第十一周作业参考解答及补充

作业

1. (习题 3.3.6)

设 L 是可分多项式 $f(x) \in K[x]$ 的一个分裂域, $K \subseteq E \subseteq L$ 是任意中间域. 证明: 对任意单同态 $\varphi : E \to L$, 若 $\varphi|_K = \mathrm{id}_K$, 则 φ 一定可以延拓成域同构 $\overline{\varphi} : L \to L$.

proof

按分裂域定义, 存在 $\alpha_1, \alpha_2, \cdots, \alpha_m \in L$ 使得 $f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)$, 且 $L = K[\alpha_1, \cdots, \alpha_m]$. 由于 $K \subseteq E \subseteq L$, $f(x) \in K[x] \subseteq E[x]$, 将 $f(x)$ 视为 $E[x]$ 中的多项式. $f(x)$ 仍有这样的分解. 且 $L = K[\alpha_1, \cdots, \alpha_m] \subseteq E[\alpha_1, \cdots, \alpha_m] \subseteq L$, 故 L 也是 $f(x)$ 在 E 上的分裂域. 由于 $\varphi|_K = \mathrm{id}_K$, 因此 $\varphi(f(x)) = f(x)$, 那么 L 也是 $f(x)$ 在 $\varphi(E)$ 上的分裂域. 由教材的定理 3.3.2, 由于 $f(x)$ 是可分多项式, 因此 $f(x)$ 在 $\varphi(E)$ 中无重根, 有 $|\{\text{域同构} L \xrightarrow{\psi} L \mid \psi|_E = \varphi\}| = [L : E] > 0$, 即该集合非空, 那么存在同构 $\psi : L \to L$ 使得 $\psi|_E = \varphi$. $\square$

注:

接 3.3.2 注记, 这种延拓对代数扩张是都成立的.

命题 已知对任意域 K 存在代数闭域 L 使得 $K \subseteq L$. 记 $i_K : K \to L$ 是域嵌入, 那么对任意代数扩张 $K \subseteq E$, 存在嵌入 $i : E \to L$ 使得 $i|_K = i_K$. 若 E 是代数闭域且 $L/i_K(K)$ 是代数的, 那么 i 是同构. 因此代数闭包在同构的意义下一定唯一. 证明需要 Zorn's Lemma. Serge Lang《Algebra》§V.2 Theorem 2.8.

另外也可以参考《近世代数引论》p136 引理 1, 这个是单代数扩张的版本, 相对简单一些, 如果只考虑有限扩张, 那么用这个版本就够了. 事实上这只是 3.1.2 的进一步解释, 在此基础上加了一个同构让他变成如下的交换图

$$
\begin{array}{ccccccc}
 & & E & & E' & & \\
 & & \cup\!\shortmid & & \cup\!\shortmid & & \\
K[x]/(\mu_\alpha(x)) & \xrightarrow{\sim} & K(\alpha) & \xrightarrow{\varphi} & K'(\alpha') & \xleftarrow{\sim} & K'[x]/(\mu_{\alpha'}(x)) \\
 & & \uparrow & & \uparrow & & \\
 & & K & \xrightarrow{\eta} & K' & &
\end{array}
$$

其中 η 是域同构, 那么根据教材引理 2.3.2, η 可以延拓成同构 $\tilde{\eta} : K[x] \xrightarrow{\sim} K'[x]$.

这个同态会把 α 的极小多项式映到 α' 的极小多项式. 这样就有

$$
\begin{tikzcd}
 & K[x] \arrow[r, "\tilde{\eta}"] \arrow[d, "\pi"] & K'[x] \arrow[d, "\pi'"] & \\
K(\alpha) \arrow[r, "\sim"] \arrow[rrr, bend right, "\varphi"'] & K[x]/(\mu_\alpha(x)) \arrow[r, "\bar{\tilde{\eta}}"] & K'[x]/(\mu_{\alpha'}(x)) \arrow[r, "\sim"] & K'(\alpha')
\end{tikzcd}
$$

注意到 $(\mu_\alpha(x)) \subseteq \ker(\pi' \circ \tilde{\eta})$, 由 quotient 的泛性质 (也就是同态基本定理的推广, 2.1.8 增加的命题) 得到 $\bar{\tilde{\eta}}$, 而这是域之间的满同态, 故只能是同构, 进而得到同构 φ, 且 $\varphi|_K = \eta$. 注意根据我们 φ 的构造一定是 $\varphi(\alpha) = \alpha'$, 若这里 $\eta = \mathrm{id}_K$, 那么 φ 就是把 α 换成 $\mu_\alpha(x)$ 的其中一个根.
这也说明我们在同构的意义下考虑域扩张是可行的. 但对代数闭包而言, 不一定是有限扩张, 比如 $\overline{\mathbb{Q}}/\mathbb{Q}$.
有了代数闭包, 可分多项式的等价定义为: $f(x) \in K[x]$ 是可分的, 即 $f(x)$ 的不可约因子在 $\overline{K}$ 中 (或者说在 $f(x)$ 的分裂域中) 无重根. 这也解释了 2.4.3 和 3.1.1 的关系, 特征零的不可约多项式可分, 从而特征零的代数扩张一定是可分扩张.

2. (习题 3.3.8)

设 $p \in \mathbb{Z}$ 是一个素数, F 是一个域, $c \in F$. 求证: $x^p - c$ 在 $F[x]$ 中不可约当且仅当 $x^p - c$ 在 F 中无根.

proof

考虑 $x^p - c$ 的分裂域 E, 或者直接考虑 F 的代数闭包, 那么有分解 $x^p - c = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_p)$. 我们证两次逆否.

" $\Longrightarrow$ " 若 $x^p - c$ 在 F 中有根, 根据教材定义 2.4.2, $x^p - c$ 有一次因式, 可约.

" $\Longleftarrow$ " 若 $x^p - c$ 可约, 按定义有 $x^p - c = f(x)g(x)$, 那么不妨设 $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, 其中 $0 < n < p$, 那么根据 Bézout's Identity, 存在 $u, v \in \mathbb{Z}$ 使得 $nu + pv = 1$. 记 $\alpha = \alpha_1\alpha_2\cdots\alpha_n \in F$(韦达定理), 注意到 α_i 都是 $x^p - c$ 的根, $\alpha_i^p = c$. 那么 $\alpha^p = \alpha_1^p\alpha_2^p\cdots\alpha_n^p = c^n$, 从而 $\alpha^{pu} = c^{nu}$, 那么 $(\alpha^u c^v)^p = c^{nu}c^{pv} = c$. 这样 $\alpha^u c^v$ 是 $x^p - c$ 的一个根, 且 $\alpha \in F$, 因此 $\alpha^u c^v \in F$.

□

3. (习题 3.3.11)

证明: $\mathbb{Q}[\sqrt[4]{2}]$ 是 $\mathbb{Q}[\sqrt{2}]$ 的正规扩张, 但不是 $\mathbb{Q}$ 的正规扩张.

proof

由 3.3.1, $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}[\sqrt{2}]$ 是二次扩张, 从而是正规扩张. 另一方面, 和 3.3.2 类似, $\sqrt[4]{2}$ 在 $\mathbb{Q}$ 上的的极小多项式 x^4-2 有非实数根 $\sqrt[4]{2}i$ 的存在, 自然不是正规扩张. $\square$

4. (习题 3.3.13)

设 $L=K[\alpha]$, α 是多项式 $x^d-a\in K[x]$ 的根. 如果 $\mathrm{Char}(K)=0$, 且 K 包含全部 d 次单位根, 则 $K\subseteq L$ 是正规扩张.

proof

这是 3.3.4 的一般情况. 设 $1=\omega_0,\omega_1,\cdots\omega_{d-1}$ 是 x^d-1 的根, 根据题设, $\omega_i\in L=K[\alpha], 0\leqslant i<d$. 而 $(\omega_i\alpha)^d=\omega^d\alpha^d=1\cdot a=a$, 从而 $\omega_i\alpha\in L$ 是 x^d-a 的 d 个根. 因此按定义 L 是 x^d-a 的分裂域. 由 3.3.14 的注记是 Galois 扩张, 自然是正规扩张. $\square$

5. (习题 3.3.14*)

设 k 是特征 $p>0$ 的域, x,y 是 k 上的代数无关元. 令 $K=k(x^p,y^p)$, $L=k(x,y)$. 试证明:

(1) $\mathrm{Gal}(L/K)=\{1\}$ (但 $[L:K]=p^2$);

(2) $K\subseteq L$ 有无穷多个中间域;

(3) $K\subseteq L$ 不是单扩张, 即不存在 $\alpha\in L$ 使得 $L=K[\alpha]$.

proof

这题是 3.1.15 的延续.

(1) 设 $\eta\in\mathrm{Gal}(L/K)$, 只需证 $\eta=\mathrm{id}_L$. 由 3.3.6, x 是 K 上的代数元, 且 x 的极小多项式是 t^p-x^p, 因此 $\eta(x)$ 是多项式 t^p-x^p 的根, 而根据 3.1.15, t^p-x^p 只有一个 p 重根 x, 因此 $\eta(x)=x$. 同理 $\eta(y)=y$, 从而 $\eta=\mathrm{id}_L$.

(2) 设 E 是一个非平凡中间域, 由于 $[L:K]=[L:E][E:K]=p^2$, 因此只能是 $[L:E]=[E:K]=p$. 而形如 $E_c=k(x+cy,y^p)$ 就是非平凡的中间域, 其中 $c\in K$ 而 K 是无穷域. 且 $c_1\neq c_2 \implies E_{c_1}\neq E_{c_2}$. 因此有无穷多个中间域.

(3) 由 Frobenius 同态可知, $\forall\alpha\in L$, $\alpha^p\in K$, 则 $t^p-\alpha^p\in K[t]$ 是 α 的化零多项式. 从而 $[K[\alpha]:K]\leqslant p<p^2$. 因此 $K[\alpha]\neq L$.

□

注:

这题教材答案的错误比较严重, K 并不是完全域, x^p 不是 K 中任何一个元素的 p 次方, 但 L/K 确实不是一个可分扩张, x 在 K 上的极小多项式 $t^p - x^p$ 在 K 上不是可分的. 事实上教材的定理 3.3.4 已经告诉我们完全域的代数扩张一定是可分扩张, 而 L/K 是有限扩张, 自然是代数扩张, 因此教材的答案是前后矛盾的.

事实上, 完全域应该定义为任意代数扩张都是可分扩张的域, 因此包括所有特征零的域. 在完全域上取分裂域得到的扩张一定是 Galois 扩张 (教材定理 3.4.1), 这也是为什么要有完全域这个概念.

课上的补充内容

Serge Lang 《Algebra》§V.3 Theorem3.3 给出了正规扩张的三个等价定义, 其中有一条是用到代数闭包的:

L/K 是正规扩张, 当且仅当延拓后的域嵌入 $\varphi : L \to \overline{K}$ 是 L 的自同构, 即 $\varphi(L) = L$.