

1, 证明任意有限域必有不等于它自身的代数扩张,

证明: 不妨设 F 是含 q 个元素的有限域, 则对属于 F^* 的任意 α , 都有 $\alpha^q - \alpha = 0$,

所以 F 中任意元素均是多项式 $x^q - x$ 的根,

从而 F 上的多项式 $f(x) = x^q - x + 1$ 在 F 中没有根,

设 β 是 $f(x)$ 的一个根, 则 β 不属于 F 且包含 F 的 $F(\beta)$ 是有限扩张,

也是代数扩张, 且 $F(\beta) \neq F$,

2, 设 F 是有限域, 证明 $F - \{0\}$ 的所有元素的乘积等于 -1 ,

证明: 设 $|F| = q$, 则 $F - \{0\} = \{\alpha_1, \alpha_2, \dots, \alpha_{q-1}\}$ 的元素是方程 $x^{q-1} - 1 = 0$ 的所有根

则 $x^{q-1} - 1 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{q-1})$

令 $x = 0$, 则 $(-1)^{q-1} \alpha_1 \alpha_2 \cdots \alpha_{q-1} = -1$

由于 -1 属于 $F - \{0\}$, 从而 $(-1)^{q-1} = 1$, 故 $\alpha_1 \alpha_2 \cdots \alpha_{q-1} = -1$

即 $F - \{0\}$ 的所有元素的乘积等于 -1

3, 求 $|GF(729) : GF(27)|$ 和 $|GF(512) : GF(8)|$,

解: $|GF(729) : GF(27)| = |GF(3^6) : GF(3^3)| = 6 \div 3 = 2$,

$|GF(512) : GF(8)| = |GF(2^9) : GF(2^3)| = 9 \div 3 = 3$,

4, 构造含 125 个元素的域, 并求其所有子域

解: 因为 $125 = 5^3$, 故需在 Z_5 上找到一个不可约的三次多项式,

易知 $f(x) = x^3 + x + \bar{4}$ 为 Z_5 上的不可约多项式,

设 α 为 $f(x)$ 的一个根, 则 $|Z_5(\alpha)| = 125$, 其所有子域为 $Z_5, Z_5(\alpha)$

5, 求 $GF(2^6)$ 的全部子域,

若 α 是 $GF(2^6)$ 的乘法群的一个生成元,

求 $GF(2^6)$ 的每个子域的乘法群的一个生成元,

解: 因为 6 的所有因子为 1, 2, 3, 6,

故 $GF(2^6)$ 的所有子域为 $GF(2)$, $GF(2^2)$, $GF(2^3)$, $GF(2^6)$,

α 是 F 的乘法群的生成元, 所以可设 α^i 是 $GF(2^k)$ 的乘法群的生成元,

根据[第二章推论 5.2(1)]可取 $i = \frac{2^6-1}{2^k-1}$

因此子域 $GF(2)$, $GF(2^2)$, $GF(2^3)$, $GF(2^6)$ 的乘法群的生成元依次为 α^{62} , α^{21} , α^9 , α

6, 设 $f(x)$ 是 $Z_p[x]$ 中的 m 次不可约元, 试证明当且仅当 $m|n$ 时, $f(x)|(x^{p^n}-x)$

证明: $g(x)=x^{p^n}-x$ 在 Z_p 上的分裂域就是一个 p^n 阶有限域,

若 $f(x)|(x^{p^n}-x)$, 设 α 是 $f(x)$ 的一个根,

则 $f(x)$ 在 Z_p 上的分裂域 $Z_p(\alpha)$ 就是一个 p^m 阶域的子域, 而 $|Z_p(\alpha)|=p^m$, 所以 $m|n$

反之, 设 α 是 $f(x)$ 的一个根, 则 $f(x)$ 在 Z_p 上的分裂域 $Z_p(\alpha)=GF(p^m)$,

若 $m|n$, 则 $Z_p(\alpha)=GF(p^m)$ 是 $GF(p^n)$ 的子域, 从而 α 是 $x^{p^n}-x$ 的根,

因为 $f(x)$ 是不可约元, 所以 $f(x)|(x^{p^n}-x)$

7, 设 $p(x)$ 是 $\mathbb{Z}[x]$ 中的 n 次不可约元,

试证明若 α 是 $p(x)$ 在其分裂域中的一个根,

则 $p(x)$ 在其分裂域中的全部根为 $\alpha, \alpha^p, \dots, \alpha^{p^{n-1}}$

证明: 因为对于 $\mathbb{Z}_p$ 中的任意元素 β 都有 $\beta^p = \beta$, 又因 $p(\alpha) = 0$ 且 $\deg p(x) = n$,

不妨设 $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, 则 $p(\alpha) = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0 = 0$

从而 $[p(\alpha)]^{p^i} = (a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0)^{p^i}$

$= a_n (\alpha^{p^i})^n + a_{n-1} (\alpha^{p^i})^{n-1} + \dots + a_1 \alpha^{p^i} + a_0 = 0 (0 \leq i \leq n-1)$

故 $\alpha, \alpha^p, \dots, \alpha^{p^{n-1}}$ 是 $p(x)$ 的根,

下证这 n 个根不同

反证, 假设存在 i, j 使得 $\alpha^{p^i} = \alpha^{p^j} (i > j)$, 则 $\alpha^{p^i} - \alpha^{p^j} = (\alpha^{p^{i-j}} - \alpha)^{p^j} = 0$,

从而 $\alpha^{p^{i-j}} - \alpha = 0$, 即 α 是 $x^{p^{i-j}} - x (i-j < n)$ 的根,

这与 α 是 n 次不可约元 $p(x)$ 的根矛盾,

8, 求属于 $\mathbb{Z}_3[x]$ 的多项式 $f(x) = x^3 + 2x + 1$ 在它的分裂域中的所有根

解: 经验证 $f(x)$ 为 $\mathbb{Z}_3[x]$ 的不可约多项式,

设 $f(\alpha) = 0$, α 为 $f(x)$ 的一个根, 则其分裂域的所有根为 $\alpha, \alpha^3, \alpha^9$

习题 1 构造含有 16 个元素的有限域

解: $x^4 + x + 1$ 是 $\mathbb{Z}_2[x]$ 中不可约多项式, 设 α 是该多项式的一个根, 则 $\mathbb{Z}_2(\alpha)$ 为所求

习题 2 求 $\text{GF}(3^{12})$ 的全部子域,

解: $\text{GF}(3^{12})$ 的全部子域为 $\text{GF}(3), \text{GF}(3^2), \text{GF}(3^3), \text{GF}(3^4), \text{GF}(3^6), \text{GF}(3^{12})$,

习题 3 求属于 $\mathbb{Q}[x]$ 的 $x^n - 1$ 在 $\mathbb{Q}$ 上的 n 次单位根和本原 n 次单位根

解: n 次单位根的集合为 $\left\{ \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \mid k = 0, 1, \dots, n-1 \right\}$

本原 n 次单位根的集合为 $\left\{ \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \mid (k, n) = 1, k = 0, 1, \dots, n-1 \right\}$

习题 4 证明映射 $\varphi: GF(p^n) \rightarrow GF(p^n), x \rightarrow x^p$ 是 $GF(p^n)$ 的自同构

证明: 对于属于 $GF(p^n)$ 任意 x, y , 有 $(x+y)^p = x^p + y^p, (xy)^p = x^p y^p$,

即 φ 是 $GF(p^n)$ 的自同态,

若 $x^p = y^p$, 则 $0 = x^p - y^p = (x-y)^p$, 从而 $x=y$, 即 φ 是单射,

因为 $GF(p^n)$ 是有限集合, 故 φ 是双射, 这就证明了 φ 是 $GF(p^n)$ 的自同构,

习题 5 试证明 $\text{Aut}_F GF(p^n) = \{\varphi_i | \varphi_i: x \rightarrow x^{p^i}, i=0, 1, \dots, n-1\}$,

证明: 先证 $\varphi_i: x \rightarrow x^{p^i}$ 是 $GF(p^n)$ 的自同构,

若 $x^{p^i} = y^{p^i}$, 则 $0 = x^{p^i} - y^{p^i} = (x-y)^{p^i}$, 从而 $x=y$, 即 φ_i 是单射,

因为 $GF(p^n)$ 是有限集合, 故 φ_i 是双射,

显然 $\varphi_i(x+y) = (x+y)^{p^i} = x^{p^i} + y^{p^i} = \varphi_i(x) + \varphi_i(y), \varphi_i(xy) = (xy)^{p^i} = x^{p^i} y^{p^i} = \varphi_i(x) \varphi_i(y)$

即 φ_i 是 $GF(p^n)$ 的自同态,

从而 φ_i 是 $GF(p^n)$ 的自同构, 即 $GF(p^n)$ 中至少有 n 个元素, 显然 φ_i 属于 $\langle \varphi_1 \rangle$,

因为 $GF(p^n)$ 是 Z_p 上的单代数扩张, 所以存在 α 使得 $GF(p^n) = Z_p(\alpha)$,

α 在 Z_p 上的极小多项式为 $f(x)$, $f(x)$ 的次数为 n ,

设 φ 是 $GF(p^n)$ 的自同构, 对属于 Z_p 的 $\bar{m}$, 有 $\varphi(\bar{m}) = m\varphi(\bar{1}) = m\bar{1} = \bar{m}$

即 φ 在 $GF(p^n)$ 上的像由 α 决定,

因为 $\varphi(f(\alpha)) = f(\varphi(\alpha))$, 即 $\varphi(\alpha)$ 是 $f(x)$ 的一个根, 知 $GF(p^n)$ 中最多有 n 个元素

综上, $GF(p^n)$ 的自同构群为 $\{\varphi_i | \varphi_i: x \rightarrow x^{p^i}, i=0, 1, \dots, n-1\} = \langle \varphi_1 \rangle$,

习题 6 有限域上的不可约多项式在分裂域中无重根

证明: 令 $F = GF(p^n)$,

设 p 为素数, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ 为 F 上不可约多项式,

若 $f(x)$ 在分裂域中有重根, 则 $f(x) = \sum_{i=0}^m b_i (x^p)^i = \left(\sum_{i=0}^m b_i x^i \right)^p$

这与 $f(x)$ 不可约矛盾

习题 7 在 $\mathbb{Z}_p[x]$ 中证明当且仅当 $m|n$ 时, $(x^{p^m}-x)|(x^{p^n}-x)$

证明: 若 $m|n$, 则 $x^{p^m}-x$ 的根都是 $x^{p^n}-x$ 的根, 因此 $(x^{p^m}-x)|(x^{p^n}-x)$

反之, 因为 $\text{GF}(p^n)$ 由 $x^{p^n}-x$ 在分裂域中的全部根组成,

所以若 $(x^{p^m}-x)|(x^{p^n}-x)$, 则 $\text{GF}(p^m)$ 是 $\text{GF}(p^n)$ 的子域, 因此 $m|n$

习题 8 设 F 是特征为 p 的有限域, α 是 F 的乘法群的生成元,

试证明 α^p 是 F 的乘法群的生成元,

证明: 设 F 的阶为 p^n , 则 F 的乘法群的阶为 p^n-1

要证 α^p 是 F 的乘法群的生成元, 只需要说明 α^p 阶为 p^n-1 ,

设 α^p 阶为 t , 则 $\alpha^{tp}=1$, 于是 $p^n-1|tp$,

由 $(p^n-1, p)=1$ 得 $(p^n-1)|t$, 而 $(\alpha^p)^{p^n-1}=1$, 于是 $t|(p^n-1)$

因此 α^p 阶为 p^n-1 ,