第十二次习题课

方法提要、习题讲解和内容扩充

助教：邓先涛

2023 年 12 月 4 日

重点知识提要

重点知识提要

- Galois 扩张：有限可分的正规扩张.
- 有限域的结构：有限域的子域刻画；有限域上的多项式性质.
- 多项式的 Galois 群的计算：了解三次多项式和四次多项式 Galois 群的分类准则.

有限域及其上的多项式

一些基本事实

- 有限域中的元素个数：设 n 为正整数，存在 n 元有限域的充分必要条件是 n 为素数方幂.
- 有限域存在唯一性：任给素数方幂 p^m，同构意义下存在唯一一个 p^m 元有限域，记作 $\mathbb{F}_{p^m}$.
- 有限域的子域：设 p 为素数，$\mathbb{F}_{p^m}$ 是 $\mathbb{F}_{p^n}$ 的子域当且仅当 $m \mid n$.
- 有限域的本原元：设 p 为素数，存在 $\alpha \in \mathbb{F}_{p^m}$ 使得 $\mathbb{F}_{p^m}^{\times} =< \alpha >$，因此 $\mathbb{F}_{p^m} = \mathbb{F}_p(\alpha)$.
- 有限域的不可约多项式：设 q 为素数方幂，任给正整数 m，$\mathbb{F}_q$ 上存在 m 次不可约多项式.
- 有限域的 Galois 扩张：$\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ 中的元素为 $\sigma_i : \alpha \to \alpha^{q^i} (i = 0, 1, \cdots, m-1)$.

第七章第 21 题 (i)

构造一个 9 个元素的域，并给出加法和乘法表

多项式环中的极大理想

证明

- 9 个元素的域的素域是 $\mathbb{F}_3$，利用多项式环的性质，构造 $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1)$.
- 加法运算规则：$ax+b+cx+d = (a+c)x+(b+d)$；
  乘法运算规则：$(ax+b)(cx+d) = (ad+bc)x+bd-ac$.
- 逐项进行加法和乘法，得到加法表或乘法表.

证明

$+$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

表: $\mathbb{F}_9$ 的加法表

总结

加法表乘法表一般是计算机运算的预处理的步骤，以存储空间换取运算时间的手段.

第五章第 22 题第 1、2 问

设 p 为素数，$\mathbb{F}_p$ 为 p 元有限域，$f(x) \in \mathbb{F}_p[x]$ 是 n 次不可约，则 $f(x) \mid x^{p^m} - x$ 当且仅当 $n \mid m$. 特别的，$x^{p^n} - x \mid x^{p^m} - x$ 当且仅当 $n \mid m$.

单扩张元素次数等于扩张次数

证明

- 设 $\alpha \in \overline{\mathbb{F}_p}$ 为 $f(x)$ 的根，则 $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$.
- 若 $n \mid m$，则 $\mathbb{F}_{p^n}$ 为 $\mathbb{F}_{p^m}$ 的子域，因此 α 为 $x^{p^m} - x$ 的根. $f(x)$ 不可约，推出 $f(x) \mid x^{p^m} - x$.
- 若 $f(x) \mid x^{p^m} - x$，则 $\alpha \in \mathbb{F}_{p^m}$，因此 $\mathbb{F}_{p^n}$ 为 $\mathbb{F}_{p^m}$ 的子域，推出 $n \mid m$.
- 注意到 $x^{p^n} - x$ 的所有根恰好是 $\mathbb{F}_{p^n}$ 中的元素全体，因此命题等价于第 3 个基本事实.

第五章第 22 题第 3、4 问

设 p 为素数，$\mathbb{F}_p$ 为 p 元有限域，$P_n(x)$ 为 $\mathbb{F}_p$ 上 n 次首一不可约多项式全体的乘积，则 $x^{p^n}-x=\prod_{d|n}P_d(x)$，且 $P_n(x)=\prod_{d|n}(x^{p^d}-x)^{\mu(n/d)}$，其中 μ 是莫比乌斯函数.

莫比乌斯反演公式：设 $f(n)$ 和 $g(n)$ 是数论函数，若 $f(n)=\prod_{d|n}g(d)$，则 $g(n)=\prod_{d|n}f(d)^{\mu(n/d)}$.

证明

- 令 $F_n(x)=\prod_{d|n}P_d(x)$，则 $F_n(x)$ 没有重根，且 $P_d(x)\mid x^{p^n}-x$ 推出 $F_n(x)\mid x^{p^n}-x$.
- 任给 $x^{p^n}-x$ 根 α，$\mathbb{F}_p(\alpha)$ 是 $\mathbb{F}_{p^n}$ 的子域，α 次数整除 n，有 $F_n(\alpha)=0$，推出 $x^{p^n}-x\mid F_n(x)$.
- 注意到 $\prod_{d|n}(x^{p^d}-x)^{\mu(n/d)}=\prod_{d|n}\left(\prod_{d'|d}P_{d'}(x)\right)^{\mu(n/d)}=\prod_{d'|n}P_{d'}(x)^{\sum_{d''|\frac{n}{d'}}\mu(d'')}$
- $\sum_{d|n}\mu(d)=[1/n]$，其中 $[\cdot]$ 为下取整. 立刻得到 $\prod_{d'|n}P_{d'}(x)^{\sum_{d''|\frac{n}{d'}}\mu(d'')}=P_n(x)$.

第五章第 22 题第 5 问

设 p 为素数，$\mathbb{F}_p$ 为 p 元有限域，N_n 为 $\mathbb{F}_p$ 上全体 n 次首一不可约多项式的数目，则 $N_n = \frac{1}{n}\sum_{d|n}\mu(n/d)p^d$.

N_n 与 P_n 的次数之间的联系

证明

- 注意到 $P_n(x)$ 为全体 n 次首一不可约多项式的乘积，因此 $N_n = \deg(P_n(x))/n$.
- $P_n(x) = \prod_{d|n}(x^{p^d} - x)^{\mu(n/d)}$，表面 $\deg(P_n(x)) = \sum_{d|n}\mu(n/d)p^d$，因此结论成立.

思维拓展

上述命题可否推至一般的 $\mathbb{F}_q$，这其中有无异同？证明 $\frac{p^n}{n} - \frac{p(p^{n/2}-1)}{n(p-1)} \leq N_n \leq \frac{p^n-p}{n}$，并探究等号成立的条件.

第五章第 24 题

证明有限域中的每一个元素可表为两个元素的平凡和.

鸽笼原理和二次互反律的应用

思维拓展

上述命题表明 $x^2+y^2=a$ 对一切 $a\in\mathbb{F}_q$ 总是有解. 记 $N(a)=|\{(x,y)\in\mathbb{F}_q^2|x^2+y^2=a\}|$，可以得到 $N(a)\neq 0$，试计算 $N(a)$.

证明

- 若特征为 2，则 $z=z^{2^m}=(z^{2^{m-1}})^2+0$ 显然成立；若特征为奇素数，则 $\mathbb{F}_q$ 中的非零平方元个数为 $\frac{q-1}{2}$.
- 若 $-1=\alpha^2$ 是平方元，则 $z=\left(\frac{z+1}{2}\right)^2+\left(\alpha\frac{z-1}{2}\right)^2$ 可以表为平方和.
- 若 $-1=\alpha^2$ 不是平方元，固定 x 的选择，则 x^2+y^2 有 $\frac{q+1}{2}$ 个不同的取值，全都非零.
- 存在非平方元可以写作 x^2+y^2，于是 $z^2(x^2+y^2)$ 给出了所有的非平方元.

多项式分裂域

设 $f(x)$ 是 $\mathbb{F}_q$ 上的 6 次首一多项式，则 $f(x)$ 的分裂域有几种可能的情况？

整数分拆和有限域与其子域的关系

思维拓展

设 $F(n)$ 为 n 次首一多项式的可能的分裂域的种数，你能写出 $F(n)$ 的表达式吗？

证明

- 设 $f(x) = f_1(x)f_2(x)\cdots f_m(x)$ 为不可约分解，则分裂域由其不可约因式完全决定，而不可约因式的分裂域由其次数完全决定.
- $6 = 6+0 = 5+1 = 4+2 = 4+1+1 = 3+2+1 = 3+1+1+1 = 2+2+2 = 2+2+1+1 = 2+1+1+1+1 = 1+1+1+1+1+1$
- 设 $n = n_1 + \cdots + n_t$ 为不可约次数的情况，则相应的扩张次数为 $n_1, \cdots, n_t$ 的最小公倍数. 因此用 6 种可能的分裂域.

三项不可约多项式

设 $f(x)=x^{2n}+x^n+1\in\mathbb{F}_2[x]$，证明：$f(x)$ 不可约当且仅当存在非负整数 k 使得 $n=3^k$.

简单的数论和多项式整除的关系

思维拓展

设 $f(x)=x^{4n}+x^n+1\in\mathbb{F}_2[x]$，则 $f(x)$ 不可约当且仅当存在非负整数 k 和 m 使得 $n=3^k\cdot 5^m$.

证明

- 若 $n=3^k$，则 $3^{k+1}\mid 4^{3^k}-1=2^{2n}-1$，
- 推出 $x^{3n}-1\mid x^{2^{2n}}-x$，因此 $f(x)\mid x^{2^{2n}}-x$.
- 设 η 为 $f(x)$ 的根，则 $\mathbb{F}_2(\eta)$ 为 $\mathbb{F}_{2^{2n}}$ 子域，并且满足 $\mathbb{F}_{2^2}\subset\mathbb{F}_2(\eta)=\mathbb{F}_{2^{2\cdot 3^t}}(t\le k)$.
- $\gcd(3^{k+1},2^{2\cdot 3^t}-1)=3^{t+1}$，若 $t<k$，则 $\eta^n=1$，即 $f(\eta)\neq 0$ 矛盾. $\mathbb{F}_2(\eta)=\mathbb{F}_{2^{2\cdot 3^t}}$.
- 若 $n=h\cdot p$ 使得 $p\neq 3$ 为素数，只需要去证明 $g(x)=x^{2p}+x^p+1$ 可约即可.
- 若 $g(x)$ 不可约，则 $g(x)\mid x^{2^{2p}-1}-1$，因此 $g(x)\mid\gcd(x^{3p}-1,x^{2^{2p}-1}-1)=x^3-1$ 矛盾.

三项不可约多项式

设 $b \in \mathbb{F}_p$，证明：$f(x) = x^p - x - b$ 在 $\mathbb{F}_{p^n}$ 不可约当且仅当 $p \nmid n$.

有限域中元素的运算

思维拓展

设 q 是素数方幂，$b \in \mathbb{F}_q$ 和 $1 \neq a \in \mathbb{F}_q$，则 $f(x) = x^q - ax - b$ 在 $\mathbb{F}_q$ 上可约.

证明

- 设 α 为 $f(x)$ 的根，$\alpha^{p^2} = (\alpha + b)^p = \alpha + 2b$. 以此类推，$\alpha^{p^m} = \alpha + mb$.
- 若 $p \nmid n$，则 $\alpha^{p^{nm}} = \alpha + nmb$，因此 $m = p$ 是使得 $\alpha^{p^{mn}} = \alpha$ 成立的最小的正整数.
- 推出 $\mathbb{F}_{p^n}(\alpha) = \mathbb{F}_{p^{pn}}$，因此不可约.
- 若 $p \mid n$，则 $\alpha^{p^n} = \alpha$，推出 $\alpha \in \mathbb{F}_{p^n}$，因此 $f(x)$ 在 $\mathbb{F}_{p^n}$ 上完全分裂.

多项式的 Galois 群

多项式的 Galois 群的必要性

设 K/F 是有限 Galois 扩张，则 K 是 F 上一个不可约多项式 $m(x)$ 的分裂域.

有限可分扩张是单代数扩张

总结

域扩张的 Galois 群 $\mathrm{Gal}(K/F)$ 就是多项式 $m(x)$ 的 Galois 群. 所谓多项式的 Galois 群就是就是多项式的分裂域的 Galois 群.

证明

- 有限 Galois 扩张是有限正规可分扩张，因此是单扩张.
- 存在 α 使得 $K = F(\alpha)$.
- 由于 K/F 是正规扩张，因此 α 的共轭元均在 K 中. 这表明 K/F 是 α 极小多项式 $m(x)$ 的分裂域.

三次多项式的 Galois 群

- 三次多项式的统一形式：设域 F 特征不是 3，三次多项式均可化作 $x^3+px+q\in F[x]$.
- n 次多项式 Galois 群结构：n 次多项式的 Galois 群均可以看作根的置换群，即 S_n 的子群.
- 三次多项式 Galois 群：设 F 特征不是 2 和 3，$f(x)=x^3+px+q$，判别式 $D(f)=-(4p^3+27q^2)$.

$$\mathrm{Gal}(f(x)/F)=\begin{cases}1, & f(x)\text{在 } F \text{ 中完全分裂}\\ S_2, & f(x)\text{在 } F \text{ 中有且仅有一个根}\\ A_3, & f(x)\text{在 } F \text{ 中不可约且}D(f)\in F^2\\ S_3, & f(x)\text{在 } F \text{ 中不可约且}D(f)\notin F^2\end{cases}$$

第八章第 16 题第 2 问

分别计算 $f(x) = x^3 - x - 1$ 在 $\mathbb{Q}$ 和 $\mathbb{Q}(\sqrt{-23})$ 上的 Galois 群.

三次多项式的 Galois 群的分类

思维拓展

对特征 2 和 3 的情况进行类似分类，给出其上三次和四次多项式 Galois 群的结构.

证明

- 判断是否可约：通过试根法得 $f(x)$ 在 $\mathbb{Q}$ 上不可约，因此也在 $\mathbb{Q}$ 的二次扩张上不可约.
- 计算判别式：计算得到 $D(f) = -23$，在 $\mathbb{Q}$ 上不可开方，但是在 $\mathbb{Q}(\sqrt{-23})$ 上可开方.
- 得到结论：$\mathrm{Gal}(f(x)/\mathbb{Q}) = S_3$，且 $\mathrm{Gal}(f(x)/\mathbb{Q}(\sqrt{-23})) = A_3$.

判别式的计算

设 $f(x)$ 是 n 次多项式，$\alpha_1, \cdots, \alpha_n$ 为全部 n 个根，定义 $D(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$ 为 f 的判别式. 将 $D(f)$ 表示为 f 的系数的多元多项式.

对称多项式基本定理

例子计算

设 $f(x) = x^3 + ax^2 + b$，计算 $D(f)$.

- $D(f) = ua^6 + va^3b + wb^2$.
- 取 $(1, 1, -1/2)$ 和 $(1, 2, -2/3)$ 进行计算.
- 得 $u = -4, v = -27$，$D(f) = -4a^3b - 27b^2$.

证明

- 注意到 $D(f)$ 是关于 n 个根的齐次对称多元多项式，因此可以由 n 个根的初等对称多项式进行表示.
- 设 $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$，设 $\sigma_i(\alpha_1, \cdots, \alpha_n) = \sum_{1 \le k_1 < \cdots < k_i \le n} \alpha_{k_1} \cdots \alpha_{k_i}$ 为初等对称多项式，则 $\sigma_i(\alpha_1, \cdots, \alpha_n) = (-1)^i a_i$
- 将 $D(f)$ 可待定系数地表为 $a_i (1 \le i \le n)$ 的多元多项式，再通过解方程得到结果.

四次多项式的 Galois 群

- 四次多项式的统一形式：设域 F 特征不是 2 和 3，四次多项式均可化作 x^4+px^2+qx+r.
- 四次多项式的预解式：设 $f(x)$ 不可约，否则可以化作 3 次或 2 的情况，此时令 $\alpha_1,\cdots,\alpha_4$ 为全部不同根. 预解式为 $g(x)=(x-\alpha)(x-\beta)(x-\gamma)=x^3-2px^2+(p^2-4r)x+q^2$，其中

$$\alpha=(\alpha_1+\alpha_2)(\alpha_3+\alpha_4),\beta=(\alpha_1+\alpha_3)(\alpha_2+\alpha_4),\gamma=(\alpha_1+\alpha_4)(\alpha_2+\alpha_3).$$

四次多项式的 Galois 群

- 四次多项式 Galois 群：设 F 特征不是 2，$f(x)$ 四次不可约多项式，$g(x)$ 为预解式，K/F 为预解式 $g(x)$ 的分裂域. 记 K_4 为克莱因四元数群，C_4 为 4 阶循环群，D_4 为 4 元二面体群.

$$\mathrm{Gal}(f(x)/F)=\begin{cases} K_4, & g(x)\text{在 } F \text{ 中完全分裂} \\ C_4, & g(x)\text{在 } F \text{ 中有且仅有一个根且}f(x)\text{在 } K \text{ 上可约} \\ D_4, & g(x)\text{在 } F \text{ 中有且仅有一个根且}f(x)\text{在 } K \text{ 上不可约} \\ A_4, & g(x)\text{在 } F \text{ 中不可约且}D(g)\in F^2 \\ S_4, & g(x)\text{在 } F \text{ 中不可约且}D(g)\notin F^2 \end{cases}$$

第八章第 18 题

设 F 的特征不为 2，$f(x)=x^4+ax^2+b\in F[x]$ 不可约，G 为 $f(x)$ 的 Galois 群. 通过讨论 a 和 b 的取值，决定 G 的所有可能情况.

四次多项式 Galois 群的结构

情况 1：b 是 F 的一个平方数

- 首先计算预解式 $g(x)=x^3-2ax^2+(a^2-4b)x=x((x-a)^2-4b)$
- 设 $b=t^2,t\in F$，则 $g(x)=x(x-a-2t)(x-a+2t)$ 在 F 中完全分解.
- 根据四次多项式 Galois 群的结构，$G\cong K_4=<(12)(34),(13)(24)>\subset S_4$.

第八章第 18 题情况 2

b 不是 F 的平方数，$b(a^2-4b)$ 是 F 的平方数.

四次多项式 Galois 群的结构和分裂域结构

情况 2 证明

- $g(x)$ 在 F 上的分裂域 K 是 F 上的二次扩张，取 $t\in\overline{F}$ 使得 $t^2=b$，则 $K=F(t)$.
- $f(x)=(x^2+\frac{a}{2})^2-\frac{a^2-4b}{4}=\frac{1}{b}\left[(tx^2+\frac{ta}{2})^2-\frac{b(a^2-4b)}{4}\right]$.
- 若 $b(a^2-4b)$ 是 F 的平方数，则 $f(x)$ 在 $K=F(t)$ 上可约.
- 根据四次多项式 Galois 群的结构，$G\cong C_4=<(1234)>\subset S_4$.

第八章第 18 题情况 3

b 不是 F 的平方数，$b(a^2-4b)$ 不是 F 的平方数.

四次多项式 Galois 群的结构和扩域中的元素表达

证明

- 反设 $f(x)$ 在 K 上可约，则由 $f(x)$ 在 F 上不可约，可写作 $f(x)=(x^2+a_1x+b_1)(x^2+a_2x+b_2)$.
- 展开得到 $a_1+a_2=0$ 且 $a_1b_2+a_2b_1=0$，$b_1b_2=b$，$a_1a_2+b_1+b_2=a$.
- 若 $a_1=0$，则 $b_1-b_2=m+nt\notin F$，推出 $b_1-b_2=nt(n\neq 0)$，因此 $b(a^2-4b)=n^2b^2$ 矛盾.
- 若 $a_1\neq 0$，则 $b_1-b_2=0$，推出 $b=b_1^2$ 和 $a=2b_1-a_1^2$.
- 注意到 $K=F(t)=F(b_1)$，设 $a_1=m+nb_1$，则 $a=2b_1-m^2-bn^2-2nmb_1$.
- 因此 $nm=1$ 且 $m^2+bn^2+a=0$，这表明 $f(m)=0$ 矛盾. 因此 $f(x)$ 在 K 上不可约，有 $G\cong D_4$.

问题补充和方法扩张

问题 1

任给 n 阶 Abel 群 G，能否找到域扩张 $L/\mathbb{Q}$ 使得 $\mathrm{Gal}(L/\mathbb{Q}) = G$? 任给一个 S_n 的子群 H 呢？

简要说明

- 注意到 $Abel$ 扩张可以嵌入到分圆扩张中，因此利用分圆扩张的性质即可得到.
- 目前仍然是一个开放问题，被称为 Galois 逆问题.

问题 2

首一无重根的整系数多项式 $f(x)$ 在 $\mathbb{Q}$ 上的群和在 $\mathbb{F}_p$ 上的群有什么联系?

简要说明

- 首一无重根的整系数多项式 $f(x)$ 在 $\mathbb{F}_p$ 上的群是它在 $\mathbb{Q}$ 上的群的子群.
- 如果 $f(x)$ 在 $\mathbb{Q}$ 上的群 (S_n 的子群) 没有 $\deg(f)$ 的轮换，则 $f(x)$ 在每一个 $\mathbb{F}_p$ 上均可约. 反过来也成立.