第十三章 域的结构
2015年12月10日

信息安全数学基础

陈恭亮　教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

§13.1.1 超越基

定义13.1.1 设F 是域K 的扩域, $a_1, a_2, \ldots, a_n$ 是F 的一个n 个元素. $a_1, a_2, \ldots, a_n$ 叫做在K 上**代数相关**, 如果存在一个非零多项式$f \in \mathbf{K}[x_1, \ldots, x_n]$ 使得对于S 的n 个不同元素$a_1, a_2, \ldots, a_n$, 有

$$f(a_1, a_2, \ldots, a_n) = 0.$$

$a_1, a_2, \ldots, a_n$ 叫做**代数无关**, 如果$a_1, a_2, \ldots, a_n$ 不是代数相关.

注 所谓$a_1, a_2, \ldots, a_n$ 代数无关, 如果有多项式$f \in \mathbf{K}[x_1, \ldots, x_n]$ 使得

$$f(a_1, a_2, \ldots, a_n) = 0,$$

则$f = 0$.

例13.1.1 圆周率$\pi = 3.14\cdots$ 在Q 上代数无关, 自然对数底$e = 2.718\cdots$ 在Q 上也代数无关.

定理13.1.1 设**F** 是域**K** 的有限生成扩域, 则**F** 是**K** 的代数扩张或者存在代数无关元$\theta_1, \ldots, \theta_t$ 使得**F** 是$\mathbf{K}(\theta_1, \ldots, \theta_t)$ 的代数扩张.

证明 设**F** 在域**K** 的有限生成元为$S = \{a_1, a_2, \ldots, a_n\}$.

如果S 中的每个元素在**K** 上代数相关, 则**F** 是**K** 的代数扩张. 否则, S 中有元素在**K** 上代数无关, 设为θ_1. 我们用$\mathbf{K}(\theta_1)$ 代替**K** 作讨论.

如果S 中的每个元素在$\mathbf{K}(\theta_1)$ 上代数相关, 则**F** 是$\mathbf{K}(\theta_1)$ 的代数扩张.

否则, 如果S 中有元素在$\mathbf{K}(\theta_1)$ 上代数无关, 设为θ_2. 这时, θ_1, θ_2 代数无关. 如此继续下去, 可找到代数无关元$\theta_1, \ldots, \theta_t$ 使得**F** 是$\mathbf{K}(\theta_1, \ldots, \theta_t)$ 的代数扩张. 证毕

13.2 有限域的构造

设$\mathbf{F}_q$ 是q 元有限域, 其特征p 为素数. 则$\mathbf{F}_q$ 包含素域$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, 是$\mathbf{F}_p$ 上的有限维线性空间. 设$n = [\mathbf{F}_q : \mathbf{F}_p]$, 则$q = p^n$, 即$q$ 是其特征p 的幂.

我们要证明: $\mathbf{F}_q^* = \mathbf{F}_q \setminus \{0\}$ 是$q-1$ 阶循环乘群. 为此, 我们先讨论$\mathbf{F}_q^*$ 的一些性质.

定理13.2.1 $\mathbf{F}_q^*$ 的任意元a 的阶整除$q-1$.

证一 设$H =< a >$ 是a 生成的循环群, 根据定理8.2.2 之推论, 有

$$\mathrm{ord}(a) = |H| \mid |\mathbf{F}_q^*| = q-1.$$

证二 设$\mathbf{F}_q^* = \{a_1,\ a_2,\ \ldots, a_{q-1}\}$. 则 $a \cdot a_1,\ a \cdot a_2,\ \ldots, a \cdot a_{q-1}$ 是$a_1,\ a_2,\ \ldots, a_{q-1}$ 的一个排列, 因此

$$(a{\cdot}a_1)(a{\cdot}a_2)\cdots(a{\cdot}a_{q-1}) = a_1a_2\cdots a_{q-1} \quad 或 \quad a^{q-1}(a_1a_2\cdots a_{q-1}) = a_1a_2\cdots a_{q-1}.$$

两端右乘$(a_1a_2\cdots a_{q-1})^{-1}$, 得到$a^{q-1} = 1$. 类似于定理5.1.1 之证明, 我们有$\mathrm{ord}(a) \mid q-1$.

定义13.2.1 有限域$\mathbf{F}_q$ 的元素g 叫做**本原元** 或**生成元**, 如果它是$\mathbf{F}_q^*$ 的生成元, 即阶为$q-1$ 的元素. 当g 是$\mathbf{F}_q$ 的生成元时, 有

$$\mathbf{F}_q = \{0\} \cup < g >= \{0,\ g^0 = 1,\ g,\ \ldots,\ g^{q-2}\}.$$

这时, **本原元g 的定义多项式**叫做**本原多项式**.

注 此处本原多项式的表述与本原多项式的定义(定义11.5.1)是一致的. 因为在有限域$\mathbf{F}_q$ 上, 对于本原元g 的定义多项式$p_g(x)$, 序列

$$u(p_g(x)) = \{x^k \mod p_g(x) \mid k \in \mathbf{N}\}$$

的最小周期与序列

$$u(g) = \{g^k \mid k \in \mathbf{N}\}$$

的最小周期是一致的.

定理13.2.2 每个有限域都有生成元. 如果g 是$\mathbf{F}_q$ 的生成元, 则g^d 是$\mathbf{F}_q$ 的生成元的当且仅当d 和$q-1$ 的最大公因数$(d, q-1) = 1$. 特别地, $\mathbf{F}_q$ 有$\varphi(q-1)$ 个生成元.

证 设a 为阶为d 的元素, 则d 个数$a^0 = 1, a, \dots, a^{d-1}$ 两两不等, 且是方程: $x^d - 1 = 0$ 的所有根(因为其根都是单根). 根据定理13.2.1, $d \mid q-1$.

用$F(d)$ 表示模$\mathbf{F}_q$ 中阶为d 的元素个数, 我们有

$$\sum_{d \mid p-1} F(d) = p - 1.$$

因为阶为d 的元素b 满足方程$x^d - 1 = 0$, , 所以b 为a 的幂, 即$b = a^i$, $1 \le i \le d$. 根据定理9.1.5, a^i 的阶为d 的充要条件是$(i, d) = 1$. 故$F(d) = \varphi(d)$. 如果$\mathbf{F}_q$ 中没有阶为d 的元素, 则$F(d) = 0$. 总之, 有

$$F(d) \le \varphi(d).$$

但根据定理2.3.9, 我们又有 $\sum_{d \mid q-1} \varphi(d) = q - 1$.

这样,
$$\sum_{d|p-1}(\varphi(d)-F(d))=0.$$
因此, 对所有正整数$d \mid q-1$, 我们有
$$F(d)=\varphi(d).$$
特别, 我们有
$$F(q-1)=\varphi(q-1).$$
这说明存在阶为$q-1$的元素, 即$\mathbf{F}_q$ 中有生成元存在. 证毕

推论1 设$q=p^n$, p 为素数, $d \mid q-1$, 则有限域$\mathbf{F}_q$ 中有阶为d 的元素.

推论2 设p 为素数, 则存在整数g 遍历模p 的简化剩余系, 即存在模p 原根.

类似于模p 原根的构造方法(定理5.2.2)及本原多项式的构造方法(定理11.5.4), 也有有限域$\mathbf{F}_{p^n-1}$ 的本原元构造方法.

定理13.2.3 给定有限域$\mathbf{F}_{p^n}$, 其中p 为素数. 设p^n-1 的所有不同素因数是$q_1,\ \ldots,\ q_s$, 则g 是$\mathbf{F}_{p^n}$ 中本原元的充要条件是

$$g^{(p^n-1)/q_i} \neq 1, \quad i=1,\ldots,s. \tag{1}$$

证 设g 是$\mathbf{F}_{p^n}$ 的一个本原元, 则g 的阶是p^n-1. 因为

$$0<\frac{p^n-1}{q_i}<p^n-1, \quad i=1,\ldots,s.$$

所以(1) 成立, 即 $g^{(p^n-1)/q_i} \neq 1, \quad i=1,\ldots,s.$

反过来, 若g 满足(1), 但g 的阶$e=\mathrm{ord}(g)<p^n-1$. 则我们有$e \mid p^n-1$. 因而存在一个素数q_j 使得$q \mid \dfrac{p^n-1}{e}$. 即

$$\frac{p^n-1}{e}=u\cdot q_j, \quad \text{或} \quad \frac{p-1}{q_j}=u\cdot e.$$

进而 $g^{(p^n-1)/q_j}=(g^e)^u=1.$

与假设(1)矛盾. 证毕

定理13.2.4 如果$\mathbf{F}_q$ 是$q = p^n$ 元域, 则其每个元素满足方程

$$x^q - x = 0.$$

更确切地说, $\mathbf{F}_q$ 是这个方程的根集合.

反过来, 对每个素数幂$q = p^n$, 多项式$x^q - x$ 在$\mathbf{F}_p$ 上的分裂域是q 元域.

证 设$\mathbf{F}_q$ 是有限域. 根据定理13.2.1, $\mathbf{F}_q$ 的每个非零元的阶都是$q-1$ 的因子, 所以$\mathbf{F}_q$ 中的任意非零元满足方程$x^{q-1} = 1$. 两端同乘x, 就是方程$x^q = x$. 0 当然满足此方程. 因为方程$x^q - x = 0$ 的根的个数$\leq q$, 所以其全部根就是$\mathbf{F}_q$ 的元素. 这说明, $\mathbf{F}_q$ 是多项式$x^q - x$ 在$\mathbf{F}_p$ 上的分裂域.

反过来, 设$q = p^n$ 是素数幂, 且$\mathbf{F}$ 是多项式$x^q - x$ 在$\mathbf{F}_p$ 上的分裂域. 注意到$x^q - x$ 的导数$qx^{q-1} - 1 = -1$ (因为q 是p 的倍数, 所以qx^{q-1} 是$\mathbf{F}_p$ 中的零元). 因此, 多项式$x^q - x$ 与其导数没有公共根, 从而$\mathbf{F}$ 至少包含$x^q - x$ 的q 个不同根.

现在, 只需证明q 个根组成的集合构成一个域. 设a, b 是方程的两个根, 即

$$a^q = a, \quad b^q = b,$$

根据定理10.3.2, 有

$$(a+b)^p = a^p + b^p, \ (a+b)^{p^2} = (a^p + b^p)^p = a^{p^2} + b^{p^2}, \ \ldots,$$

$$(a+b)^{p^n} = (a^{p^{n-1}} + b^{p^{n-1}})^p = a^{p^n} + b^{p^n} = a + b,$$

又有$(ab)^{p^n} = a^{p^n} b^{p^n} = ab$, 这说明, $a + b$ 和ab 都是方程的根. 因此, q 个根组成的集合是包含$x^q - x$ 的根的最小域, 即$x^q - x$ 的分裂域是q 元域. 证毕

13.3 有限域的Galois 群

13.3.1 有限域的Frobenius 映射

先研究有限域上的Frobenius 映射.

定理13.3.1 设$\mathbf{F}_q$ 是$q = p^n$ 元有限域, 设σ 是$\mathbf{F}_q$ 到自身的映射,

$$\sigma : a \longmapsto a^p.$$

则σ 是$\mathbf{F}_q$ 的自同构, 且$\mathbf{F}_q$ 中在σ 下的不动元是素域$\mathbf{F}_p$ 的元素, 而σ 的n 次幂是恒等映射.

证 根据定理10.3.2 以及定理13.2.4 之证明, 我们有

$$\sigma(a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b),$$

$$\sigma(a\,b) = (a\,b)^p = a^p\,b^p = \sigma(a)\,\sigma(b).$$

因此, σ 是$\mathbf{F}_q$ 的自同构.

因为

$$\sigma^2(a)=\sigma(a^p)=a^{p^2},\ \ldots,\ \sigma^j(a)=\sigma(a^{p^{j-1}})=a^{p^j},\ \ldots,\ \sigma^n(a)=\sigma(a^p)=a^{p^n}=a,$$

所以σ^j 的不动元是$x^{p^j}-x$ 的根. 特别地, 当$j=1$ 时, σ 的不动元是x^p-x 的根, 这些根就是素域$\mathbf{F}_p$ 的p 个元素(根据定理2.4.2 (Fermat 小定理)). 而当$j=n$ 时, σ 的不动元是x^q-x 的根, 这些根就是域$\mathbf{F}_q$ 的所有q 个元素. 因此, σ^n 是恒等映射, σ 的逆映射是σ^{n-1}. 证毕

定理13.3.1 中的映射σ 叫做**Frobenius 自同构**.

推论1 设$\mathbf{F}_q$ 是$q=p^n$ 元有限域, 设$\sigma: a\longmapsto a^p$ 是$\mathbf{F}_q$ 到自身的映射, $\{\alpha_1,\alpha_2,\ldots,\alpha_d\}$ 是$\mathbf{F}_q$ 的子集, 且在σ 保持不变, 即$\{\sigma(\alpha_1),\sigma(\alpha_2),\ldots,\sigma(\alpha_d)\}$ 是$\{\alpha_1,\alpha_2,\ldots,\alpha_d\}$ 的一个置换, 则$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_d)$ 是$\mathbf{F}_p$ 上的多项式.

证 因为多项式f 的系数是$\alpha_1,\alpha_2,\ldots,\alpha_d$ 的对称多项式, 所以它们在σ 下保持不变, 即它们属于$I(<\sigma>)=\mathbf{F}_p$. 证毕

定理13.3.2 设$\mathbf{F}_q$ 是$q = p^n$ 元有限域, 设σ 是$\mathbf{F}_q$ 到自身的映射,

$$\sigma : a \longmapsto a^p.$$

如果α 是$\mathbf{F}_q$ 的任意元, 则α 在$\mathbf{F}_p$ 上的共轭元是元素$\sigma^j(\alpha) = \alpha^{p^j}$.

证 设$d = [\mathbf{F}_p(\alpha) : \mathbf{F}_p]$, 则$\mathbf{F}_p(\alpha)$ 可作为有限域$\mathbf{F}_{p^d}$(在同构意义下). 因此, α 满足$x^{p^d} = x$, 但不满足$x^{p^j} = x$, $1 \le j < d$. 由此, 并重复运用σ, 就得到d 个不同元 $\alpha,\ \sigma(\alpha) = \alpha^p,\ \ldots,\ \sigma^{d-1} = \alpha^{p^{d-1}}$.

断言: 这些元素是α 的定义多项式的全部根. 事实上, 设α 的定义多项式为

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0, \quad a_i \in \mathbf{F}_p,$$

则 $f(\alpha) = \alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0 = 0.$

两端作p 次方, 根据定理10.3.2, 并注意到$a_i^p = a_i$, $0 \le i < d$, (根据定理2.4.2 (Fermat 小定理)), 我们有

$$f(\alpha^p) = (\alpha^p)^d + a_{d-1}(\alpha^p)^{d-1} + \cdots + a_1\alpha^p + a_0 = f(\alpha)^p = 0.$$

依次继续作p 次方, 对于$1 \le j < d$, 我们有

$$f(\alpha^{p^j}) = (\alpha^{p^j})^d + a_{d-1}(\alpha^{p^j})^{d-1} + \cdots + a_1\alpha^{p^j} + a_0 = f(\alpha)^{p^j} = 0.$$

证毕

推论1 设$\mathbf{F}_q$ 是$q = p^n$ 元有限域, 设σ 是$\mathbf{F}_q$ 到自身的映射, $\sigma : a \longmapsto a^p$. 设$f(x)$ 是$\mathbf{F}_p$ 上d 次不可约多项式. 如果α 是$f(x)$ 在$\mathbf{F}_q$ 中的根, 则

$$\alpha,\ \sigma(\alpha) = \alpha^p,\ \ldots,\ \sigma^{d-1}(\alpha) = \alpha^{p^{d-1}}$$

是$f(x)$ 在$\mathbf{F}_q$ 中的全部根, 其中d 是使得$\sigma^d(\alpha) = \alpha$ 的最小正整数.

证 设e 是使得$\sigma^e(\alpha) = \alpha$ 成立的最小正整数. 则根据定理13.3.1 之推论,

$$g(x) = (x-\alpha)(x-\sigma(\alpha))\cdots(x-\sigma^{e-1}(\alpha))$$

是$\mathbf{F}_p$ 上的多项式. 因为$f(x)$ 是α 的定义多项式, 所以$f(x) \mid g(x)$. 从而, $d \le e$, 且$\alpha, \sigma(\alpha) = \alpha^p, \ldots, \sigma^{d-1}(\alpha) = \alpha^{p^{d-1}}$ 是$f(x)$ 的d 个不同根. 故结论成立. 证毕

推论2 设g 是$\mathbf{F}_q$ $(q = p^n)$ 的生成元(或原根). 对于整数u, $1 \le u \le q-2$, 设d 是使得$g^{up^d} = g^u$ 成立的最小正整数(这时$u = (p^n-1)/(p^d-1)$). 则

$$f(x) = (x-g^u)(x-g^{up})\cdots(x-g^{up^{d-1}})$$

是$\mathbf{F}_p$ 上的d 次不可约多项式.

有限域的具体构造. 应用定理11.4.4, 我们可以具体构造素域$\mathbf{F}_p$ 上的d 次代数扩张.

取$p(x)$ 为$\mathbf{F}_p[X]$ 中的d 次首一不可约多项式, 在商环$\mathbf{F}_p[x]/(p(x))$ 上定义加法:

$$f(x)+g(x)=((f+g)(x) \pmod{p(x)}),$$

和乘法:

$$f(x)g(x)=((fg)(x) \pmod{p(x)}).$$

则$\mathbf{F}_p[x]/(p(x))$ 对于上述运算法则构成一个域. 根据定理**??**, 这个域在$\mathbf{F}_p$ 上是d 次扩张. 我们记这个域为$\mathbf{F}_q$ 或$GF(q)$, 其中$q=p^d$.

$\mathbf{F}_2/(x^4+x+1)$ 的生成元是x,

例13.3.1 证明x^4+x+1 是$\mathbf{F}_2[x]$ 中的不可约多项式, 从而$\mathbf{F}_2[x]/(x^4+x+1)$ 是一个$\mathbf{F}_{2^4}$ 域.

因为$\mathbf{F}_2[x]$ 中的所有次数≤ 2 的不可约多项式为$x,\ x+1,\ x^2+x+1$, 且

$$\begin{aligned}x^4+x+1 &= x(x^3+1)+1,\\ x^4+x+1 &= (x+1)(x^3+x^2+x)+1,\\ x^4+x+1 &= (x^2+x+1)(x^2+x)+1,\end{aligned}$$

所以$x \nmid x^4+x+1,\ x+1 \nmid x^4+x+1,\ x^2+x+1 \nmid x^4+x+1$. 这说明, x^4+x+1 是$\mathbf{F}_2[x]$ 中的不可约多项式. 因此, $\mathbf{F}_2[x]/(x^4+x+1)$ 是一个$\mathbf{F}_{2^4}$ 域.

例13.3.2 求$\mathbf{F}_{2^4} = \mathbf{F}_2[x]/(x^4+x+1)$ 中的生成元$g(x)$，并计算$g(x)^t$，$t=0,1,\ldots,14$ 和所有生成元.

解 因为$|\mathbf{F}_{2^4}^*| = 15 = 3\cdot 5$, 所以满足

$$g(x)^3 \not\equiv 1 \pmod{x^4+x+1}, \quad g(x)^5 \not\equiv 1 \pmod{x^4+x+1}$$

的元素$g(x)$ 都是生成元.

对于$g(x)=x$, 有

$$x^3 \equiv x^3 \not\equiv 1 \pmod{x^4+x+1}, \quad x^5 \equiv x^2+x \not\equiv 1 \pmod{x^4+x+1},$$

所以$g(x)=x$ 是$\mathbf{F}_2[x]/(x^4+x+1)$ 的生成元.

对于$t=0,1,2,\ldots,14$, 计算$g(x)^t \pmod{x^4+x+1}$:

$$\begin{array}{lll}
g(x)^0 \equiv 1, & g(x)^1 \equiv x, & g(x)^2 \equiv x^2, \\
g(x)^3 \equiv x^3, & g(x)^4 \equiv x+1, & g(x)^5 \equiv x^2+x, \\
g(x)^6 \equiv x^3+x^2, & g(x)^7 \equiv x^3+x+1, & g(x)^8 \equiv x^2+1, \\
g(x)^9 \equiv x^3+x, & g(x)^{10} \equiv x^2+x+1, & g(x)^{11} \equiv x^3+x^2+x, \\
g(x)^{12} \equiv x^3+x^2+x+1, & g(x)^{13} \equiv x^3+x^2+1, & g(x)^{14} \equiv x^3+1.
\end{array}$$

所有生成元为$g(x)^t$, $(t,\varphi(15))=1$:

$$\begin{aligned} g(x)^1 &= x, & g(x)^2 &= x^2, \\ g(x)^4 &= x+1, & g(x)^7 &= x^3+x+1, \\ g(x)^8 &= x^2+1, & g(x)^{11} &= x^3+x^2+x, \\ g(x)^{13} &= x^3+x^2+1, & g(x)^{14} &= x^3+1. \end{aligned}$$

例13.3.3 求$\mathbf{F}_{2^8} = \mathbf{F}_2[x]/(x^8+x^4+x^3+x+1)$ 中的生成元$g(x)$.

解 因为$|\mathbf{F}_{2^8}^*| = 255 = 3\cdot 5\cdot 17$, 所以满足

$$g(x)^{15} \not\equiv 1,\ g(x)^{51} \not\equiv 1,\ g(x)^{85} \not\equiv 1 \pmod{x^8+x^4+x^3+x+1}$$

的元素$g(x)$ 都是生成元.

对于$g_1(x) = x$, 有

$$g_1(x)^{15} \equiv x^5+x^3+x^2+x+1, \qquad g_1(x)^{51} \equiv 1,$$
$$g_1(x)^{85} \equiv x^7+x^5+x^4+x^3+x^2+1 \pmod{x^8+x^4+x^3+x+1}.$$

因此, $g_1(x) = x$ 不是$\mathbf{F}_2[x]/(x^8+x^4+x^3+x+1)$ 中的生成元.

对于$g_2(x) = x + 1$, 有

$$
\begin{aligned}
&g_2(x)^2 \equiv x^2 + 1, && g_2(x)^3 \equiv x^3 + x^2 + x + 1,\\
&g_2(x)^4 \equiv x^4 + 1, && g_2(x)^7 \equiv x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,\\
&g_2(x)^8 \equiv x^4 + x^3 + x, && g_2(x)^{15} \equiv x^5 + x^4 + x^2 + 1,\\
&g_2(x)^{16} \equiv x^6 + x^4 + x^3 + x^2 + x + 1, && g_2(x)^{32} \equiv x^7 + x^6 + x^5 + x^2 + 1,\\
&g_2(x)^{48} \equiv x^6 + x^4 + x + 1, && g_2(x)^{51} \equiv x^3 + x^2,\\
&g_2(x)^{83} \equiv x^7 + x^6 + x^4, && g_2(x)^{85} \equiv x^7 + x^5 + x^4 + x^3 + x^2 + 1.
\end{aligned}
$$

因此,

$$g_2(x)^{15} \not\equiv 1, \quad g_2(x)^{51} \not\equiv 1, \quad g_2(x)^{85} \not\equiv 1 \pmod{x^8+x^4+x^3+x+1}.$$

$g_2(x) = x + 1$ 是$\mathbf{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$ 中的生成元.

定理13.3.3 $\mathbf{F}_{p^n}$ 的子域为$\mathbf{F}_{p^d}$, $(d \mid n)$, 它是$\mathbf{F}_{p^n}$ 中的元素在$\mathbf{F}_p$ 上生成的域.

证 设$\mathbf{K}$ 为$\mathbf{F}_{p^n}$ 的子域, 则存在$\alpha \in \mathbf{F}_{p^n}$ 使得

$$\mathbf{K} = \mathbf{F}_p(\alpha), \quad |\mathbf{K}| = p^d.$$

因为它们都是$\mathbf{F}_p$ 的扩域, 根据定理12.1.1, 我们有

$$[\mathbf{F}_{p^n} : \mathbf{F}_p] = [\mathbf{F}_{p^n} : \mathbf{F}_{p^d}][\mathbf{F}_{p^d} : \mathbf{F}_p].$$

反过来, 对任意的$d \mid n$, 有限域$\mathbf{F}_{p^d}$ 包含在$\mathbf{F}_{p^n}$ 中, 事实上, 方程

$$x^{p^d} = x$$

的任一解都是$x^{p^n} = x$ 的解. 证毕

定理13.3.4 对任意$q=p^n$, 多项式x^q-x 可在$\mathbf{F}_p[x]$ 中分解成首一不可约多项式的乘积, 且每个多项式的次数$d\mid n$.

证 设$f(x)$ 是任一次数为d 首一不可约多项式, 其根为α. 根据定理12.1.8 之推论, α 在$\mathbf{F}_p$ 上生成的域为$\mathbf{F}_p(\alpha)$, 其可作为$\mathbf{F}_{p^d}$, 包含在$\mathbf{F}_{p^n}$. 因为α 满足$x^q-x=0$, 所以$f(x)\mid x^q-x$. 因而, $f(x)$ 在$\mathbf{F}_q$ 中有根, 且$f(x)$ 的次数$d\mid n$. (因为$\mathbf{F}_p(\alpha)$ 是$\mathbf{F}_q$ 的子域). 因此, 所有整除x^q-x 的首一不可约多项式的次数$d\mid n$. 因为x^q-x 没有重根, 这蕴含着x^q-x 是所有这样的不可约多项式的乘积. 证毕

推论 如果n 是素数, 则$\mathbf{F}_{p^n}[x]$ 中有$\dfrac{p^n - p}{n}$ 个不同的次数为n 的首一不可约多项式的乘积.

证: 设m 是$\mathbf{F}_{p^n}[x]$ 中次数为n 的首一不可约多项式的个数.
根据定理13.3.4, 次数为p^n 的多项式$x^{p^n} - x$ 是m 个次数为n 的多项式和p 个次数为1 的不可约多项式$x - a,\ a \in \mathbf{F}_p$ 的乘积(因为n 是素数). 由此得到方程$p^n = mn + p$. 证毕

定理13.3.5 设p, r 都是素数. 则在$\mathbf{F}_p$ 上, 多项式$\dfrac{x^r-1}{x-1}$ 可分解为次数为$\mathrm{ord}_r(p)$ 的不可约多项式的乘积.

证 设$d=\mathrm{ord}_r(p)$, $Q_r(x)=\dfrac{x^r-1}{x-1}$. 设$Q_r(x)$ 有一个次数为t 的不可约因式$h(x)$, 根据定理11.4.4 及定理11.5.1, $\mathbf{F}_p[x]/(h(x))$ 构成一个p^k 元域. 根据定理13.2.2, $\mathbf{F}_p[x]/(h(x))$ 有一个生成元, 设为$g(x)$. 根据定理10.3.3, 在$\mathbf{F}_p[x]$ 上, 有

$$g(x)^p=g(x^p),\ g(x)^{p^2}=g(x^p)^p=g(x^{p^2}),\ \ldots,\ g(x)^{p^d}=g(x^{p^{d-1}})^p=g(x^{p^d}).$$

因为$p^d\equiv 1 \pmod r$, 根据例11.4.3, 在$\mathbf{F}_p[x]$ 上, 有

$$g(x^{p^d})\equiv g(x) \pmod{x^r-1},$$

进而,

$$g(x)^{p^d}\equiv g(x) \pmod{h(x)}.$$

这就是说, 在$\mathbf{F}_p[x]/(h(x))$ 中, 有

$$g(x)^{p^d-1}=1.$$

因为(p^k-1) 是$g(x)$ 在$\mathbf{F}_p[x]/(h(x))$ 中的阶, 根据定理9.1.3 (iv), 我们得到$(p^k-1)|(p^d-1)$.
另一方面, 因为$h(x)|x^r-1$, 所以在$\mathbf{F}_p[x]/(h(x))$ 中恒有

$$x^r-1=0.$$

这说明x 是$\mathbf{F}_p[x]/(h(x))$ 中阶为r 的元素(因为r 是素数, $x\neq 1$.) 因此, $r|(p^k-1)$, 即$p^k\equiv 1 \pmod r$. 根据定理5.1.1, 我们得到$d|k$. 故$d=k$. 结论成立. 证毕

定理13.3.6 设p 是素数, m 是正整数. 则$x^{p^m}-x$ 在$\mathbf{F}_p$ 上可分解成两两不同的不可约多项式$p_0(x)=x$, $p_i(x)$, $1\le i\le s$ 的乘积,

$$x^{p^m}-x=x\prod_{i=1}^{s}p_i(x)=\prod_{i=0}^{s}p_i(x).$$

推论1 在定理的假设条件下, 设$p_i(x)$ 在$\mathbf{F}_{p^m}$ 的全部根集为$E_i=\{\alpha_1^{(i)},\alpha_2^{(i)},\ldots,\alpha_{n_i}^{(i)}\}$ $(0\le i\le s)$. 则我们有E_i 两两不交, 且

$$E_0\cup E_1\cup\cdots\cup E_s=\mathbf{F}_{p^m}.$$

应用1 求多项式$f(x)$ 在$\mathbf{F}_{p^m}$ 的全部根集X .

方法一 直接在$\mathbf{F}_{p^m}$ 中穷尽所有元素, 以找出全部根集X.

方法二 对每个$1 \le i \le s$, 直接在E_i 中穷尽所有元素, 以找出全部根集$X_i = X \cap E_i$. 从而得到

$$X_0 \cup\ X_1 \cup \cdots \cup X_s = X.$$

13.3.2 有限域的Galois 群

定理13.3.7 $\mathbf{F}_{q^n}$ 在$\mathbf{F}_q$ 上的自同构集是一个阶为n 的循环群, 其生成元为自同构$\sigma_q(\alpha)=\alpha^q$.

证 设β 是$\mathbf{F}_{q^n}$ 中的本原元, 则β 在$\mathbf{F}_q$ 上的阶为q^n-1, 且其最小多项式$p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbf{F}_q[x]$ 有根

$$\beta,\ \sigma_q(\alpha)=\beta^q,\ \sigma_q^2(\alpha)=\beta^{q^2},\ \ldots,\ \sigma_q^{n-1}(\alpha)=\beta^{q^{n-1}}.$$

现在, 设$f(x)$ 是$\mathbf{F}_q$ 上的多项式. 因为$\mathbf{F}_{q^n}$ 在$\mathbf{F}_q$ 上的自同构τ 保持$f(x)$ 的系数不变, 所以$f(\alpha)=0$ 的充要条件是$f(\tau(\alpha))=0$. 换句话说, τ 对$f(x)$ 在$\mathbf{F}_{q^n}$ 中的根进行了置换. 特别, 对于$p(x)$ 的根β, 存在i 使得 $\tau(\beta)=\beta^{q^i}$.

因此, $\sigma_q^i(\beta)=\sigma_q(\sigma_q^{i-1}(\beta))=\beta^{q^i}=\tau(\beta)$.

因为β 是$\mathbf{F}_{q^n}$ 的本原元, 我们推出$\tau=\sigma_q^i$.

因此, $\mathbf{F}_{q^n}$ 在$\mathbf{F}_q$ 上的自同构集是一个阶为n 的循环群, 其生成元为自同构$\sigma_q(\alpha)=\alpha^q$. 证毕

13.3.4 正规基

设α 是$\mathbf{F}_q$ 上次数为n 的$\mathbf{F}_{q^n}$ 中的元素, 则$1,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}$ 构成$\mathbf{F}_{q^n}$ 在$\mathbf{F}_q$ 上的基底. 这个基底叫做**多项式基底**.

定义13.4.1 $\mathbf{F}_{q^n}$ 在$\mathbf{F}_q$ 上形为$\alpha,\ \alpha^q,\ \alpha^{q^2},\ \ldots,\ \alpha^{q^{n-1}}$ 的基底叫做$\mathbf{F}_{q^n}$ 在$\mathbf{F}_q$ 上的**正规基**.

定理13.4.1 (Artin 引理) 设$\psi_1,\ \ldots,\ \psi_s$ 是群G 到$\mathbf{F}^*$ (域$\mathbf{F}$ 的乘法群)的不同同态, 则$\psi_1,\ \ldots,\ \psi_s$ 在$\mathbf{F}$ 上线性无关, 也就是说, 对不全为零的数$c_1,\ldots,c_s \in \mathbf{F}$, 存在元素$g \in G$ 使得

$$c_1\psi_1(g) + \cdots + c_s\psi_s(g) \neq 0.$$

在证明有限域有正规基存在之前, 我们先叙述线性代数中的一个命题.

命题 设ψ 是n 维线性空间上的线性变换, 则ψ 的特征多项式$P_\psi(\lambda)$ 是n 次多项式, 并且ψ 的最小多项式$m(\lambda)$ 满足$m(\lambda) \mid P_\psi(\lambda)$.

定理13.4.2 有限域$\mathbf{F}_{q^n}$ 在其子域$\mathbf{F}_q$ 上有正规基存在.

证 $n=1$ 时, 结论显然成立. 设$n>1$. 因为$\mathbf{F}_{q^n}$ 在$\mathbf{F}_q$ 上的自同构群是

$$\mathrm{Aut}(\mathbf{F}_{q^n}) = \{id,\ \sigma_q,\ \sigma_q^2,\ \ldots,\ \sigma_q^{n-2},\ \sigma_q^{n-1}\},$$

其中$\sigma_q(\alpha)=\alpha^q$, 对任意$\alpha\in\mathbf{F}_{q^n}$, 所以$id,\ \sigma_q,\ \sigma_q^2,\ \ldots,\ \sigma_q^{n-2},\ \sigma_q^{n-1}$ 是$G = \mathbf{F}^*$ 到$\mathbf{F}^*$ 的n 个不同的同态. 根据定理??, $id,\ \sigma_q,\ \sigma_q^2,\ \ldots,\ \sigma_q^{n-2},\ \sigma_q^{n-1}$ 在$\mathbf{F}_{q^n}$ 上线性无关, 这意味着, σ 的最小多项式$m(\lambda)$ 的次数$\geq n$.

又对任意$\alpha\in\mathbf{F}_{q^n}$, 有$\sigma_q^n(\alpha)=\alpha^{q^n}=\alpha$, 这说明$\sigma$ 的特征多项式$P_\sigma(\lambda)=\lambda^n-1$.

根据命题, σ 的最小多项式$m(\lambda)=P_\sigma(\lambda)=\lambda^n-1$.

因此, 存在一个$\beta\in\mathbf{F}_{q^n}$ 使得

$$id(\beta)=\beta,\ \sigma_q(\beta)=\beta^q,\ \sigma_q^2(\beta)=\beta^{q^2},\ \ldots,\ \sigma_q^{n-2}(\beta)=\beta^{q^{n-2}},\ \sigma_q^{n-1}(\beta)=\beta^{q^{n-1}}$$

构成$\mathbf{F}_{q^n}$ 在$\mathbf{F}_q$ 上的基底. 证毕

例13.4.1 求$\mathbf{F}_{2^4} = \mathbf{F}_2[x]/(x^4+x+1)$ 中的生成元$g(x)$，并计算$g(x)^t$, $t=0,1,\dots,14$ 和所有生成元.

解

i) 对于$\beta = x$, 我们有

$$\begin{aligned}\beta &= x\\ \beta^2 &= x^2\\ \beta^4 &= x+1\\ \beta^8 &= x^2+1\end{aligned}$$

所以$\beta,\ \beta^2,\ \beta^{2^2},\ \beta^{2^3}$ 不构成一个基底.

ii) 对于$\beta = x^3$, 我们有

$$
\begin{aligned}
\beta &= x^3 &&= x^3 \\
\beta^2 &= x^6 &&= x^3 + x^2 \\
\beta^4 &= x^{12} &&= x^3 + x^2 + x + 1 \\
\beta^8 &= x^9 &&= x^3 + x
\end{aligned}
$$

所以β, β^2, β^{2^2}, β^{2^3} 构成一个基底, 是正规基.

例13.4.2 求$\mathbf{F}_{2^8}=\mathbf{F}_2[x]/(x^8+x^4+x^3+x+1)$ 中的正规基$g(x)$.

解 i) 对于$\beta=x$, 我们有

$$
\begin{aligned}
\beta &= x &&= x\\
\beta^2 &= x^2 &&= x^2\\
\beta^4 &= x^4 &&= x^4\\
\beta^8 &= x^8 &&= x^4+x^3+x+1\\
\beta^{16} &= x^{16} &&= x^6+x^4+x^3+x^2+x\\
\beta^{32} &= x^{32} &&= x^7+x^6+x^5+x^2\\
\beta^{64} &= x^{64} &&= x^6+x^3+x^2+1\\
\beta^{128} &= x^{128} &&= x^7+x^6+x^5+x^4+x^3+x
\end{aligned}
$$

所以$\beta,\ \beta^2,\ \beta^{2^2},\ \beta^{2^3},\ \beta^{2^4},\ \beta^{2^5},\ \beta^{2^6},\ \beta^{2^7}$ 不构成一个基底.

ii) 对于$\beta = x + 1$, 我们有

$$\begin{aligned}
\beta &= x+1\\
\beta^2 &= x^2+1\\
\beta^4 &= x^4+1\\
\beta^8 &= x^4+x^3+x\\
\beta^{16} &= x^6+x^4+x^3+x^2+x+1\\
\beta^{32} &= x^7+x^6+x^5+x^2+1\\
\beta^{64} &= x^6+x^3+x^2\\
\beta^{128} &= x^7+x^6+x^5+x^4+x^3+x+1
\end{aligned}$$

所以β, β^2, β^{2^2}, β^{2^3}, β^{2^4}, β^{2^5}, β^{2^6}, β^{2^7} 不构成一个基底.

iii) 对于$\beta = x^5$, 我们有

$$\begin{aligned}
\beta &= x^5 &&= x^5 \\
\beta^2 &= x^{10} &&= x^6 + x^5 + x^3 + x^2 \\
\beta^4 &= x^{20} &&= x^7 + x^4 + x^2 + x + 1 \\
\beta^8 &= x^{40} &&= x^7 + x^4 + x^2 \\
\beta^{16} &= x^{80} &&= x^7 + x^4 + 1 \\
\beta^{32} &= x^{160} &&= x^7 \\
\beta^{64} &= x^{65} &&= x^7 + x^4 + x^3 + x \\
\beta^{128} &= x^{130} &&= x^7 + x^6 + x^2 + 1
\end{aligned}$$

所以β, β^2, β^{2^2}, β^{2^3}, β^{2^4}, β^{2^5}, β^{2^6}, β^{2^7} 构成一个基底, 为正规基.