第十一次习题课

小测讲解、方法提要、习题讲解和内容扩充

助教：邓先涛

2023 年 11 月 27 日

小测讲解

小测第 1 题

有多少个互不同构的 72 阶交换群?

有限交换群结构定理

总结

设 $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$，$n$ 阶交换群的互不同构类型的数目是 $h(e_1) \cdot h(e_2) \cdots h(e_r)$，其中 $h(e)$ 表示 e 的整数分拆数.

证明

- 注意到 $72 = 2^3 \times 3^2$，初等因子分解

$$(2^3, 3^2), \quad (2^3, 3, 3)$$
$$(2^2, 2, 3^2), \quad (2^2, 2, 3, 3)$$
$$(2, 2, 2, 3^2), \quad (2, 2, 2, 3, 3)$$

- 不变因子分解

$$(2^3 \times 3^2), \quad (2^3 \times 3, 3)$$
$$(2^2 \times 3^2, 2), \quad (2^2 \times 3, 2 \times 3)$$
$$(2 \times 3^2, 2, 2), \quad (2 \times 3, 2 \times 3, 2)$$

小测第 2 题

设 $\alpha \in \mathbb{R}$ 为多项式 $f(x) = x^3 - 3x + 4 \in \mathbb{Q}[x]$ 的实根，证明 $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$，将 α^4 和 $(\alpha - 1)^{-1}$ 表示为 $1, \alpha, \alpha^2$ 的 $\mathbb{Q}$ 线性组合.

单扩张扩张次数等于极小多项式次数

思维拓展

你能否对 $f(x)$ 进行变形使得它可以用 Eisenstein 判别法？你能否找到 $\mathbb{Q}$ 上的一个不可约多项式 $f(x)$ 使得 $f(\frac{x+a}{b})$ 总是对 Eisenstein 判别法失效？

证明

- 三次多项式在 F 上不可约当且仅当在 F 上没有根
- 验证 $f(x)$ 的可能的根为 $\pm 1, \pm 2, \pm 4$，均不是多项式的真正的根，因此多项式不可约.
- $\alpha^4 = \alpha\alpha^3 = 3\alpha^2 - 4\alpha.$
- 设 $(\alpha - 1)(a\alpha^2 + b\alpha + c) = 1$，展开得到 $(b - a)\alpha^2 + (c - b + 3a)\alpha - c - 4a = 1.$
- $a = b = -\frac{1}{2}$，$c = 1.$

小测第 3 题

设 K/F 为域的有限扩张，$\overline{F}$ 为 F 的代数闭包，$\sigma : K \to \overline{F}$ 是 F 嵌入. 证明：$\sigma(K)$ 是 $\overline{F}/F$ 的中间域且 $[\sigma(K) : F] = [K : F]$.

有限扩张可以写作单扩张链

思维拓展

利用 K 的内在性质刻画 K 的 F 嵌入 σ 的个数.

证明

- 设 $K = F(\alpha_1, \cdots, \alpha_n)$，且 $F \subset F(\alpha_1) = F_1 \subset F(\alpha_1, \alpha_2) = F_2 \subset \cdots \subset F(\alpha_1, \cdots, \alpha_n) = F_n = K$.
- $\sigma(K)$ 显然是一个域，且包含 F，因此是中间域.
- 得到 $\sigma(F_i) \subset \sigma(F_{i+1}) = \sigma(F_i)(\sigma(\alpha_{i+1}))$.
- $[\sigma(F_{i+1}) : \sigma(F_i)] = [F_{i+1} : F_i]$，命题成立.

重点知识提要

重点知识提要

- 可分扩张：可分扩张的基本概念；可分扩张的性质；可分闭包和纯不可分扩张的概念.
- 正规扩张：正规扩张的基本概念；正规扩张的刻画和性质；正规闭包的概念.
- 扩张所对应的 F 自同构映射和嵌入映射

正规扩张

正规扩张

- 正规扩张：对于代数扩张 K/F，若任给 $\alpha \in K$，α 的 F 共轭元也均在 K 中.
- 有限正规扩张：对于有限扩张 K/F，K/F 正规当且仅当 K 是 F 上的一个多项式的分裂域.
- 正规闭包：对于代数扩张 K/F，K/F 的正规闭包是包含 K 的最小的 F 的正规扩张.
  注意区分：F 在 K 中的正规闭包和 K/F 的正规闭包.
- 正规扩张的 F 自同构：设 K/F 是一个正规扩张，任给 $\alpha \in K$ 和 α 的一个 F-共轭元 α'，则 F 同构 $\sigma : F(\alpha) \to F(\alpha')$ 可以提升为 K 的自同构.

第七章第 14 题

设 $F \subset K \subset L$ 是代数扩张链，如果 L/K 和 K/F 均正规，那么 L/F 是否正规？

证明

- 取 $F = \mathbb{Q}$，$K = \mathbb{Q}(\sqrt{2})$ 和 $L = \mathbb{Q}(\sqrt[4]{2})$.
- L/F 不是正规扩张，因为 $i \notin L$.

二次扩张总是正规扩张

思维拓展

设 $F \subset K \subset L$ 是代数扩张链，那么 L/F 是正规扩张能否推出 L/K 是正规扩张？L/F 是正规扩张能否推出 K/F 是正规扩张？

第七章第 17 题

设 K, L 是 E/F 的中间域，若 K/F 和 L/F 均正规，则 KL/F 和 $K \cap L/F$ 也正规.

正规扩张是针对元素的性质

思维拓展

举例说明上述命题的逆命题不成立. 即 KL/F 和 $K \cap L/F$ 均正规推不出 K/F 和 L/F 均正规.

证明

- K 和 L 是代数扩张，验证 L 和 K 的复合域为 $KL = \{\sum_i a_i b_i | a_i \in K, b_i \in L\}$.
- 任给 $\alpha \in KL$ 写作 $\alpha = a_1 b_1 + \cdots + a_n b_n$.
- 设 a_i 的极小多项式为 f_i，b_j 的为 g_j，则 α 落在 $\prod_{i,j} f_i g_j$ 的分裂域 E' 中.
- K 和 L 是 F 的正规扩张意味着 $E' \subset KL$，因此 α 的共轭元在 KL 中.
- 任给 $\alpha \in K \cap L$，α 的共轭元会在 $K \cap L$ 中，因此 $K \cap L/F$ 正规. 注：上述证明用映射的观点来看会更加简洁.

补充题

设 E/F 是正规扩张，$f(x) \in F[x]$ 是不可约的，则 $f(x)$ 在 E 上可以分解为 $f(x) = [f_1(x) \cdots f_r(x)]^k$，其中 f_i 是次数相同的两两互素的不可约多项式，F 特征为 0 时，$k = 1$；F 特征为素数 p 时，$k = p^e$.

映射观点下的正规扩张

证明

- 任给 i 和 j 存在 E 的 F 自同构 σ 使得 $\sigma(f_i) = f_j$. 故 $\deg(f_i) = \deg(f_j)$ 对一切 $1 \leq i, j \leq r$ 成立.
- 若是特征 0 域，则没有重根，立刻得到 $k = 1$.
- 若是特征 p 域，则考察 $f_1 \cdots f_r$ 的系数，它们在任意 σ 作用下不变，因此共轭元只有自己.
- 考察 f_i 的幂次，同样利用同构进行轮换得到，$f_i^{k_i}$ 变成 $f_j^{k_i}$，推出 $k_i = k_j$ 幂次相同.
- 设 $h = f_1 \cdots f_r = \sum_{i=0}^{m} a_i x^i$，有最小的 e 使得 $a_i^{p^e} \in F$ 对一切 $0 \leq i \leq m$ 成立. 推出 $h^{p^e} \in F[x]$.
- 由 f 的不可约性 $f(x) \mid h(x)^{p^e}$，由 e 的极小性 $f(x) = h(x)^{p^e}$，因此命题成立.

可分扩张

可分扩张

- 可分扩张：对于代数扩张 K/F，若 K 中元素的极小多项式均没有重根.

  有限可分扩张扩张等价刻画：对于有限代数扩张 K/F，K/F 是可分扩张当且仅当恰有 $[K:F]$ 个 F 嵌入 $K \to \overline{F}$.
- 可分闭包：对于代数扩张 K/F，K 中的所有可分元构成的集合是一个子域，称为可分闭包.
- 可分扩张的性质：若 K/F 为有限可分扩张，则存在 $\gamma \in K$ 使得 $K = F(\gamma)$.
- 纯不可分扩张：对于代数扩张 K/F，若它的可分闭包是 F，则称 K/F 是纯不可分扩张.
- 纯不可分元：称 α 是纯不可分元，若 $F(\alpha)/F$ 是纯不可分扩张.

可分元的性质

设 K/F 为域扩张，$\alpha \in K$ 是可分元，则 $F(\alpha)/F$ 是可分扩张.

可分扩张的等价定义

思维拓展

设 K/F 是有限扩张，$K^p := \{x^p | x \in K\}$. 证明 K/F 是可分扩张当且仅当 $K = F(K^p)$.

证明

- 设 α 次数为 n，则 $[F(\alpha) : F] = n$.
- 设 α 的共轭元为 $\alpha = \alpha_1, \alpha_2, \cdots, \alpha_n$.
- $\sigma_i : F(\alpha) \to F(\alpha_i) \subset \overline{F}$ 为两两不同 F 嵌入
- 等价定义表明 $F(\alpha)/F$ 是可分扩张.

纯不可分元的刻画

设 F 的特征为 p，$\alpha \in \overline{F}$ 且 $\alpha \notin F$，α 是纯不可分元当且仅当存在正整数 $n \geq 1$ 使得 $\alpha^{p^n} \in F$.

纯不可分扩张的定义和特征 p 域上的不可约多项式

思维拓展

设 t 为未定元，p 为奇素数，$\mathbb{F}_p$ 特征为 p 的素域，$f(x) = x^{2p} - tx^p + 1$，$K/\mathbb{F}_p(t)$ 为 $f(x)$ 在域 $\mathbb{F}_p(t)$ 上的分裂域，求出 $K/\mathbb{F}_p(t)$ 的可分闭包.

证明

- 若存在 n 使得 $\alpha^{p^n} \in F$，任给 $\beta \in F(\alpha)$ 写作 $\beta = f(\alpha)$，有 $\beta^{p^n} \in F$.
- β 在 F 上的零化多项式为 $(x-\beta)^{p^n}$，因此要么在 F 上，要么不可分.
- 若 α 是纯不可分元，则 $F(\alpha)/F$ 是纯不可分扩张.
- 设 α 的极小多项式为 $f(x)$ 写作 $g(x^{p^n})$，则 $g(x)$ 不可约，且 $g(\alpha^{p^n}) = 0$.
- $F(\alpha^{p^n})$ 为可分扩张推出 $\alpha^{p^n} \in F$.

推论

设 F 是特征 p 域，K/F 为域扩张，$\alpha \in K$ 是代数元，则存在正整数 n 使得 α^{p^n} 为可分元.

极小多项式的性质和可分元的性质

证明

- 设 α 的极小多项式为 $f(x)$ 写作 $g(x^{p^n})$，其中 $g(x)$ 是 F 上的不可约多项式.
- 同样道理，$g(x)$ 没有重根，因此 $g(x)$ 是可分多项式.
- α^{p^n} 的极小多项式是 $g(x)$，因此是可分元.

第七章第 26 题

设域扩张 K/F 中的非零元素 α 和 β 分别是 F 上的可分元和纯不可分元，证明

$$F(\alpha,\beta)=F(\alpha+\beta)=F(\alpha\beta).$$

纯不可分元的等价刻画

思维拓展

题中纯不可分条件是否必要？即是否存在非零元素 α 和 β 分别是 F 上的可分元和不可分元，使得 $F(\alpha,\beta)\neq F(\alpha+\beta)$?

证明

- β 纯不可分意味着存在 n 使得 $\beta^{p^n}\in F$，这里素数 p 是 F 的特征.
- $\alpha^{p^n}=(\alpha+\beta)^{p^n}-\beta^{p^n}\in F(\alpha+\beta)$
- α^{p^n} 的极小多项式没有重根，且 $x^{p^n}-\alpha^{p^n}$ 可以零化 α.
- α 在 $F(\alpha+\beta)$ 上的极小多项式为 $x-\alpha$. 推出 $\alpha\in F(\alpha+\beta)$.
- $F(\alpha,\beta)=F(\alpha\beta)$ 同理可得.

第七章第 28 题

设 F 的特征为素数 p，若不可约多项式 $f(x)$ 满足 $p \nmid \deg(f(x))$，则 $f(x)$ 可分. 特别的，若扩域 K 满足 $p \nmid [K:F]$，则 K/F 是可分扩张.

不可约多项式的性质

思维拓展

设域为 F，给出 F 不可分多项式存在的充分必要条件.

证明

- $p \nmid \deg(f(x))$ 意味着 $f'(x) \neq 0$.
- 因此 $\gcd(f(x), f'(x)) = 1$ 推出 $f(x)$ 无重根.
- 任给 $\alpha \in K$，$p \nmid [F(\alpha):F]$.
- α 的极小多项式没有重根，因此可分.

第七章第 29 题

设域的特征为 p，K/F 为域扩张，$\alpha \in K$ 是代数且可分的充要条件是 $F(\alpha) = F(\alpha^{p^n})$ 对一切正整数 $n \geq 1$ 成立.

可分元的极小多项式无重根

思维拓展

如果只是说存在一个 $n \geq 1$ 使得 $F(\alpha) = F(\alpha^{p^n})$，那么能否推出 α 是代数可分元吗？

证明

- 前推后：显然有 $F(\alpha^{p^n}) \subset F(\alpha)$
- α 在 $F(\alpha^{p^n})$ 上的零化多项式 $x^{p^n} - \alpha^{p^n}$，因此极小多项式为 $x - \alpha$，推出 $\alpha \in F(\alpha^{p^n})$.
- 后推前：代数是显然的，否则 $\alpha \notin F(\alpha^p)$.
- 取 n 使得 α^n 为可分元，则 $\alpha \in F(\alpha^n)$ 为可分元.

单代数扩张的刻画

单代数扩张

- 单代数扩张：对于代数扩张 K/F，称 K/F 是单代数扩张，若存在 $\gamma \in K$ 使得 $K = F(\gamma)$.
- 设 K/F 是有限可分扩张，则 K/F 是单代数扩张. 特别的，有限域的有限扩张均为单代数扩张.
- 单代数扩张的性质：若 $K = F(\alpha)$ 是单代数扩张，则 $[K : F]$ 等于 α 的次数.

单代数扩张的刻画

设 F 是无限域，若代数扩张 K/F 只有有限多个中间域，则 K/F 是单扩张.

鸽笼原理

思维拓展

如何有效判断一个无限域的扩张只有有限多个中间域呢？

证明

- 有限多个中间域表明是有限扩张，因此可以令 $K = F(\alpha_1, \cdots, \alpha_n)$.
- F 是无限域，$F(\alpha_1 + x\alpha_2)$ 作为中间域只有有限多种可能，因此存在 $x \neq y$ 使得 $F(\alpha_1 + x\alpha_2) = F(\alpha_1 + y\alpha_2)$
- 取 $\gamma = \alpha_1 + x\alpha_2$，有 $F(\alpha_1, \alpha_2) = F(\gamma)$.
- $K = F(\gamma, \alpha_3, \cdots, \alpha_n)$，以此类推即可.

单代数扩张的刻画

若代数扩张 K/F 是一个单扩张，则 K/F 只有有限多个中间域.

极小多项式与扩张次数

思维拓展

利用该思路写出 $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ 的所有中间域.

证明

- 设 $K=F(\gamma)$，$f(x)\in F[x]$ 为 γ 在 F 上的极小多项式，L 为中间域.
- 设 $f_L=x^m+a_{m-1}x^{m-1}+\cdots+a_0\in L[x]$ 为 γ 在 L 上的极小多项式.
- 则 $L'=F(a_0,\cdots,a_{m-1})\subset L$，且极小多项式 $f_L(x)$ 也是 L' 上的不可约多项式.
- $K=L'(\gamma)\subset L(\gamma)=K$，有 $[K:L]=\deg(f_L)=[K:L']$，因此 $L=L'$
- $f_L\mid f$ 在 F 的代数闭包中只有有限多中选择，因此 L 只有有限多种可能.

推论：第七章第 40 题

单代数扩张的中间域也是单代数扩张.

K/F 是单代数扩张当且仅当 K/F 只有有限多个中间域

思维拓展

是否存在代数扩张不是单代数扩张，但是它的真的中间域均是单扩张呢？

证明

- 设 K/F 是单代数扩张，L/F 是中间域.
- L/F 的中间域均是 K/F 的中间域，只有有限多个.
- L/F 只有有限多中间域，因此单扩张.

第七章第 31 题

设 $\mathbb{F}_p[x,y]$ 是 $\mathbb{F}_p$ 上二元多项式环，K 为其商域，$F=K^p:=\{a^p|a\in K\}$. 则 $F=\mathbb{F}_p(x^p,y^p)$ 且 K/F 不是单代数扩张.

单代数扩张的次数刻画

思维拓展

试找出 K/F 的可分闭包，并思考可分闭包在单代数扩张中扮演的角色.

证明

- 直接验证 $F=\mathbb{F}_p(x^p,y^p)$，故 $[K:F]=p^2$.
- 设 $K=F(f(x,y))$，则 $t^p-(f(x,y))^p$ 是二元多项式 $f(x,y)$ 在 F 上的零化多项式.
- 推出 $[K:F]\le p$ 与 $[K:F]=p^2$ 矛盾.
- K/F 不是单扩张推出 K/F 有无限多个中间域，且中间域扩张次数是素数，手动找出.
- 令 $f_n(x)=x+y^{np+1}\notin F$，令 $F_n=F(f_n)$.
- 若 $F_n=F_m(n\neq m)$，则 $f_n-f_m\in F_n$，推出 $y(y^{np}-y^{mp})\in F_n$，推出 $y\in F_n$ 矛盾.

单代数扩张的基本事实

- **单代数扩张在可分部分的性质**：设 F 是无限域，对于有限扩张 K/F，记 K_s 为 K/F 的可分闭包，则 K/F 是单代数扩张当且仅当 K/K_s 为单代数扩张.

  推论：对于有限扩张 K/F，若 K 可以写作 $K = F(\alpha_1, \cdots, \alpha_n, \beta)$，其中 β 是 F 上的代数元，同时 α_i 是 $F(\beta)$ 上的可分元，则 K/F 是单代数扩张.

- **完全域上的一元函数域**：设 F 是特征 p 的完全域，即 $F^p := \{x^p | x \in F\} = F$. 设 t 为未定元，则有理函数域 $F(t)$ 上的有限扩张均为单代数扩张.

- **特征 p 域上的单代数扩张**：设 F 是特征 p 域，K/F 是有限扩张，则 K/F 是单代数扩张当且仅当 $[K : F(K^p)] \leq p$.

问题补充和方法扩张

问题 1

可分扩张的正规闭包是否还是可分的？正规扩张的可分闭包是否还是正规的？

简要说明

- 注意到可分扩张的刻画：$K/E/F$ 是代数扩张，K/F 可分当且仅当 K/E 和 E/F 均可分，因此第一个论断正确.
- 后者直接用元素去说明即可.

问题 2

设 F 是一个域，K_i/F 为有限扩张，则 K_i 均可以作为 F 线性空间，那么 $\dim_F(K_1+K_2+\cdots+K_n)$ 应该如何有效计算？

简要说明

- $\dim(K_1+K_2)=\dim(K_1)+\dim(K_2)-\dim(K_1\cap K_2)$
- $\dim(K_1+K_2+K_3)=\dim(K_1)+\dim(K_2+K_3)-\dim(K_1\cap(K_2+K_3))$
- 是否总有 $\dim(K_1\cap(K_2+K_3))=\dim(K_1\cap K_2+K_1\cap K_3)$？在 $F=\mathbb{Q}$ 情况下举反例说明.