2           |
| $2\alpha$   | 0 | $2\alpha$   | $\alpha$    | 1           | $1+2\alpha$ | $1+\alpha$  | 2           | $2+2\alpha$ | $2+\alpha$  |
| $1+2\alpha$ | 0 | $1+2\alpha$ | $2+\alpha$  | $1+\alpha$  | 2           | $2\alpha$   | $2+2\alpha$ | $\alpha$    | 1           |
| $2+2\alpha$ | 0 | $2+2\alpha$ | $1+\alpha$  | $1+2\alpha$ | $\alpha$    | 2           | $2+\alpha$  | 1           | $2\alpha$   |



## 本原元表示法

设  $\xi$  是  $F_q$  中的本原元, 则  $F_q = \{0, \xi, \xi^2, \dots, \xi^{q-1}\}$ 。在本原元表示下, 乘法很容易实现, 但加法需要结合  $F_q$  的多项式表示来计算。

**例 6.4.2** 设  $F_9 = F_3(\xi)$ , 其中  $\xi$  是  $F_9$  中的本原元, 且  $\xi$  是多项式

$x^2 + x + 2$  的根, 则有  $F_9 = \{0, \xi, \xi^2, \dots, \xi^8\}$ 。注意到, 若  $\alpha^2 + 1 = 0$ ,

则  $\xi = 1 + \alpha$  是多项式  $x^2 + x + 2$  的根, 可建立对应关系:  $\xi = 1 + \alpha$ ,

$\xi^2 = 2\alpha$ ,  $\xi^3 = 1 + 2\alpha$ ,  $\xi^4 = 2$ ,  $\xi^5 = 2 + 2\alpha$ ,  $\xi^6 = \alpha$ ,  $\xi^7 = 2 + \alpha$ ,

$\xi^8 = 1$ 。这样就可以很方便的计算  $F_9$  中的加法。



## 伴随矩阵表示法

设  $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ ，定义  $f(x)$  的伴随矩阵为

$$A = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}$$

经过计算有， $f(x) = |xI - A| = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ ，即  $f(x)$  是  $A$  的特征多项式。

因此， $f(A) = A^n + a_{n-1}A^{n-1} + \cdots + a_1A + a_0I = 0$ ，其中  $I$  是单位矩阵。所以  $A$  可以看作是  $f(x)$  的根。

利用上述结果可给出有限域中元素的伴随矩阵表示，其加法和乘法均为矩阵的加法和乘法。



## 伴随矩阵表示法（续）

例 6.4.3 设  $f(x) = x^2 + 1 \in F_3[x]$ ，其伴随矩阵为

$$A = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix},$$

所以  $F_9$  中的元素可以表示为  $F_9 = \{0, I, 2I, A, I + A, 2I + A, 2A, I + 2A, 2I + 2A\}$ ，其加法和乘法为矩阵的加法和乘法，如

$$(I + A) + A = I + 2A = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix},$$

$$A \cdot (I + 2A) = A + 2A^2 = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = A + I。$$



## 6.5 有限域中的算法

- 素域 $F_p$ 中的加法和乘法可由第二章介绍的模整数的加法和乘法来实现。求逆运算也可由算法2.5.1来实现。
- 根据 $F_{p^n}$ 中元素的多项式表示， $F_{p^n}$ 中元素的乘法和求逆运算都可以通过模 $F_p$ 上的不可约多项式来实现。

设  $f(x)$  是  $F_p$  上的  $n$  次不可约多项式，取  $\alpha$  为  $f(x)$  的根，设

$g(\alpha), h(\alpha) \in F_{p^n}$ ，则  $g(\alpha), h(\alpha)$  乘积可以这样得出，先将

$g(\alpha)h(\alpha)$  按照一般的多项式乘法求积，再以  $f(\alpha)$  去除得出余式，余式即为所求。




# 逆元的实现

---

**算法 6.5.1** 在  $F_{p^n}$  中计算乘法逆元

输入：非零多项式  $g(\alpha) \in F_{p^n}$  ( $F_{p^n}$  中的元素以  $f(x)$  的根  $\alpha$  的次数小于  $n$  的多项式形式表示，其中  $f(x) \in F_p[X]$  是  $Z_p$  上的次数为  $n$  的不可约多项式)；

输出：  $g(\alpha)^{-1} \in F_{p^n}$ ；

- 1、利用适用于多项式的扩展的欧几里得算法（算法 5.5.2）得出两个多项式  $s(\alpha), t(\alpha) \in F_p(\alpha)$ ，使得  $s(\alpha)g(\alpha) + t(\alpha)f(\alpha) = 1$ ；
  - 2、返回  $(s(\alpha))$ 。
- 

# 幂运算的实现（重复平方乘）

算法 6.5.2 适用于  $F_{p^n}$  中幂运算的重复平方乘算法

输入：  $g(\alpha) \in F_{p^n}$ ，整数  $0 \leq k \leq p^n - 1$  其二进制表示为  $k = \sum_{i=0}^t k_i 2^i$ 。

（  $F_{p^n}$  中的元素以  $f(x)$  的根  $\alpha$  的次数小于  $n$  的多项式形式表

示，其中  $f(x) \in F_p[X]$  是  $F_p$  上的次数为  $n$  的不可约多项式）

输出：  $g(\alpha)^k$





# 幂运算的实现（重复平方乘）

- 1、令  $s(\alpha) \leftarrow 1$ ，如果  $k = 0$ ，返回  $(s(\alpha))$ ；
- 2、令  $G(\alpha) \leftarrow g(\alpha)$ ；
- 3、如果  $k_0 = 1$ ，则令  $s(\alpha) \leftarrow g(\alpha)$ ；
- 4、对  $i$  从 1 到  $t$ ，作
  - 4.1 令  $G(\alpha) \leftarrow G(\alpha)^2 \bmod f(\alpha)$ ；
  - 4.2 如果  $k_i = 1$ ，则令  $s(\alpha) \leftarrow G(\alpha) \cdot s(\alpha) \bmod f(\alpha)$ ；
- 5、返回  $(s(\alpha))$ 。



## 有限域运算实现举例

**例 6.5.1** 考察阶为 16 的有限域  $F_{2^4}$ 。容易验证多项式  $f(x) = x^4 + x + 1$  在  $F_2$  上不可约。设  $\alpha$  是  $f(x)$  的一个根。因此有限域  $F_{2^4}$  可以表示为  $\alpha$  的所有  $F_2$  次数小于 4 的多项式集合，即

$$F_{2^4} = \{a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 \mid a_i \in \{0,1\}\}$$

为方便起见，多项式  $a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$  可以用长度为 4 的向量  $(a_3a_2a_1a_0)$  表示，且

$$F_{2^4} = \{(a_3a_2a_1a_0) \mid a_i \in \{0,1\}\}$$



## 有限域运算实现举例（续）

- 域  $F_{2^4}$  中算术的一些例子：
- （1）域中元素相加，即为对应分量的简单相加，例如  $(1011)+(1001)=(0010)$ ；
- （2）要将域中元素  $(1101)$  与  $(1001)$  相乘，将它们做多项式乘法，再模去  $f(\alpha)$  得到的乘积，取其余式：

$$\begin{aligned}(\alpha^3 + \alpha^2 + 1)(\alpha^3 + 1) &= \alpha^6 + \alpha^5 + \alpha^2 + 1 \\ &\equiv \alpha^3 + \alpha^2 + \alpha + 1 \pmod{f(\alpha)}\end{aligned}$$

- 因此  $(1101) \times (1001) = (1111)$ ；
- （3） $F_{2^4}$  的乘法单位元是  $(0001)$ ；
- （4） $(1011)$  的逆元是  $(0101)$ ，因为：

$$\begin{aligned}(\alpha^3 + \alpha + 1)(\alpha^2 + 1) &= \alpha^5 + \alpha^2 + \alpha + 1 \\ &\equiv 1 \pmod{f(x)}\end{aligned}$$

- 即  $(1011) \times (0101) = (0001)$ 。



# GF (256) 中运算的快速实现

域  $F_2$  上的 8 次不可约多项式  $f(x) = x^8 + x^6 + x^5 + x + 1$ ,  $\alpha$  是  $f(x)$  的一个根。因此有限域  $F_{2^8}$  可以表示为  $\alpha$  的所有  $F_2$  次数小于 8 的多项式集合, 即

$$F_{2^8} = \{a_7\alpha^7 + a_6\alpha^6 + a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 \mid a_i \in \{0, 1\}\}$$

定义一个由  $a_7a_6a_5a_4a_3a_2a_1a_0$  组成的字节  $a$  可表示为系数为  $\{0, 1\}$  的二进制多项式:

$$a_7\alpha^7 + a_6\alpha^6 + a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$$



## GF (256) 中运算的快速实现

- 还可以将每个字节表示为一个16进制数，即每4比特表示一个16进制数，代表较高位的4比特的符号仍在左边。例如，01101011可表示为6B。
- 也可以用0-255这256个十进制整数来表示域中的元素。
- 加法定义为二进制多项式的加法，且其系数模2
- 乘法定义为多项式的乘积模一个次数为8的不可约多项式。
- 元素“02”是域中的一个本原元。



## 乘法的两种方法

- 直接模多项式 $m(x)$ 
  - 需要64次GF(2)上乘法以及模多项式运算
- 建立乘法表
  - 需要 $256 \times 256$ 字节（64K）的存储空间
- 建立指数对数表
  - 512个字节的存储，每次乘法仅需要查表3次和1次加法



## 指数对数表的建立

- 域GF(256)中的元素用0-255这256个十进制整数来表示

(1) 将元素‘02’表示成为 $\alpha$ ，依次计算 $\alpha^i \bmod(f(\alpha))$ ， $i = 0, 1, \dots, 254$ ，将所得结果转变为十进制数，设为 $\beta_i$ ， $i = 0, 1, \dots, 254$ ；如下表所示：

(2) 建表。第一行为 $0, 1, \dots, 254, 255$ ，第二行元素依次为 $\beta_i$ ， $i = 0, 1, \dots, 254$ 。

由于 $\alpha^0 \equiv \alpha^{255} \bmod(f(\alpha))$ ，约定第2行，第255列元素为0。

|   |   |   |   |     |     |     |     |
|---|---|---|---|-----|-----|-----|-----|
| 0 | 1 | 2 | 3 | ... | 253 | 254 | 255 |
| 1 | 2 | 4 | 8 | ... | 233 | 177 | 0   |



## 指数对数表的建立（续）

（3）按所建表的第二行元素的大小进行重排列，如下表所示：

|            |          |          |            |            |            |            |            |
|------------|----------|----------|------------|------------|------------|------------|------------|
| <b>255</b> | <b>0</b> | <b>1</b> | <b>197</b> | <b>...</b> | <b>72</b>  | <b>230</b> | <b>104</b> |
| <b>0</b>   | <b>1</b> | <b>2</b> | <b>3</b>   | <b>...</b> | <b>253</b> | <b>254</b> | <b>255</b> |

（4）将（3）中表的第一行放在（2）中表的第三行，即

|                 |            |          |          |            |            |            |            |            |
|-----------------|------------|----------|----------|------------|------------|------------|------------|------------|
| 序号              | <b>0</b>   | <b>1</b> | <b>2</b> | <b>3</b>   | <b>...</b> | <b>253</b> | <b>254</b> | <b>255</b> |
| $(02)^i$        | <b>1</b>   | <b>2</b> | <b>4</b> | <b>8</b>   | <b>...</b> | <b>233</b> | <b>177</b> | <b>0</b>   |
| $\log_{(02)} i$ | <b>255</b> | <b>0</b> | <b>1</b> | <b>197</b> | <b>...</b> | <b>72</b>  | <b>230</b> | <b>104</b> |





## 指数对数表的使用

例 6.5.2 取  $F_2$  上的 8 次不可约多项式  $f(x) = x^8 + x^6 + x^5 + x + 1$

$\alpha$  是  $f(x)$  的一个根。试求  $F_{2^8}$  中元素  $\alpha+1$  和

$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1$  的乘积，并计算  $\alpha+1$  的逆元。

解：  $\alpha+1$  对应于 “03”，  $\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1$  对应于 “253”。通过查指数对数表可得  $03 = (02)^{197}$ ，  $253 = (02)^{72}$ ， 因此，

$$(03) \cdot (253) = (02)^{197+72(\bmod 255)} = (02)^{14} = 100。$$

“100” 对应于  $\alpha^6 + \alpha^5 + \alpha^2$ ， 即

$$(\alpha+1)(\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1) \equiv (\alpha^6 + \alpha^5 + \alpha^2) \pmod{f(\alpha)}$$



由  $03 = (02)^{197}$ ，而  $255 - 197 = 58$ ，所以  $(03)^{-1} = (02)^{58} = 222$ 。

“222” 对应于

$$\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha,$$

即  $(\alpha + 1)^{-1} \equiv (\alpha^7 + \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha) \bmod(f(\alpha))$ 。

## 实验内容

1. 实现 $2^8$ 域上元素的多项式基表示，实现模多项式的乘法运算和求逆运算，从而实现 $2^8$ 域上元素乘法运算和逆元运算。
2. 构造指数对数表，从而通过查表实现 $2^8$ 域上元素乘法运算和逆元运算。

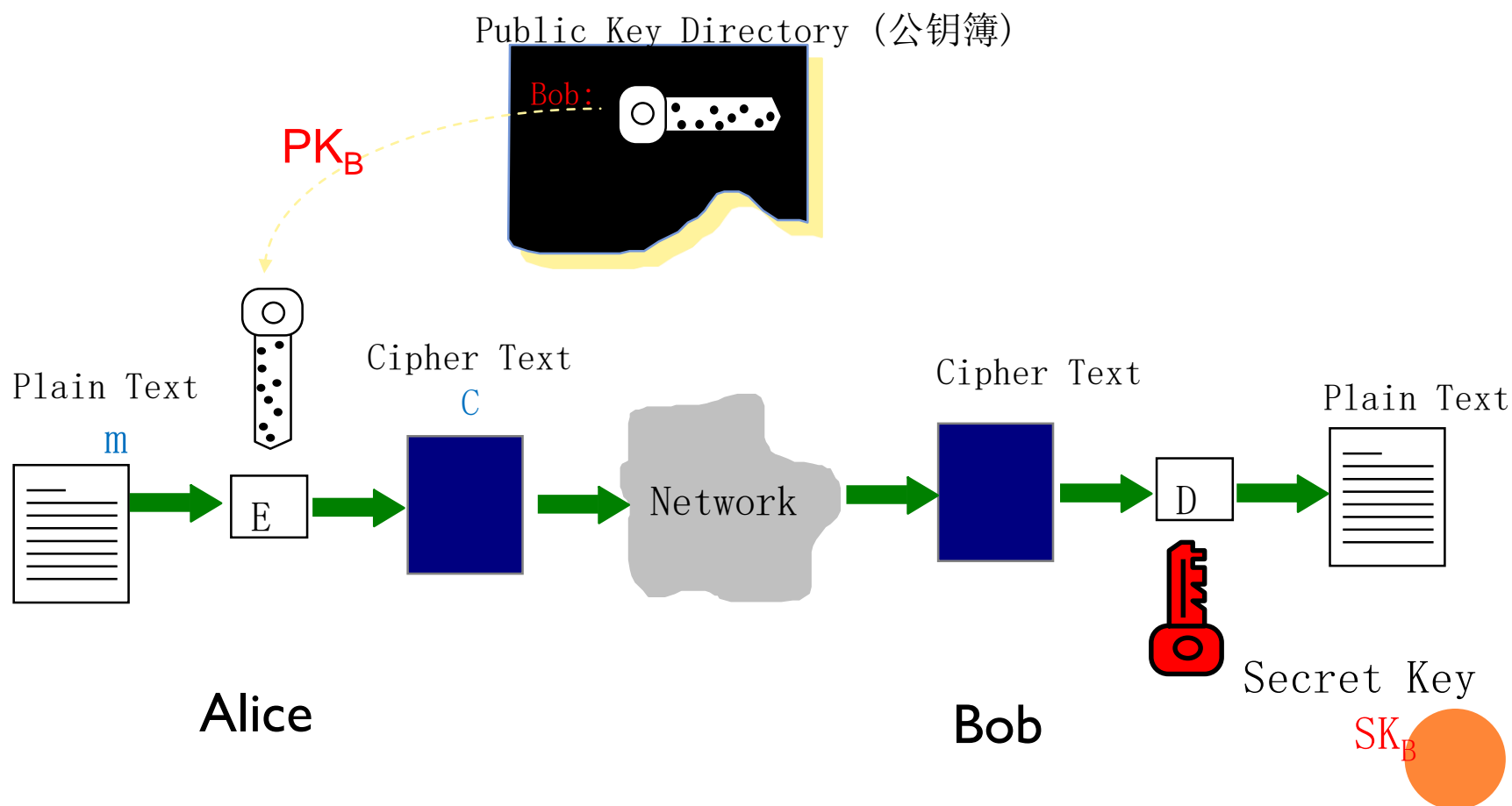


## 习题

- P95: 11, 20, 21



# 公钥密码体制的原理



# RSA

## 算法描述

- 选择两个素数 $p$ 和 $q$  ( $p \neq q$ );
- 计算出 $n = p * q$ ;
- 计算出 $f(n) = (p-1) * (q-1)$ ;
- 选择一个 $e$ 使得其与 $f(n)$ 互素,并且小于 $f(n)$ ;
- 确定 $d$ 使得 $de \equiv 1 \pmod{f(n)}$ 且 $d < f(n)$ ;

注: $f(n)$ 是Euler函数,即小于 $n$ 且与 $n$ 互素的正整数的个数.



# RSA

## RSA算法中要用到元素

- 两个素数: $p$ 和 $q$ ;(保密,选定的)
- $n=p*q$ ;(公开,计算得出的)
- $e, \gcd(f(n), e)=1; 1 < e < f(n)$ ;(公开,选定的)
- $d \equiv e^{-1} \bmod f(n)$ (保密,计算得出的)

公钥:  $PK_B=\{e, n\}$ ; 私钥:  $SK=\{d, n\}$



# RSA

## RSA的加密

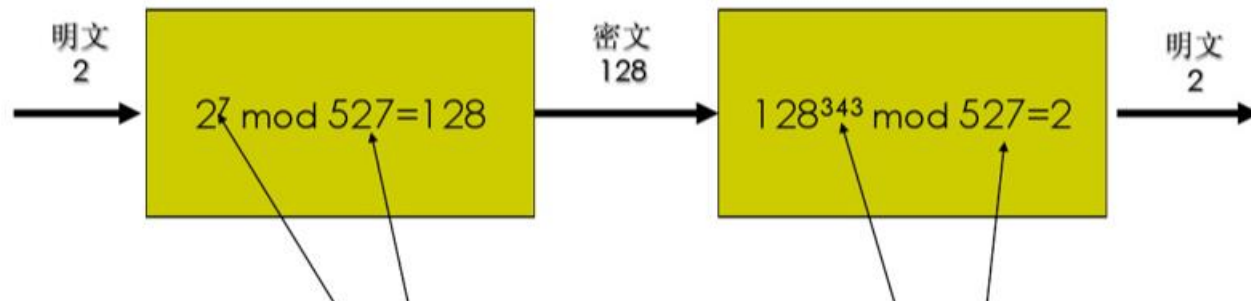
- 明文:  $M < n$
- 密文:  $C = M^e \pmod{n}$

## RSA的解密

- 明文:  $C$
- 密文:  $M = C^d \pmod{n}$

## RSA算法举例

$P=17, q=31, e=7, M=2, d=343;$



$PK_B = \{7, 527\}; \quad SK = \{343, 527\}$

# RSA

那么，已知 $p$ ， $q$ 和公钥（私钥）如何求私钥呢？

例如：  $p=7, q=13$ , 公钥 $e=5$ , 求私钥 $d$ ？





# RSA

## RSA的安全性

RSA的安全性主要是依赖于:

大素数的难于分解.

注:现今加密中 $p, q$ 的取值相当于十进制100位以上的大素数.

