第十三次习题课

方法提要、习题讲解和内容扩充

助教：邓先涛

2023 年 12 月 11 日

重点知识提要

重点知识提要

- 分圆域与分圆多项式
- Galois 群子群的固定子域：了解固定子域的概念；能够计算简单的子群的固定子域.
- Artin 引理：了解域扩张相对固定子域的 Galois 群；能够应用该引理计算一些多项式在扩域上的 Galois 群.

分圆扩张与分圆多项式

分圆扩张与分圆多项式的基本事实

- 分圆扩张的定义：若 n 与域 F 的特征互素，则称 $F(\zeta_n)$ 为 F 的 n 次分圆扩张，其中 ζ_n 为 n 次本原单位根. 它的极小多项式记作 $\Phi_n(x)$.
- 有理数域上分圆扩张的群：设 n 为正整数，则 $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$.
- 有理数域上分圆扩张之间的关系：$\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{\mathrm{lcm}(m,n)})$，$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{\mathsf{gcd}(m,n)})$.
- 有理数域上分圆多项式：$\Phi_n(x) = \prod_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})}(x - \sigma(\zeta_n)) = \prod_{m\in(\mathbb{Z}/n\mathbb{Z})^\times}(x - \zeta_n^m) \in \mathbb{Z}[x]$.
- 有理数域上分圆多项式公式：$x^n - 1 = \prod_{d|n} \Phi_d(x)$，$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$，其中 μ 是莫比乌斯函数.

n 次本原单位根的极小多项式

设 ζ_n 是 $\mathbb{Q}$ 上固定的 n 次本元根，证明：ζ_n 的极小多项式 $m(x)$ 等于 $\Phi_n(x)=\prod_{m\in(\mathbb{Z}/n\mathbb{Z})^\times}(x-\zeta_n^m)$.

多项式模 p 法

证明

- 注意到 ζ_n 的共轭元落在 $S=\{\zeta_n^m|m\in(\mathbb{Z}/n\mathbb{Z})^\times\}$，因此 $m(x)\mid\Phi_n(x)$.
- 任给素数 $p\nmid n$，设 ζ_n^p 的极小多项式为 $h(x)\neq m(x)$，有 $m(x)h(x)\mid x^n-1$ 且 $h(x^p)=m(x)q(x)$.
- $x^n-1 \bmod p$ 无重根推出 $m(x)$ 和 $h(x)$ 模 p 也是互素，因此 $m(x)q(x)\equiv(h(x))^p \bmod p$ 矛盾.
- 上述结论表明 ζ_n^p 也是 $m(x)$ 的根，因此 S 中的元素均是 $m(x)$ 的根，推出 $\deg(m(x))=\varphi(n)$.

思维拓展

仿造 244 页 22 题的证明方法，利用莫比乌斯反演公式证明第五点有理数域上分圆多项式公式

第七章第 32 题第 1 问

设 $n = p_1^{r_1} \cdots p_s^{r_s}$，则 $\Phi_n(x) = \Phi_{p_1 \cdots p_s}(x^m)$，其中 $m = \frac{n}{p_1 \cdots p_n}$.

$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$

证明

- 注意到 $\mu(n/d)$ 只有在 $n/d \mid p_1 \cdots p_s$ 时不取零，因此 $\Phi_n(x) = \prod_{d|p_1 \cdots p_s}(x^{dm} - 1)^{\mu(p_1 \cdots p_s/d)}$.
- 注意到 $\Phi_{p_1 \cdots p_s}(x) = \prod_{d|p_1 \cdots p_s}(x^d - 1)^{\mu(p_1 \cdots p_s/d)}$
- 因此 $\Phi_{p_1 \cdots p_s}(x^m) = \prod_{d|p_1 \cdots p_s}(x^{md} - 1)^{\mu(p_1 \cdots p_s/d)} = \Phi_n(x)$ 是恒等式.

第七章第 32 题第 2 问

若 n 为正奇数，则 $\Phi_{2n}(x)=\Phi_n(-x)$.

数论函数的初等变形

证明

- 有 $\Phi_{2n}(x)=\prod_{d|2n}(x^d-1)^{\mu(2n/d)}=\prod_{d|n}(x^d-1)^{\mu(2n/d)}\prod_{d|n}(x^d-1)^{\mu(n/d)}\prod_{d|n}(x^d+1)^{\mu(n/d)}$.
- 注意到 $\prod_{d|n}(x^d-1)^{\mu(2n/d)}\prod_{d|n}(x^d-1)^{\mu(n/d)}=1$.
- $\Phi_{2n}(x)=\prod_{d|n}(x^d+1)^{\mu(n/d)}=\prod_{d|n}\left((-x)^d-1\right)^{\mu(n/d)}\cdot\prod_{d|n}(-1)^{\mu(n/d)}$
- 由于 $\sum_{d|n}\mu(n/d)=0(n>1)$，因此 $\prod_{d|n}(-1)^{\mu(n/d)}=(-1)^{\sum_{d|n}\mu(n/d)}=1$.
- $\Phi_{2n}(x)=\prod_{d|n}\left((-x)^d-1\right)^{\mu(n/d)}\cdot\prod_{d|n}(-1)^{\mu(n/d)}=\prod_{d|n}\left((-x)^d-1\right)^{\mu(n/d)}=\Phi_n(-x)$.

思维拓展

试用一般多项式相等的证明方法证明该结论. 即证明 $\Phi_{2n}(x)\mid\Phi_n(-x)$ 和 $\Phi_n(-x)\mid\Phi_{2n}(x)$.

第七章第 32 题第 3 问

设 p 为素数且 $p \nmid n$，则 $\frac{\Phi_n(x^p)}{\Phi_n(x)} = \Phi_{pn}(x)$.

数论函数的初等变形

证明

- 利用公式 $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$
- 得到 $\Phi_{pn}(x) = \prod_{d|pn}(x^d - 1)^{\mu(pn/d)} = \prod_{d|n}(x^d - 1)^{\mu(pn/d)} \cdot \prod_{d|n}(x^{pd} - 1)^{\mu(n/d)}$.
- $\frac{\Phi_n(x^p)}{\Phi_n(x)} = \prod_{d|n}(x^d - 1)^{-\mu(n/d)} \cdot \prod_{d|n}(x^{pd} - 1)^{\mu(n/d)}$.
- 莫比乌斯函数 μ 是乘性函数，$p \nmid n$ 和 $d \mid n$ 推出 $\mu(pn/d) = \mu(p)\mu(n/d) = -\mu(n/d)$.

思维拓展

利用第一问可以看出，若 $p \mid n$，则 $\Phi_{pn} = \Phi_n(x^p)$. 事实上，上述结论显示，只需要计算素数次分圆多项式就可以计算一般分圆多项式表达.

第七章第 33 题

设 ζ_n 是复数域中的本原 $n>2$ 次单位根，证明：$[\mathbb{Q}(\zeta_n+\zeta_n^{-1}):\mathbb{Q}]=\frac{\varphi(n)}{2}$.

扩张次数的传递性：$[E:F]=[E:K][K:F]$.

证明

- 注意到 ζ_n 满足方程 $x^2-(\zeta_n+\zeta_n^{-1})x+1=0$，因此 $[\mathbb{Q}(\zeta_n):\mathbb{Q}(\zeta_n+\zeta_n^{-1})]\leq 2$.
- 注意到 $\zeta_n+\zeta_n^{-1}\in\mathbb{R}$，且 $\zeta_n\notin\mathbb{R}$，因此 $[\mathbb{Q}(\zeta_n):\mathbb{Q}(\zeta_n+\zeta_n^{-1})]=2$.
- 利用 $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\varphi(n)$ 和扩张次数传递性，得到 $[\mathbb{Q}(\zeta_n+\zeta_n^{-1}):\mathbb{Q}]=\frac{\varphi(n)}{2}$.

思维拓展

能否找到代数数 α 使得 $\mathbb{Q}(\alpha)=\mathbb{Q}(\alpha+\alpha^{-1})$？能否找到虚代数数 α 使得 $\mathbb{Q}(\alpha)=\mathbb{Q}(\alpha+\alpha^{-1})$？

第八章第 20 题

设 F 是特征不为 2 的域，若 F 包含一个 n 次本原单位根且 n 为奇数，则 F 包含一个 $2n$ 次本原单位根.

本原根的基本定义

思维拓展

32 题及教材中关于 Φ_n 的结果，添加什么限制可以放在正特征的域上？

证明

- 设 ζ_n 为 F 中的一个 n 次本原单位根.
- 令 $t=-\zeta_n$，设 m 是最小使得 $t^m=1$ 成立的的正整数.
- 注意到 $t^{2n}=1$，因此 $m \mid 2n$.
- 注意到 $\zeta_n^{2m}=1$，因此 $n \mid 2m$.
- n 为奇数，因此 $m=2n$.
- 易错点：直接使用 $\Phi_n(-x)=\Phi_{2n}(x)$.

第八章第 21 题

设 F 是 $\mathbb{Q}$ 上的一个有限扩张，证明 F 只包含有限多个单位根.

欧拉函数的粗略估计

思维拓展

设 F 是 $\mathbb{Q}$ 上的有限扩张，是否存在中间域 K 使得 K 中不包含 $n > 2$ 次单位根，且 $F = K(\zeta_m)$.

证明

- 若 $\zeta_n \in F$，则 $[F : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$
- 直接利用公式验证 $\varphi(n) \geq \frac{\sqrt{n}}{2}$.
- $S_r := \{x \in \mathbb{C} | \exists n \leq r, x^n = 1\}$ 是有限的.
- 若 F 中有无限多个单位根，则存在 $\zeta_m \in F$，这里 $m > 4[F : \mathbb{Q}]^2$.
- $[F : \mathbb{Q}] > \varphi(m) \geq \sqrt{m}/2 > [F : \mathbb{Q}]$ 矛盾.

给定子群的固定子域

第八章第 11 题

设 $E=\mathbb{F}_p(t)$ 为单超越扩张，$\sigma \in \mathrm{Gal}(E/\mathbb{F}_p)$ 使得 $\sigma(t)=t+1$，令 $G=<\sigma>$，决定 G 的不动域 E^G.

不动域定义：$E^G=\{\alpha \in E|\tau(\alpha)=\alpha, \forall \tau \in G\}$

总结

Artin 引理的作用是确定寻找不动元素的范围，否则无法确定是否已经找完了所有的不动元.

证明

- 确定群的大小：由于 $\sigma^m(t)=t+m$，因此 G 是 p 阶群，Artin 引理表明 $[E:E^G]=p$.
- 确定不动元素：注意到 $\sigma(t^p-t)=(t+1)^p-(t+1)=t^p-t$，因此 $\mathbb{F}_p(t^p-t) \subset E^G$.
- 检验：$p \geq [E:\mathbb{F}_p(t^p-t)] \geq [E:E^G]=p$ 推出二者相等.

第八章第 12 题

设 $E=\mathbb{C}(t)$，$\sigma,\tau\in \mathrm{Gal}(E/\mathbb{C})$ 满足 $\sigma(t)=\omega t,\tau(t)=t^{-1}$，其中 ω 是 3 次本原根. 证明：$G=<\sigma,\tau>$ 是 6 阶群，$E^G=\mathbb{C}(t^3+t^{-3})$.

Artin 引理

思维拓展

将题中 ω 改为 ζ_n，即 n 次本原单位根，那么 G 的表现如何？固定子域是什么？

证明

- 验证得到 $\sigma^3=1=\tau^2$，$\tau\sigma=\sigma^2\tau$，因此 G 中元素形如 $\sigma^i\tau^j$ 为 6 阶群. $[E:E^G]=6$.
- 进一步有 $\mathbb{C}(t^3+t^{-3})\subset E^G$
- 因此 $6\geq[E:\mathbb{C}(t^3+t^{-3})]\geq[E:E^G]=6$，推出二者相等.

Lüroth 定理

设 F 是一个域，t 是未定元，则域扩张 $F(t)/F$ 的每一个中间域均形如 $F(u)$，其中 $u \in F(t)$.

超越扩张中的不可约多项式

思维拓展

L 的固定子群 $\mathrm{Gal}(F(t)/L)$ 应该如何通过 $L = F(u)$ 和 $u = \frac{f(t)}{g(t)}$ 去刻画？

证明

- 设 $L \neq F$ 是中间域，$u = \frac{f(t)}{g(t)} \in L \setminus F$ 是集合 $L \setminus F$ 中次数最低的元素，这里次数定义为 $\max\{\deg(f(t)), \deg(g(t))\}$，且二者互素.
- $h(T) = f(T) - ug(T) \in L[T]$ 是 t 在 L 上的零化多项式，$f(T)$ 和 $g(T)$ 互素推出 $h(T)$ 在 L 中不可约，$[F(t) : L] = \deg(h(T))$.
- $h(T) \in F(u)[T]$ 是不可约的，推出 $h(T)$ 在 $F(u)$ 中不可约，$[F(t) : F(u)] = \deg(h(T))$.
- $F(u) \subset L$ 推出 $F(u) = L$.

固定子域与 Galois 子群的对应

设 $\mathbb{F}_{q^m}$ 为有限域，证明 $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ 的子群 H 所对应的固定子域 $\mathbb{F}_{q^m}^H$ 恰好给出了 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 的所有中间域.

有限域上有限扩张的 Galois 群

总结

该结论推至一般的域上，就是域扩张的 Galois 基本定理. 即 Galois 扩张的中间域与扩张的 Galois 群的子群一一对应.

证明

- $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ 是 m 阶循环群，循环群的生成元为 $\sigma : x \to x^q$.
- 作为循环群，任给 $n \mid m$ 恰有一个 m/n 阶子群 $H_n =< \sigma^n >$.
- 可以验证 $\mathbb{F}_{q^m}^{H_n} = \mathbb{F}_{q^n}$，这与 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 的中间域一一对应.

计算 Galois 群

第八章第 17 题第 3 问

计算 x^4-2 在 $\mathbb{Q}(\sqrt{-1})$ 上的群.

Artin 引理及其推论：$\mathrm{Gal}(K/K^H)=H$

思维拓展

试用教材 P262 定理 6 直接解决该问题.

证明

- 彭老师 week13 课件上给出了 x^4-2 在 $\mathbb{Q}$ 上的群为 $D_4=<\sigma,\tau>$.
- 作用方式：
  $\sigma(\sqrt{-1})=\sqrt{-1},\sigma(\sqrt[4]{2})=\sqrt{-1}\sqrt[4]{2}$;
  $\tau(\sqrt{-1})=-\sqrt{-1},\tau(\sqrt[4]{2})=\sqrt[4]{2}$.
- 现在需要确定固定 $\mathbb{Q}(\sqrt{-1})$ 的子群 H，可以验证 $H=<\sigma>$.
- x^4-2 在 $\mathbb{Q}(\sqrt{-1})$ 上的群为 H，是四阶循环群.

第八章第 35 题

写出 $f(x) = x^5 - 2$ 在 $\mathbb{Q}$ 上的 Galois 群.

生成元的代数关系

思维拓展

任给素数 p 确定 $x^p - 2$ 在 $\mathbb{Q}$ 上的 Galois 群.

证明

- f 在 $\mathbb{Q}$ 上的分裂域为 $K = \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$.
- $x^4 + x^3 + x^2 + x + 1$ 在 $\mathbb{Q}(\sqrt[5]{2})$ 上不可约，这是因为 $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$ 没有非平凡中间域.
- $[K : \mathbb{Q}] = 20$，表明 ζ_5 与 $\sqrt[5]{2}$ 是互不影响.
- 确定群中的元素：$\sigma_i : \sqrt[5]{2} \to \sqrt[5]{2} \cdot \zeta_5^i$，$\tau_j : \zeta_5 \to \zeta_5^j$，其中 $0 \le i \le 4$，$1 \le j \le 4$.
- $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_i \tau_j | 0 \le i \le 4, 1 \le j \le 4\}$.

第八章第 35 题第 2 问

写出 $f(x)=x^5-2$ 在 $\mathbb{Q}(\sqrt{5})$ 上的 Galois 群.

Artin 引理及其推论

思维拓展

$\mathbb{Q}(\sqrt{5})$ 是 $\mathbb{Q}(f)$ 的二次子域，还有其他不同的二次子域吗？对于素数 p，令 $f(x)=x^p-2$，试确定 $\mathbb{Q}(f)$ 的所有二次子域.

证明

- $s=\zeta_5+\zeta_5^4$ 满足 $s^2=\zeta_5^2+\zeta_5^3+2=-s+1$，因此 $s=\frac{-1\pm\sqrt{5}}{2}$.
- 这表明 $\sqrt{5}\in K=\mathbb{Q}(f)$，且 $\tau_4(\sqrt{5})=\sqrt{5}$.
- 这表明 $\sigma_i\tau_j(0\le i\le 4, j=1,4)$ 固定 $\sqrt{5}$
- $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{5}))=\{\sigma_i\tau_j|0\le i\le 4, j=1,4\}$.

置换群 S_n 的生成元

第二章第 10 题

证明 S_n 可由 $n-1$ 个对换 $(1i)(2 \leq i \leq n)$ 生成，S_n 也可由 $n-1$ 个对换 $(i\ i+1)(1 \leq i \leq n-1)$ 生成.

S_n 中元素运算法则

思维拓展

S_n 中的元素均可写作对换的乘积，$\sigma \in S_n$，那么 σ 必可用最少的对换的乘积进行表达，此时对换的数量如何刻画？如 $(12) = (12)(34)(34)$，前者就是最少的.

证明

- S_n 中任一元素均可写作不相交的轮换乘积.
- $(i_1\ i_2 \cdots\ i_k) = (1\ i_1)(1\ i_k) \cdots (1\ i_1)$，其中 i_j 是两两不同的数，且 $i_j \neq 1 (j \neq 1)$.
- 这表明 S_n 中的任一元素可以写作 $(1\ i)$ 型对换乘积.
- 注意到 $(1\ i) = (12)(23) \cdots (i-1\ i)(i-1\ i-2) \cdots (32)(21)$，因此命题成立.

第二章第 11 题

S_n 可由 (12) 和 $(123\cdots n)$ 生成.

S_n 中元素运算法则

思维拓展

是否任给对换和 n 轮换均可生成 S_n?

证明

- 只需要去生成 $(i\ i+1)(1\le i\le n-1)$.
- $(12\cdots n)(i\ i+1)(12\cdots n)^{-1}=(i+1\ i+2)$, 其中 i 取 1 到 $n-2$.
- 将 (12) 代入即可生成 $(23),\cdots,(n-1\ n)$.

问题补充和方法扩张

问题 1

设 L/F 是域扩张，$f(x) \in F[x]$ 是不可约多项式，若已知 f 在 F 上的群，如何考虑 $f(x)$ 在 L 上的群？

简要说明

- 设 E 是 f 在 F 上的分裂域，则 f 在 L 上的分裂域为 EL.
- 有 $\mathrm{Gal}(EL/L) \cong \mathrm{Gal}(E/E \cap L)$，即 $f(x)$ 在 L 上的群为 $\mathrm{Gal}(E/F)$ 中保持 $E \cap L$ 元素不动的元素全体. 特别的，若 $E \cap L = F$，则二者相同.

问题 2

Kronecker-Weber 定理表明每一个有限 Abel 数域 (即 Galois 群为交换群的 $\mathbb{Q}$ 上有限 Galois 扩张) 均含于某一个分圆域中. $\mathbb{Q}$ 上的二次扩张总是一个 Abel 数域，那么如何寻找包含它的分圆域呢？

简要说明

- 回顾 $\zeta_5+\zeta_5^4=\frac{-1\pm\sqrt{5}}{2}$. 类似的，$1+\zeta_p+\cdots+\zeta_p^{p-1}=1+\sum_{a=1}^{(p-1)/2}\zeta_p^{a^2}+\sum_{b=1}^{(p-1)/2}\zeta_p^{rb^2}$，其中 r 是模 p 的非平凡剩余.
- 进行变形得到 $1+2\sum_{a=1}^{(p-1)/2}\zeta_p^{a^2}=\sum_{a=1}^{(p-1)}\left(\frac{a}{p}\right)\zeta_p^a=s$.
- $s^2=\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(\frac{ab}{p}\right)\zeta_p^{a+b}=\sum_{a=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{c}{p}\right)\zeta_p^{a(1+c)}=(-1)^{(p-1)/2}p$.
- 因此 $\sqrt{p}\in\mathbb{Q}(\zeta_{4p})$，进一步的 $\sqrt{d}\in\mathbb{Q}(\zeta_{4d})$.