第十次习题课

方法提要、习题讲解和内容扩充

助教：邓先涛

2023 年 11 月 20 日

重点知识提要

重点知识提要

- 分裂域：了解分裂域的结构和表达；了解分裂域的扩张次数.
- 域扩张的 Galois 群：掌握 Galois 群的定义与基本性质；能够计算简单域扩张的 Galois 群.
- 同构延拓定理：了解域同构在扩域上的延拓规律.

第七章习题讲解

第七章第 9 题

设 K/F 是一个代数扩张，则 K 的任一 F 自同态 σ 均是一个 F 自同构.

F 自同态保持代数扩张中代数关系

思维拓展

该题动机是考虑 $\sigma : K \to K$ 使得 $\sigma|_F = \mathrm{id}_F$，这样的域同态总是存在的. 如果任给 $\tau : F \to F$ 为域同构，K/F 为域扩张，是否总是存在域同态 $\sigma : K \to K$ 使得 $\sigma|_F = \tau$？K/F 是代数扩张呢？

证明

- σ 是单态，直接验证 $\sigma(a) \neq 0, \forall a \in K^*$.
- 任给 $\eta \in K$，$m(x)$ 为 η 的极小多项式.
- 任给 $i \in \mathbb{Z}_{>0}$，有 $m(\sigma^i(\eta)) = 0$ 且 $m(x)$ 只有有限多个根.
- 存在 $i > j$ 使得 $\sigma^i(\eta) = \sigma^j(\eta)$.
- 利用单性立刻得到 $\sigma^{i-j}(\eta) = \eta$，因此满.

第七章第 10 题

决定多项式 x^4-2 在有理数域上的分裂域.

分裂域的概念：添加多项式在代数闭包的所有根得到的域.

证明

- 直接在 $\overline{\mathbb{Q}}$ 对 x^4-2 进行分解，有
$$x^4-2=(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-\sqrt[4]{2}i)(x+\sqrt[4]{2}i)$$
- 分裂域为 $\mathbb{Q}[\sqrt[4]{2},i]$，其中 $i=\sqrt{-1}$.

思维拓展

分裂域的一个良好性质：设 d 是无平方因子整数，$\mathbb{Q}[\sqrt{d}]$ 是 $\mathbb{Q}$ 上 x^2-d 的分裂域，则任给 $\mathbb{Q}[x]$ 中的不可约多项式 $f(x)$，要么 $f(x)$ 在 $\mathbb{Q}[\sqrt{d}]$ 中可分解为一次多项式乘积，要么 $f(x)$ 在 $\mathbb{Q}[\sqrt{d}]$ 中没有根.

第七章第 11 题

决定 $f(x)=x^{p^e}-1(e\geq 1)$ 在特征 p 的素域 $\mathbb{F}_p$ 上的分裂域.

简单的组合

思维拓展

决定 $f(x)=x^{p^e}-x(e\geq 1)$ 在特征 p 的素域 $\mathbb{F}_p$ 上的分裂域 E_f，同时给出扩张次数 $[E_f:\mathbb{F}_p]$.

证明

- 任给素数 p 和正整数 e，有 $p\mid\binom{p^e}{i}$，其中 i 是小于 p^e 的正整数.
- $(x-1)^{p^e}=\sum_{i=0}^{p^e}\binom{p^e}{i}x^i=f(x)$.
- 故 $f(x)$ 只有单根 $x=1$，分裂域为 $\mathbb{F}_p$ 本身.

第七章第 13 题

设 E 为 $f(x) \in F[x]$ 在 F 上的分裂域，K 为 E/F 的中间域，则 E 也是 $f(x)$ 在 K 上的分裂域.

分裂域的定义

思维拓展

考虑上述问题的另一个方面. 设 E 为 $f(x) \in F[x]$ 在 F 上的分裂域，K 为 $g(x) \in E[x]$ 在 E 上的分裂域，那么 K 也是 F 上某个多项式的分裂域吗？

证明

- 设 $f(x)$ 的全部的根为 $\alpha_1, \cdots, \alpha_n$，则 $E = F(\alpha_1, \cdots, \alpha_n)$.
- 利用 $K \subset E$，得到 $E \subset K(\alpha_1, \cdots, \alpha_n) \subset E$.

第七章第 27 题

设域 F 的特征是 p，若 $a \in F$ 且 $a \notin F^p$，则任给正整数 e，均有 $x^{p^e} - a$ 在 F 上不可约.

简单的数论

思维拓展

能否给一个特征为 p 的域 F 使得存在 $a \in F$ 且 $a \notin F^p$？特别的，说明任给 $\mathbb{F}_p$ 的代数扩张 E，总有 $E = E^p$.

证明

- 设 $\alpha \in \overline{F}$ 使得 $\alpha^{p^e} - a = 0$.
- 有 $x^{p^e} - a = x^{p^e} - \alpha^{p^e} = (x-\alpha)^{p^e}$，设 α 在域 F 上的极小多项式为 $m(x)$.
- 若 $x^{p^e} - a$ 可约，则 $m(x) = (x-\alpha)^k \in F[x]$ 满足 $k < p^e$. 令 $d = \gcd(k, p^e) = uk + vp^e$.
- 推出 $(x-\alpha)^d \in F[x]$，因此 $d = k \mid p^e$.
- $\alpha^k \in F$ 推出 $a = \alpha^{p^e} = (\alpha^k)^{p^i} \in F^p$ 矛盾.

第八章习题讲解

第八章第 2 题

域 F 的非零自同态保持 F 内素域元素不动，记 P 为素域，则 $\mathrm{Aut}(F) = \mathrm{Gal}(F/P)$.

素域的概念

思维拓展

能否找到域扩张 K/F，使得 F 不是素域，且满足 $\mathrm{Aut}(K) = \mathrm{Gal}(K/F)$？在这其中有什么深刻的观察吗？

证明

- 素域的全体类型为 $\mathbb{Q}$ 和 $\mathbb{F}_p$，其中 p 跑遍全体素数.
- 什么叫素域？考察 $\psi : \mathbb{Z} \to F$，$\psi(\mathbb{Z})$ 在 F 中的分式域就是素域.
- 分别验证域同态总是保持素域不变.

第八章第 4 题

决定 $\mathrm{Gal}(K/\mathbb{Q})$，其中 $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$.

Galois 群的定义与概念

思维拓展

试决定 $\mathrm{Gal}(K/\mathbb{Q})$，其中 $K=\mathbb{Q}(\sqrt[3]{2},\sqrt{-1})$ 和 $K=\mathbb{Q}(\sqrt{\sqrt{5}+\sqrt{3}},\sqrt{\sqrt{5}-\sqrt{3}})$.

证明

- 验证 $K=\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.
- 验证 $\sqrt{2}+\sqrt{3}$ 的所有共轭元为 $\pm\sqrt{2}\pm\sqrt{3}$ 均在域 K 中.
- 验证 $\mathrm{Gal}(K/\mathbb{Q})$ 是克莱因四元数群.
- 不严谨做法：$\sqrt{2}\to\pm\sqrt{2}$ 和 $\sqrt{3}\to\pm\sqrt{3}$ 决定了 $\mathrm{Gal}(K/\mathbb{Q})$. 要如此构造必须先证明两个元素的无关性

补充课题：手算简单的域扩张 Galois 群细节

域扩张 Galois 群的一些事实

- 域扩张 Galois 群的定义：设 K/F 是域扩张，$\mathrm{Gal}(K/F)$ 定义为 K 到 K 的保持 F 不变的域同构所构成的群.
- 域扩张 Galois 群的一般刻画方法：若 K/F 是域扩张，$K = F(\alpha_1, \cdots, \alpha_n)$，则决定 $\mathrm{Gal}(K/F)$ 等价于兼容地决定 α_i 的像.
- 域扩张 Galois 群的基本事实：设 K/F 是有限扩张，则 $|\mathrm{Gal}(K/F)| \leq [K : F]$.

补充第 1 题

设 $K=\mathbb{Q}(\sqrt{2},\sqrt[3]{3})$，决定 $\mathrm{Gal}(K/\mathbb{Q})$.

证明

- 决定共轭元是否在集合中：$\sqrt{2}$ 的共轭元 $-\sqrt{2}\in K$；$\sqrt[3]{3}$ 的共轭元 $\sqrt[3]{3}\zeta_3,\sqrt[3]{3}\zeta_3^2\notin K$.
- 决定生成元的像：$\sqrt[3]{3}$ 只能映射到自身，$\sqrt{2}$ 可以映射到 $\pm\sqrt{2}$.
- 决定 $\mathrm{Gal}(K/\mathbb{Q})$：记 $\sigma:\sqrt{2}\to-\sqrt{2}$，则 $\mathrm{Gal}(K/\mathbb{Q})=\{1,\sigma\}$ 是二阶循环群.

补充第 2 题

设 $K=\mathbb{Q}(\sqrt{2},\zeta_8)$，其中 ζ_8 是 8 次本原单位根，决定 $\mathrm{Gal}(K/\mathbb{Q})$.

证明

- 决定共轭元是否在集合中：ζ_8 的在 $\mathbb{Q}$ 上的极小多项式为 x^4+1，共轭元 $\zeta_8^3,\zeta_8^5,\zeta_8^7\in K$；$\sqrt{2}$ 的共轭元 $-\sqrt{2}\in K$。
- 决定生成元的像：$\sqrt{2}$ 可以映射到 $\pm\sqrt{2}$，需要考虑 $\sqrt{2}$ 对 ζ_8 的影响.
- ζ_8 在 $\mathbb{Q}(\sqrt{2})$ 上的极小多项式：$x^4+1=(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)$，不妨设 ζ_8 在 $\mathbb{Q}[\sqrt{2}]$ 的极小多项式是 $x^2-\sqrt{2}x+1$.
- 若 $\sqrt{2}\to\sqrt{2}$，则 ζ_8 极小多项式没有改变，因此 ζ_8 映到自身或 $\mathbb{Q}(\sqrt{2})$ 上的共轭元 ζ_8^7；
- 若 $\sqrt{2}\to-\sqrt{2}$，则 ζ_8 极小多项式改变，因此 ζ_8 映到 $x^2+\sqrt{2}x+1$ 的根 ζ_8^3 和 ζ_8^5.
- 决定 $\mathrm{Gal}(K/\mathbb{Q})$：$\mathrm{Gal}(K/\mathbb{Q})$ 是克莱因四元数群.

补充第 3 题

设 K 为 $x^3 - x - 1$ 在 $\mathbb{Q}$ 上的分裂域，决定 $\mathrm{Gal}(K/\mathbb{Q})$.

证明

- 决定多项式的根的情况：容易验证该多项式有一对共轭的复根 α 和 $\overline{\alpha}$ 以及一个实根 β.
- 决定生成元的像：总是有一个合理的 $\mathrm{Gal}(K/\mathbb{Q})$ 中的元素，即共轭映射 $a + bi \to a - bi$.
- $\mathrm{Gal}(K/\mathbb{Q})$ 的基本结构：是 S_3 的可迁子群，这是因为任何两根之间都可以建立子域的同构，从而延拓为大域的同构.
- S_3 具有二阶元的可迁子群只有 S_3 自身，$\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.

补充第 4 题

设 $K=\mathbb{R}$，决定 $\mathrm{Gal}(K/\mathbb{Q})$.

证明

- 正数的像：任给 $0<a\in\mathbb{R}$，有 $\sigma(a)=(\sigma(\sqrt{a}))^2>0$.
- 同构保序：任给 $a>b$，有 $\sigma(a-b)>0$ 推出 $\sigma(a)>\sigma(b)$.
- 分类讨论：若 $\sigma(a)>a$，则存在有理数 b 使得 $\sigma(a)>b>a$，根据保序性 $\sigma(\sigma(a))>\sigma(b)>\sigma(a)$ 矛盾. 反过来同样可得，因此 $\sigma(a)=a$.
- $\mathrm{Gal}(\mathbb{R}/\mathbb{Q})=\{1\}$.

补充第 5 题

设 F 是一个域，u 为未定元，试决定 $\mathrm{Gal}(F(u)/F)$.

证明

- 设 $\sigma : u \to \frac{f(u)}{g(u)} = t$，其中 $f(x), g(x) \in F[x]$ 满足 $\gcd(f(x), g(x)) = 1$，记 $m = \max\{\deg(f), \deg(g)\}$.
- 注意到 u 在 $F(t)$ 上满足 $f(x) - tg(x) = 0$ 的代数元.
- 若 $f(x) - tg(x) = H(x,t)G(x,t)$ 可在 $F[t][x]$ 中分解，则分解出的因式之一系数均在 F 中，推出它会整除 $f(x)$ 和 $g(x)$，与 $\gcd(f(x), g(x)) = 1$ 矛盾.
- 同构表明 $F(u) = F(t)$，因此 $f(x) - tg(x)$ 是 $F[t]$ 中的一次多项式，即 $m = 1$.
- $\sigma(u) = \frac{au+b}{cu+d}$ 使得 $ac - bd \neq 0$ 确实是自同构，因此 $\phi : \mathrm{GL}_2(F) \to \mathrm{Gal}(F(u)/F)$ 是群同态.
- $\ker(\phi) = \{\mathrm{diag}(a,a) | a \in F^\times\}$，因此 $\mathrm{Gal}(F(u)/F) \cong \mathrm{PGL}_2(F)$.

问题补充和方法扩张

问题 1

域扩张与不可约多项式密切相关. 任给正整数 n，$\mathbb{Q}$ 上是否总是存在 n 次不可约多项式？$\mathbb{F}_p$ 上是否总是存在 n 次不可约多项式？进一步的，$\mathbb{F}_p$ 上的 n 次首一多项式个数有 p^n 个，那不可约多项式个数是多少呢？

简要说明

- 在 $\mathbb{Q}$ 上，$x^n - p$ 总是不可约的.
- 在 $\mathbb{F}_p$ 上，总是存在 n 次不可约多项式的个数，且个数是可算的.

问题 2

能否找到一些整系数不可约多项式 $f(x)$，使得 $f(x)$ 在任意 $\mathbb{F}_p$ 上都是可约的？是探究这其中的理论背景.

简要说明

- x^4+1 满足要求.
- 这样的多项式的数量以及在整个多项式或不可约多项式中的密度是多少是值得挖掘的内容.

问题 3

设 F 是域，K 是不可约多项式 $f(x) \in F[x]$ 在 F 上的分裂域，是否存在不同于 $f(x)$ 的不可约多项式 $g(x)$ 使得 K 也是 $g(x)$ 的分裂域？二者具有什么样的关系？

简要说明

- 在有限域上，次数相同的不可约多项式生成的分裂域是一样的.
- 在 $\mathbb{Q}$ 上如 $K = \mathbb{Q}(\sqrt{2})$，$f(x) = x^2 - 2$，其他能够生成 K 的不可约多项式总是形如 $g(x) = f(\frac{x-a}{b})$. 你能举一些例子使得 $f(x)$ 和 $g(x)$ 之间没有平移关系，且可以生成相同的分裂域.