1 基本理论

引理1. 任何一个有限域中的元素个数是一个素数的幂。

证明：设 E 是一个有限域。则它的特征不等于零，它必定是一个素数 p. 因此 E 含有一个同构于 $\mathbb{F}_p$ 的子域。设 $n = [E : F]$. 则 $|E| = p^n$. □

设 p 是一个素数。记 $\bar{\mathbb{F}}_p$ 为 $\mathbb{F}_p$ 的代数闭包。

定理2. 设 n 是任意一个自然数，则在 $\bar{\mathbb{F}}_p$ 中存在唯一的子域 E 含 p^n 个元素。

证明：令 E 为 $\mathbb{F}_p$ 上的多项式 $x^{p^n}-x$ 在$\bar{\mathbb{F}}_p$ 的全部零点所构成的集合。

设 $a_1, a_2 \in E$. 则

$$(a_1-a_2)^{p^n}-(a_1-a_2)=a_1^{p^n}-a_2^{p^n}-a_1-a_2=0.$$

$$(a_1a_2)^{p^n}-(a_1a_2)=0.$$

若 a 是 E 中的非零元。则

$$(1/a)^{p^n}-1/a=(1/a^{p^n})-1/a=0.$$

所以 E 是 $\bar{\mathbb{F}}_p$ 的子域。

由于 $x^{p^n}-x$ 的导数为 -1. 因此 $x^{p^n}-x$ 没有重根。所以E 恰好含 p^n 个元素。这证明了存在性。

假定 K 是 $\bar{\mathbb{F}}_p$ 的另一个含 p^n 个元素的子域。我们以前已经知道 K 中的每个元素是 $x^{p^n}-x$ 的零点。因此$K=E$. □

系3. $\bar{\mathbb{F}}_p$ 含无限多个元素。

系4. 设 E, F 是 $\bar{\mathbb{F}}_p$ 的子域。 E 含 p^n 个元素，F 含 p^m 个元素。则 $F \subseteq E$ 当且仅当 $m|n$.

证明：由于 E, F 分别是 $x^{p^n} - x$ 和 $x^{p^m} - x$ 在$\bar{\mathbb{F}}_p$ 中的零点集，所以

$$F \subseteq E \Leftrightarrow$$

$$x^{p^m} - x | x^{p^n} - x \Leftrightarrow$$

$$x^{p^m-1} - 1 | x^{p^n-1} - 1 \Leftrightarrow$$

$$p^m - 1 | p^n - 1 \Leftrightarrow$$

$$m|n. \square$$

注1. 由于 $\mathbb{F}_p$ 的任何一个有限扩张都可以嵌入到 $\bar{\mathbb{F}}_p$ 中，所以在同构的意义下含 $q = p^n$ 的有限域是唯一的，记之为 $\mathbb{F}_q$.

2 有限域的乘法群的结构

引理5. 设 G 是一个 n 阶的有限Abel 群。假定对任何一个自然数 m, G 中最多有一个 m 阶子群，则 G 是循环群。

证明：设 $n = p_1^{e1} \dots p_r^{er}$ 是 n 的素因子分解式。对 $1 \leq i \leq r$, 设 G_i 是 G 的Sylow p_i-子群。根据Abel 群的结构定理，G_i 是若干个循环子群的直积。设 $G_i = H_1 \times \cdots \times H_t$, 其中每个 H_j 是循环群。由Lagrange 定理，每个 H_j 的阶都是 p_i 的幂。因此每个 H_j 含一个p_i 阶子群，于是 G 至少有 t 个 p_i 阶子群，这推出$t = 1$. 也就是说 G 的每个Sylow 子群是循环群。因此 G 是循环群。 □

定理6. 设 p 是一个素数， n 是一个自然数。当 $p|n$ 时， $\bar{\mathbb{F}}_p^*$ 中不存在 n 阶子群。当 $p \not| n$ 时， $\bar{\mathbb{F}}_p^*$ 中存在唯一的 n 阶子群，它是一个循环群。

证明：先设 $p|n$. 假定 H 是 $\bar{\mathbb{F}}_p^*$ 的一个 n 阶子群。则在 H 中存在一个 p 阶元 α, 即 $\alpha^p = 1$. 于是 $(\alpha - 1)^p = 0$. 产生矛盾，因此 $\bar{\mathbb{F}}_p^*$ 中不存在 n 阶子群。

再设 $p \not| n$. 多项式 $x^n - 1$ 的形式导数与 $x^n - 1$ 互素，因此 $x^n - 1$ 在 $\bar{\mathbb{F}}_p$ 中没有重零点。因为 $\bar{\mathbb{F}}_p$ 是代数闭域， $x^n - 1$ 在 $\bar{\mathbb{F}}_p$ 中恰好有 n 个零点，将其全体记作 H. 显然 H 是 $\bar{\mathbb{F}}_p^*$ 的 n 阶子群。

假定 K 是 $\bar{\mathbb{F}}_p^*$ 的任意一个 n 阶子群。根据 Lagrange 定理， $a^n = 1$ 对所有 $a \in K$ 成立，也就是说 K 中每个元素是多项式 $x^n - 1$ 在 $\bar{\mathbb{F}}_p$ 中的零点。因此 $K = H$. 这证明了 n 阶子群的唯一性。

特别，对于任意自然数 m, H 最多有一个 m 阶子群。根据引理 5 H 是循环群。 □

系7. 设 $q = p^n, p$ 是素数。则乘法群 $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ 是循环群。

系8. 设 E, F 是有限域，$F \subseteq E$. 则 E/F 是单扩张。

证明：任取循环群 E^* 的生成元 α, 则 $E = F[\alpha]$. □

系9. 任意一个有限域 $\mathbb{F}_q$ 上都存在任意次的不可约多项式。

证明：对任何自然数 n, 根据上面推论

$$\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha].$$

α 的极小多项式就是 $\mathbb{F}_q$ 上的一个 n 次不可约多项式。□

定义1. 设 F 是一个有限域。则循环群 F^* 的任何一个生成元称为 F 的一个**本原元**(primitive element)。

例1. 设 p 是一个素数， m 是一个不被 p 整除的自然数。求证存在自然数 n 使 m 整除 $p^n - 1$.

证明：根据定理 6 $\bar{\mathbb{F}}_p^*$ 中存在一个 m 阶循环群。设 α 是这个循环群的生成元。令 $E = \mathbb{F}_p[\alpha]$. 设 E 中的元素个数是 p^n. 根据 Lagrange 定理 $m|p^n - 1$. □

从这个例子看到初等数论中的某些问题可以用有限域的方法解决。

定理10 (Wilson 定理)**.** 设 p 是一个素数，则

$$(p-1)! \equiv -1 \pmod{p}.$$

证明：当 $p = 2$ 时定理显然成立，以下设 p 是奇素数。于是在$\mathbb{F}_p$ 中 $1 \neq -1$ 且 $1, -1$ 是方程 $x^2 = 1$ 在$\mathbb{F}_p$ 中的全部解。对任意 $t \in \mathbb{F}_p$, 只要 $t \neq \pm 1$ 就有 $t^{-1} \neq t$. 因此

$$\prod_{t \in \mathbb{F}_p^* \setminus \{1,-1\}} t = 1.$$

从而

$$\prod_{t \in \mathbb{F}_p^*} t = -1.$$

所以在 $\mathbb{F}_p$ 中等式

$$\prod_{j=1}^{p-1} \bar{j} = -1$$

成立。转换成 $\mathbb{Z}$ 中的同余式就就是要证明的式子。□

例2. 设 p 是素数， $q=p^n$. 求方程 $y^q+y=x^{q+1}$ 在 $\mathbb{F}_{q^2}$ 中的解的个数。

证明：对任意 $\alpha\in\mathbb{F}_{q^2}$, 都有

$$\left(\alpha^{q+1}\right)^q=\alpha^{q^2+q}=\alpha^{q+1}.$$

因此 $\alpha^{q+1}\in\mathbb{F}_q$. 令

$$f(y)=y^q+y-\alpha^{q+1}\in\mathbb{F}_q[y].$$

由于 $f'(y)=1,\ f(y)=0$ 在 $\bar{\mathbb{F}}_q$ 中有 q 个两两不同的根。设 $\beta\in\bar{\mathbb{F}}_q$ 满足 $f(\beta)=0$, 则

$$\beta^q+\beta-\alpha^{q+1}=0,$$

$$\beta^{q^2}+\beta^q-\alpha^{q+1}=0.$$

相减得

$$\beta^{q^2}-\beta=0.$$

因此 $\beta\in\mathbb{F}_{q^2}$.

所以原方程有 q^3 组解。

作业：第102 页4
第104 页2，5