信息安全数学基础

第六章 有限域

聂旭云
信息与软件工程学院
电子科技大学

信息安全数学基础

有限域的性质

聂旭云
信息与软件工程学院
电子科技大学

代数元

- 定义6.2.1 设K是F的一个子域，α∈F，如果α满足K上的一个非零多项式，则称 α为K上的代数元。不是代数元的元素称为超越元。
- 定义6.2.2 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

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

- 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6.2.1 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6.2.1 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$f(x)$是不可约多项式。

- 证明： 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

$$f_1(\alpha)f_2(\alpha) = f(\alpha) = 0,$$

- 因而有$f_1(\alpha) = 0$或$f_2(\alpha) = 0$。
- 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。

代数元（续）

定理6.2.2 设α是域F上的代数元，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：

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

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

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

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

定理6.2.2 证明（续）

（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。

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。

有限域性质

定理6.2.3 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6.2.4（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6.2.5（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。

定理6.2.6 设F_q是q元域，则其乘法群$F_q^* = F_q \backslash \{0\}$是一个循环群。

有限域中元素的个数

- **定理6.2.3** 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。

分裂域

定义6.2.3 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6.2.2 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。

定理6.2.7 设$f(x) \in F[x]$,则$f(x)$在F上的任何两个分裂域是同构的。

有限域的存在性

定理6.2.4（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：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$f(x)$无重根，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。

有限域的惟一性

定理6.2.5（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：$\boldsymbol{F}$是具有$\boldsymbol{q=p^n}$个元素的有限域，则$\boldsymbol{F}$的特征为$\boldsymbol{p}$，以$\boldsymbol{GF(p)}$为其子域。所以$\boldsymbol{F}$是$\boldsymbol{GF(p)}$上的多项式$\boldsymbol{x^q-x}$的分裂域。

由于多项式的分裂域是同构的。

因此，$\boldsymbol{p^n}$元域都同构于$\boldsymbol{GF(p)}$上的多项式$\boldsymbol{x^q-x}$的分裂域。

有限域的乘法群

定理6.2.6 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

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

有限域的乘法群（续）

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$m|(q-1)/p_i$。故

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

当$j \neq i$时，有$p_j^{e_j}|(q-1)/p_i$，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6.2.4 F_q^*中的生成元称为F_q的本原元。

根据定理4.5.1，F_q中的本原元有$\varphi(q-1)$个。

例6.2.3 $\boldsymbol{x^2+x+1}$是$\boldsymbol{F_2}$上的不可约多项式，设$\boldsymbol{\alpha}$是$\boldsymbol{x^2+x+1}$的根，则

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

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

有限域的子域

定理6.2.8 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6.2.4 $F_{2^{30}}$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

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

定理6.2.8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$m|n$。

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。

感 谢 聆 听!

xynie@uestc.edu.cn