第九次习题课

方法提要、习题讲解和内容扩充

助教：邓先涛

2023 年 11 月 13 日

重点知识提要

重点知识提要

- 域扩张的次数：域扩张的次数的传递性；有限扩张的刻画；代数扩张的刻画.
- 尺规作图：三大古典问题的解决.

第七章习题讲解

第七章第 1 题

设 K/F 是有限扩张，$[K:F]=p$ 是一个素数，则任给 $\alpha\in K\setminus F$，有 $K=F(\alpha)$.

扩张次数的传递性：$[K:E][E:F]=[K:F]$.

思维拓展

设 K/F 是有限扩张，定义等价关系 $\alpha\sim\beta$ 当且仅当 $F(\alpha)=F(\beta)$，记 $S=K/\sim$ 为 K 在该等价关系下的等价类集合. S 是否总是有限集？特别的，若 $[K:F]$ 为素数，则 S 是怎样的集合.

证明

- 令 $E=F(\alpha)$，则 $E\neq F$ 且 $[E:F]\mid[K:F]$.
- 注意到 $[E:F]\neq 1$，故 $[E:F]=p$.
- 注：证明域相同，只需要有包含关系，同时扩张次数为 1.

第七章第 2 题

设 K/F 是有限扩张，$\alpha \in K$ 是 F 上的 n 次元素，则 $n \mid [K:F]$.

扩张次数的传递性：$[K:E][E:F] = [K:F]$.

思维拓展 1

设 K/F 为有限扩张，任给 $n \mid [K:F]$，是否总可以找到 $\alpha \in K$ 为 n 次元素？放宽条件来看，是否总可以找到 $E \subset K$ 使得 $[E:F] = n$?

证明

- 令 $E = F(\alpha)$，有 $[K:F] = [K:E][E:F]$.
- 因此有 $n \mid [K:F]$.
- 注：n 次元素的定义是极小多项式次数为 n 次的代数元.

第七章第 4 题

设 K 为 F 上的域扩张，若 $u \in K$ 是 F 上的次数为奇数的代数元，则 $F(u) = F(u^2)$.

$F(\alpha) = F(\beta)$ 当且仅当 $\alpha \in F(\beta)$ 且 $\beta \in F(\alpha)$.

思维拓展

设 u 在 F 上的次数为 n，任给 $d < n$ 满足 $\gcd(n, d) = 1$，是否有 $F(u) = F(u^d)$. 试着找出反例.

证明

- 显然有 $u^2 \in F(u)$ 推出 $F(u^2) \subset F(u)$.
- 设 u 的极小多项式为

  $x^{2n+1} + a_{2n}x^{2n} + \cdots + a_1 x + a_0$.
- $u(u^{2n} + a_{2n-1}u^{2n-2} + \cdots + a_1) + (a_{2n}u^{2n} + \cdots a_2 u^2 + a_0) = 0$
- $u \in F(u^2)$ 推出 $F(u) \subset F(u^2)$.

第七章第 5 题

若 $x^n - a \in F[x]$ 不可约，则任给正整数 $m \mid n$，$x^m - a \in F[x]$ 也是不可约.

多项式的赋值法 (赋待定元)

思维拓展 1

类似可证：$a_n x^n + \cdots + a_1 x + a_0$ 不可约当且仅当 $a_0 x^n + \cdots + a_{n-1} x + a_n$ 不可约.

证明

- 反设 $x^m - a = f(x)g(x)$ 可约.
- 令 $n = km$，$x^n - a = x^{km} - a = f(x^k)g(x^k)$
- $f(x)$ 和 $g(x)$ 非常值推出 $x^n - a$ 可约矛盾.

思维拓展 2

类似可证：对于 F 上的超越元 u，若 $F(u)/F$ 的中间域 $E \neq F$，则 $[F(u) : E]$ 是有限的.

第七章第 8 题第 1、2 问

设 L 和 M 是域扩张 K/F 的中间域，则 $[LM:F]$ 有限当且仅当 $[L:F]$ 和 $[M:F]$ 有限. 特别的，$[LM:F] \leq [L:F][M:F]$.

有限扩张总可以写作累次扩张和扩张次数的传递性.

思维拓展

设着举例说明 $[LM:F] \mid [L:F][M:F]$ 未必总是成立.

证明

- 设 $S \subset K$ 是有限多个 F 上的代数元集合，断言 $[M(S):M] \leq [F(S):F]$.
- 任给 $\alpha \in K$ 为代数元，利用 α 的 F 线性和 M 线性关系，有 $[M(\alpha):M] \leq [F(\alpha):F]$.
- 将 $M(S)$ 写作累次添加的形式，即可证明.
- 设 $L = F(S)$ 与 M 均是 F 有限扩张，则有 $[LM:F] = [LM:M][M:F]$ $= [M(S):M][M:F] \leq [L:F][M:F]$.

第七章第 8 题第 3 问

设 L 和 M 是 K/F 中间域，若 $[L:F]$ 和 $[M:F]$ 有限且互素，则 $[LM:F]=[L:F][M:F]$.

扩张次数的传递性和简单的数论

思维拓展

在 $[LM:F]$ 有限的情况下，能否由条件 $L\cap M=F$ 推出 $[LM:F]=[L:F][M:F]$? 试举例说明之.

证明

- 注意到 $[LM:F]=[LM:L][L:F]$.
- 这表明 $[L:F]\mid[LM:F]$，同理推出 $[M:F]\mid[LM:F]$.
- 互素推出 $[L:F][M:F]\mid[LM:F]$. 根据前面的结论立刻得到二者相等.

第七章第 8 题第 4 问

设 L 和 M 是域扩张 K/F 的中间域，若 L/F 和 M/F 均为代数扩张，则 LM/F 也是代数扩张.

$F(S)$ 中元素的刻画

思维拓展

代数元的加减乘除也是代数元，即 $\alpha \in K$ 是 F 代数元，任给 $f(x) \in F[x]$ 有 $f(\alpha)$ 是 F 代数元. 若 $\alpha \in K$ 使得 $f(\alpha)$ 是代数元，那么 α 是否一定是代数元？

证明

- 存在 $S \subset K$ 和 $T \subset K$ 为代数元使得 $L = F(S)$ 和 $M = F(T)$.
- $LM = F(S \cup T)$，任给 $\alpha \in LM$，总存在有限多个代数元 $a_1, \cdots, a_n \in S \cup T$ 使得 $\alpha \in F(a_1, \cdots, a_n)$ 是代数元.
- 注：若 L/F 和 M/F 均为代数扩张，则 $LM = \{\sum_{i=1}^{n} a_i b_i | n \in \mathbb{N}, a_i \in L, b_i \in M\}$.

代数闭包

代数闭包题 1

设 F 是一个域，$\overline{F}$ 是 F 的代数闭包，则 $\overline{F}$ 是一个无限域.

不可约多项式的判定

证明

- $\overline{F}$ 每一个元素均可在 F 上找到极小多项式
- 若 $\overline{F}$ 是有限域，则 F 上只有有限多个不可约多项式，全部记为 $f_1, \cdots, f_n$.
- 则 $F = f_1 \cdots f_n + 1$ 同样不可约，矛盾.

代数闭包题 2

设 $\overline{\mathbb{Q}}$ 是 $\mathbb{Q}$ 的代数闭包，则 $\overline{\mathbb{Q}}/\mathbb{Q}$ 是无限扩张.

不可约多项式的判定

证明

- 任给正整数 n，Eisenstein 判别法表明多项式 x^n-2 是 $\mathbb{Q}$ 上的不可约多项式.
- 设 α_n 为 x^n-2 的根，则 $\mathbb{Q}(\alpha)/\mathbb{Q}$ 是 n 次扩张.
- 因此 $[\overline{\mathbb{Q}}:\mathbb{Q}]\geq n$ 对一切正整数 n 成立，所以是无限扩张.

代数闭包题 3

设 $\overline{F}$ 是 F 的代数闭包，$L \subset \overline{F}$ 是 F 的代数扩张，证明 L 中的非常数多项式在 $\overline{F}$ 中均可完全分解为一次多项式乘积.

最小数原理和共轭元方法

证明

- 反设 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in L[x]$ 是 $L[x]$ 中使得 $[F(a_n, \cdots, a_0) : F]$ 最小的且在 $\overline{F}[x]$ 中不能完全分解的非常数多项式.
- 代数闭包条件表明 $F(a_n, \cdots, a_0) \neq F$，取 a_i 使得 $F(a_n, \cdots, a_{i+1}, a_{i-1}, \cdots, a_0) \subset F(a_n, \cdots, a_0)$.
- 令 $h(x) = a_n x^n + \cdots + a_{i+1} x^{i+1} + a_{i-1} x^{i-1} + a_1 x + a_0$，$g(x) \in F[x]$ 为 $-a_i = b_1$ 的极小多项式.
- 令 $g(x) = \prod_{s=1}^{m} (x - b_s)$，$F(x) = \prod_{s=1}^{m} (h(x) - b_s x^i) \in F(a_n, \cdots, a_{i+1}, a_{i-1}, \cdots, a_0)[x]$ 不能在 $\overline{F}[x]$ 中完全分解，要么矛盾，要么回到第一步，最终在有限步之内推出矛盾.

推论

设 $\overline{F}$ 是 F 的代数闭包，$L \subset \overline{F}$ 是 F 的代数扩张，则 $\overline{F}$ 也是 L 的代数闭包.

代数基本定理

复数域 $\mathbb{C}$ 是代数闭域.

代数闭域的不变性

若 E 是代数闭域，$E \cong E'$ 是域同构，则 E' 是代数封闭的.

$\mathbb{C}$ 中的代数闭子域

存在无穷多个 $\mathbb{Q} \subset E \subset \mathbb{C}$ 使得 E 是代数封闭的.

问题补充和方法扩张

问题 1

尺规作图作正 n 边形时，用域扩张的办法容易知道只有 $\varphi(n)$ 为 2 的方幂时有可能作出来. 那么我们如何证明如正 5 边形，正 17 边形一定可以尺规作图得到呢？

简要说明

- 正 n 边形作出的等价条件是作出 $\cos(\frac{2\pi}{n})$，等价于作出 $\zeta_n = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$
- 当只需要考虑 n 为素数的情形作出即可，也就是费马素数，根据分圆数进行逐步化解.
- 以 5 为例，令 $x = \zeta_5$，注意到 $1 + x + x^2 + x^3 + x^4 = 0$
- $(x + x^4)^2 = 2 + x^2 + x^3$，满足 $(x + x^4)^2 + (x + x^4) - 1 = 0$，因此 $x + x^4 = \frac{-1\pm\sqrt{5}}{2}$.
- $x + x^4 = \eta_0$，$x \cdot x^4 = 1$，因此 x 是方程 $t^2 - \eta_0 t + 1 = 0$ 的解，$x = \frac{\eta_0\pm\sqrt{\eta_0^2-4}}{2}$

问题 2

设 L/F 是域扩张，$\tau : L \to L$ 是保持 F 不动的域同态. L 满足什么条件可以使得 τ 总是一个同构? 什么条件可以使得 τ 总是一个恒等映射?

简要说明

- 有限扩张是显然的，代数扩张总是一个同构，超越扩张可以不是.
- 这就是正规扩张的概念的一个出发点.