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

AES加密算法都是在GF(2^n), 那么

1. 如何表示有限域的元素?

2. 如何定义加法和乘法?

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≠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 $\{m\cdot 1 \mid m\in Z\}\subset P$。构造映射

$$\phi: Z\to P: m\mapsto m\cdot 1.$$

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

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

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

容易验证 ϕ 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⊆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**。

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

扩域、单扩域

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

- 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 $S=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$，我们记 $F(S)=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$。如果 S 仅含一个元 α，则称 F(α) 为 F 的单扩域。

代数元

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

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

2. 有没有$\boldsymbol{Q}$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α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α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

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

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

这与 $f(x)$ 是 α 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 $\boxed{\text{任意多项式}\,h(x),g(x)\in I}$，有 $h(\alpha)-g(\alpha)=0$，即有 $\boxed{h(x)-g(x)\in I}$ 且对于 $\boxed{\text{任意多项式}\ q(x)\in F[x]}$， 有 $q(\alpha)h(\alpha)=0$，即有 $\boxed{q(x)h(x)\in I}$。所以 I 是是 $K[x]$ 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**：$(a, v) \to av \in V$。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：$\mathbb{R}^{\mathbf{2}}$（复数域$\boldsymbol{C}$）为$\mathbb{R}$上的向量空间。

向量空间（线性空间）

若存在 $v_1, v_2, \cdots, v_n \in V$ 使得对于任意 $v \in V$ 都可唯一表示为 $v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$，其中, $a_i \in F$，$1 \le i \le n$，则称 V 为有限维向量空间，$v_1, v_2, \cdots, v_n \in V$ 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$[E:F]=n$，$\boxed{\{\alpha_1,\alpha_2,\cdots,\alpha_n\}}$是 E 在 F 上的一组基，$\boxed{\{\beta_1,\beta_2,\cdots,\beta_m\}}$是 K 在 E 上的一组基，于是 K 的任一元素α可表示成为

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

于是有

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

这说明$\boxed{\{\alpha_j\beta_i\mid j=1,2,\cdots,n;i=1,2,\cdots,m\}}$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$\{\beta_1,\beta_2,\cdots,\beta_m\}$是 **K** 在 **E** 上的一组基，所以有

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

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

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

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 $1,\alpha,\alpha^2,\cdots,\alpha^n$ 一定线性相关。所以存在不全为零的元素 $a_i\in F, i=0,1,2,\cdots,n$，使得 $\sum_{i=0}^{n}a_i\alpha^i=0$。因此，$\alpha$ 满足多项式 $f(x)=\sum_{i=0}^{n}a_ix^i$，即 α 是代数元。

代数扩张（续）

定理 6.1.5 设α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$\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$是$F[\alpha]$在$F$上的一组基。

证明：（1）定义$\phi:F[x]\to F(\alpha)$如下：

$$\phi(\sum_{i=0}^{k}a_i x^i)=\sum_{i=0}^{k}a_i\alpha^i \text{ 。}$$

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

$$\phi(F[x])\cong F[x]/\langle p(x)\rangle \text{。}$$

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 β 可以表示成 $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ 的组合。

定理6.1.5 证明（续）

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

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

则可得α满足多项式$f(x)=a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，但是$\alpha$的极小多项式的次数为$n$，所以只有$f(x)=0$，从而有$a_{n-1}=\cdots=a_1=a_0=0$。因此，$1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$线性无关，即有$[F(\alpha):F]=n$，且$\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$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 $f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r)f_1(x)$，$f_1(x)\in E_1[x]$，$\alpha_i\in E_1$，$i=1,\cdots,r$，$r\geq 1$。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

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

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

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$\alpha_1,\alpha_2,\cdots,\alpha_n$是$F$在$GF(p)$上的一组基，则

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

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 （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。

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α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。

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$m|n$；反之，对于任意正整数m，若$m|n$，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

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

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，$m\le n$。又F_q是K的扩域，设$[F_q:K]=s$，则$q=t^s$即$p^n=p^{ms}$，所以$m|n$。

反之，若$m|n$，有$p^m-1|p^n-1$，进而$x^{p^m}-x|x^{p^n}-x$。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，α 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 α 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 $f(x)\mid x^{q^n}-x$。α 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 α 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 α 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 $\alpha,\alpha^q,\alpha^{q^2},\cdots,\alpha^{q^{m-1}}$。

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 $\alpha,\alpha^q,\alpha^{q^2},\cdots,\alpha^{q^{m-1}}$ 是 $f(x)$ 的根，并且两两不同即可。

定理6.3.3的证明

假设α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α^q。设$f(x)=a_m x^m+a_{m-1}x^{m-1}+\cdots+a_1 x+a_0$，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 $\alpha,\alpha^q,\alpha^{q^2},\cdots,\alpha^{q^{m-1}}$ 两两不同。假设 $\alpha^{q^j}=\alpha^{q^k}$，其中 $0\le j<k\le m-1$，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 $\alpha,\alpha^q,\alpha^{q^2},\cdots,\alpha^{q^{m-1}}$ 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 $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}$ 为 α 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 α 在 F_q 上的特征多项式。

特征多项式

当$\alpha,\alpha^q,\alpha^{q^2},\cdots,\alpha^{q^{m-1}}$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$\alpha,\alpha^q,\alpha^{q^2},\cdots,\alpha^{q^{d-1}}$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

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

迹

定义 6.3.3 设$\alpha \in E = F_{q^m}$， $F = F_q$，定义α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$\tau: F_{2^n} \to F_{2^n}$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δ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α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 α，根据定理 6.1.5，$F_p(\alpha)\cong F_q$，且 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 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 α 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$\mathbf{F_9}$的元素表示，并给出$\mathbf{F_9}$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α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 α 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α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	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
2	0	2	1	2α	$2+2\alpha$	$1+2\alpha$	α	$2+\alpha$	$1+\alpha$
α	0	α	2α	2	$2+\alpha$	$2+2\alpha$	1	$1+\alpha$	$1+2\alpha$
$1+\alpha$	0	$1+\alpha$	$2+2\alpha$	$2+\alpha$	2α	1	$1+2\alpha$	2	α
$2+\alpha$	0	$2+\alpha$	$1+2\alpha$	$2+2\alpha$	1	α	$1+\alpha$	2α	2
2α	0	2α	α	1	$1+2\alpha$	$1+\alpha$	2	$2+2\alpha$	$2+\alpha$
$1+2\alpha$	0	$1+2\alpha$	$2+\alpha$	$1+\alpha$	2	2α	$2+2\alpha$	α	1
$2+2\alpha$	0	$2+2\alpha$	$1+\alpha$	$1+2\alpha$	α	2	$2+\alpha$	1	2α

本原元表示法

设ξ是F_q中的本原元，则$F_q=\{0,\xi,\xi^2,\cdots,\xi^{q-1}\}$。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ξ是F_9中的本原元，且ξ是多项式x^2+x+2的根，则有$F_9=\{0,\xi,\xi^2,\cdots,\xi^8\}$。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：$\xi=1+\alpha$，$\xi^2=2\alpha$，$\xi^3=1+2\alpha$，$\xi^4=2$，$\xi^5=2+2\alpha$，$\xi^6=\alpha$，$\xi^7=2+\alpha$，$\xi^8=1$。这样就可以很方面的计算$F_9$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$\mathbf{F_p}$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$\boldsymbol{F_p}$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 α 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 α 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： $g(\alpha)^{-1}\in \mathbf{F}_{p^m}$；

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 $0 \le k \le p^n - 1$ 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 α 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 α 是 $f(x)$ 的一个根。因此有限域 F_{2^4} 可以表示为 α 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：

$$(\alpha^3+\alpha^2+1)(\alpha^3+1)=\alpha^6+\alpha^5+\alpha^2+1$$

$$\equiv \alpha^3+\alpha^2+\alpha+1(\bmod f(\alpha))$$

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

$$(\alpha^3+\alpha+1)(\alpha^2+1)=\alpha^5+\alpha^2+\alpha+1$$

$$\equiv 1(\bmod f(x))$$

- 即(1011) × (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 $f(x)=x^8+x^6+x^5+x+1$，α 是 $f(x)$ 的一个根。因此有限域 F_{2^8} 可以表示为 α 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256×256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α，依次计算$\alpha^i \bmod(f(\alpha))$，$i=0,1,\cdots,254$，将所得结果转变为十进制数，设为$\beta_i$，$i=0,1,\cdots,254$；如下表所示：

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

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**	$\cdots$	**253**	**254**	**255**
1	**2**	**4**	**8**	$\cdots$	**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：

255	0	1	197	···	72	230	104
0	1	2	3	···	253	254	255

（4）将（3）中表的第一行放在（2）中表的第三行，即

序号	0	1	2	3	···	253	254	255
$(02)^i$	1	2	4	8	···	233	177	0
$\log_{(02)} i$	255	0	1	197	···	72	230	104

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 $f(x)=x^8+x^6+x^5+x+1$

α 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，

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

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

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

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

“222”对应于

$$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha\text{，}$$

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**