近世代数之十三

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

1. 有限域
2. 有限域的子域与自同构群

有限域的概念

设E为有限域E。

1. $\mathrm{char}(E) = p > 0$
2. $\mathbb{F}_p \subseteq E$
3. 视E为$\mathbb{F}_p$-线性空间: $\bar{m}.a = ma$，即m个a相加
4. 从而, $|E| = p^n$，其中$n = \dim_{\mathbb{F}_p} E$
5. p元域必同构于$\mathbb{F}_p$

Frobenius自同构

定义

有限域E上的**Frobenius自同构**$\sigma\colon E \to E$定义为$\sigma(a) = a^p$。

1. Fermat小定理(1640): $\bar{n}^p = \bar{n}$
2. 考虑$\mathbb{F}_p(t)$，其Frobenius自同态$x \mapsto x^p$不是满射!

单位群

设$|E| = p^n$。则单位群$E^* = E\backslash\{0_E\}$满足$|E^*| = p^n - 1$.

引理 (Lagrange定理的特殊情况！)

任何$a \in E^*$，我们有$a^{p^n-1} = 1_E$。

故，任何$a \in E$均为$x^{p^n} - x = \bar{0}$的根。

证明：设有最小的d满足$a^d = 1_E$ (why?)。考虑$H = \{1, a, \cdots a^d\}$以及E^*上的等价关系$c \simeq d$，若$cd^{-1} \in H$。考虑相应的分拆, 得出$d|(p^n - 1)$

存在唯一性定理

定理

对于任何n，唯一存在p^n阶有限域。

通常记为$\mathbb{F}_{p^n}$！（警告：它只是“本质唯一”！）

证明：$\mathbb{F}_{p^n}$为$x^{p^n}-x\in\mathbb{F}_p[x]$的分裂域！

特别地，我们有

$$x^{p^n}-x=\prod_{a\in\mathbb{F}_{p^n}}(x-a).$$

$\mathbb{F}_p$上不可约多项式

命题

$$x^{p^n}-x=\prod_{d|n}\ \prod_{\{f(x)\in\mathbb{F}_p[x]|\ \text{monic irr. of degree } d\}} f(x)$$

证明：考虑$x^{p^n}-x$的因子$f(x)$，以及$a\in \mathrm{Root}_E(f)$。
则$\mathbb{F}_p(a)\subseteq E$，维数公式。

反之，设$g(x)\in\mathbb{F}_p[x]$为d次首一不可约。考虑其添根构造$K=\mathbb{F}_p[x]/(g(x))$。则有$g(x)|(x^{p^d}-x)|(x^{p^n}-x)$。

例子

例子 ($p = 2$)

$$x^4 - x = x(x + \bar{1})(x^2 + x + \bar{1})$$

$$x^8 - x = x(x + \bar{1})(x^3 + x^2 + \bar{1})(x^3 + x + \bar{1})$$

$$x^{16} - x =$$

$$x(x+\bar{1})(x^2+x+\bar{1})(x^4+x^3+x^2+x+\bar{1})(x^4+x^3+\bar{1})(x^4+x+\bar{1}).$$

例子 ($p = 3$)

$$x^9 - x = x(x + \bar{1})(x - \bar{1})(x^2 + \bar{1})(x^2 + x - \bar{1})(x^2 - x - \bar{1})$$

子域

取定E使得$|E| = p^n$。

命题

1. 设$K \subseteq E$为子域。则$|E| = p^d$且$d|n$。
2. 设$d|n$。则存在唯一的子域$K \subseteq E$满足$|K| = p^d$。

考虑根集$\mathrm{Root}_E(x^{p^d} - x)$。

思考：尝试描述E的子域格（子域的包含关系!）

例子

$\mathbb{F}_{2^6}$的子域格。

生成元

设$n = q_1^{r_1} \cdots q_t^{r_t}$。则$E$的极大真子域$K_i$，阶为$p^{\frac{n}{q_i}}$。

命题

我们有$\cup_{i=1}^{t} K_i \neq E$。故，存在$u \in E$满足$E = \mathbb{F}_p(u)$。

1. $\mathbb{F}_p[x]$上总有n次不可约多项式; 取$f(x)$。
2. 设$u \in \mathrm{Root}_E(f(x))$。则$f(x) = \prod_{i=0}^{n-1}(x - \sigma^i(u))$.
3. 特别地，$\sigma^i(u) \neq u$，对于$1 \leq i \leq n-1$

自同构

注意$\sigma \in \mathrm{Aut}(E)$满足$\sigma^n = \mathrm{Id}_E$。

定理

$\mathrm{Aut}(E) = \{\mathrm{Id}_E, \sigma, \cdots, \sigma^{n-1}\}$.

证明：考虑自同构$\delta \in \mathrm{Aut}(E)$在生成元$u$上的作用。

故, $\mathrm{Aut}(E)$为**循环群**。考虑其子群...

有限域的Galois对应

设E为有限域，$|E| = p^n$。

定理 (有限域的Galois对应)

存在格的反同构

$$\{K \subseteq E \text{ 子域}\} \longleftrightarrow \{H \subseteq \mathrm{Aut}(E) \text{ 子群}\}$$

使得$K \mapsto \mathrm{Aut}(E/K)$以

及$H \mapsto E^H = \{a \in E \mid h(a) = a, \textit{for any } h \in H\}$

所有的子域和子群均具体给出。

注：该处，整数整除关系的两种不同“代数提升”!