第十周作业参考解答及补充

作业

1. (习题 3.3.1)

设 $f(x)=x^2+ax+b\in K[x]$ 不可约, $E=K[u_1]$(其中 $f(u_1)=0$) 证明: E 必包含 $f(x)=0$ 的另一个根 (所以 E 是 $f(x)$ 的分裂域).

proof

由于 $u_1\in E$ 是 $f(x)$ 的根, 因此在 $E[x]$ 中有分解 $f(x)=(x-u_1)f_1(x)$. 而 $\deg(f)=2$, 故只能是 $\deg(f_1)=1$, 即 $f_1=x-u_2$, $u_2\in E$ 自然是 $f(x)$ 的另一个根.
或设 $f(x)$ 的分裂域是 E', 令 f 的另一个根为 $u_2\in E'$, 则有 $u_1+u_2=a\in K\subseteq E$. 而 $u_1\in E$, 因此 $u_2\in E$, 即 $E'=E$. $\square$

注:

若要严谨一点, 则不能在 E 中直接使用韦达定理, 因为 $u_2\in E$ 是要证的结论. 韦达定理实际上是 f 在其分裂域可以分解成一次因式的乘积 (即分裂), 再对比系数得到的结论. 而按分裂域的定义可知它是使得 f 分裂的最小扩域. 那么直接使用韦达定理是在用结论证结论. 不过由于代数闭包总存在且唯一 (见 3.3.2 和 3.3.6), 我们总能把任意多项式分解成一次多项式的乘积, 所以直接使用事实上是没问题的.
这题也告诉我们, 二次扩张都是正规扩张.

2. (习题 3.3.2)

设 $f(x)=x^3-2\in\mathbb{Q}[x], u_1=\sqrt[3]{2}$. 证明: $E=\mathbb{Q}[u_1]$ 不包含 $f(x)=0$ 的其他两个根.

proof

教材例 3.3.4.
由于 $\mathbb{Q}\subseteq\mathbb{C}$, 而 $\mathbb{C}$ 是代数闭域, 我们可以把所有根都明确的写出来. x^3-2 的根为 $\alpha_k=\sqrt[3]{2}e^{\frac{2k\pi i}{3}}=\sqrt[3]{2}\zeta_3^k$, $k=0,1,2$, $u_1=\alpha_0$. 而 $\mathbb{Q}[u_1]\subseteq\mathbb{R}$, $\alpha_{1,2}\in\mathbb{C}\setminus\mathbb{R}$. $\square$

注:

借此补充代数扩张的一个结论, 任何域在同构的意义下都有唯一的代数闭包. 这个结果的证明分为两部分, 一是存在性, 二是 3.3.6 提到的延拓.

定义 若域 K 满足任意次数大于 1 的多项式 $f(x)\in K[x]$ 在 K 中都有根,

我们称 K 是一个代数闭域. 根据教材的定义 2.4.2, K 是代数闭域等价于 $K[x]$ 中的不可约多项式都是一次多项式. 即 $f(x)$ 总能分解成一次多项式的乘积.

由定义, K 是代数闭域意味着 K 无法再做非平凡的代数扩张了. 若有代数扩张 $K \subseteq L$ 且 $[L:K] > 1$, 则存在 $\alpha \in L \setminus K$ 在 K 上代数, 即存在非零多项式 $f(x) \in K[x]$ 使得 $f(\alpha) = 0$, 而 K 是代数闭域, $f(x)$ 的所有根都在 K 里, 这就矛盾了. 换句话说, 代数闭域做代数扩张只能得到它自己. 反过来也是对的, 若 K 没有非平凡代数扩张, 且有次数大于 1 的不可约多项式, 那根据 3.1.2 就能做真代数扩张, 矛盾.

定义 设域扩张 $K \subseteq L$, 考虑所有的代数元

$$E = \{\alpha \in L \mid \alpha \text{ 在} K \text{ 上代数}\}$$

由教材的推论 3.1.1 可知 E 是一个中间域, 且 $K \subseteq E$ 是代数扩张. E 称为 K 在 L 中的 (相对) 代数闭包.

比如对于扩张 $\mathbb{Q} \subseteq \mathbb{R}$, 这里的 E 就是所有的实代数数. 把 $\mathbb{R}$ 换成 $\mathbb{C}$, E 就是所有的复代数数, 也就是 $\mathbb{Q}$ 的代数闭包, 一般用 $\overline{\mathbb{Q}}$ 表示.

相对代数闭包 E 在 L 内没有非平凡代数扩张, 即若 $E \subseteq E' \subseteq L$ 且 $E \subseteq E'$ 是代数扩张, 则 $E = E'$. 证明这个结论需要一个很基本的定理.

定理 代数扩张的代数扩张仍是代数扩张, 即代数扩张是可以传递的. 《近世代数引论》p105, Serge Lang《Algebra》p228. 即对域扩张 $K \subseteq E \subseteq L$, L/K 是代数扩张 $\iff$ E/K 和 L/E 都是代数扩张.

那么 E'/E 代数, E/K 代数, 就有 E'/K 代数. 但根据 E 的定义是所有 K 上代数元构成的中间域, 因此 $E' \subseteq E$, 所以 $E' = E$.

定义 设 $K \subseteq L$ 是代数扩张, 若 L 是代数闭域, 称 L 是 K 的 (绝对) 代数闭包. 一般用记号 $\overline{K}$ 表示. (所以教材定理 3.3.2 的记号容易引起误解)

一般说代数闭包默认指绝对代数闭包.

命题 设 $K \subseteq L$ 是域扩张, L 是代数闭域, E 是 K 在 L 中的相对代数闭包, 则 $E = \overline{K}$.

只需证明这样得到的相对代数闭包是一个代数闭域, 注意到次数大于 1 的多项式 $f(x) \in E[x] \subseteq L[x]$, 而 L 是代数闭的, 因此 $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$, $\alpha_1, \cdots, \alpha_n \in L$ 在 E 上代数, 自然就在 K 上代数, 按 E 的定义就有 $\alpha_1, \cdots, \alpha_n \in E$. 从而 $f(x) \in E[x]$ 总能在 E 上分解称一次多项式的乘积.

命题 对任意域 K, 存在代数闭域 L 使得 $K \subseteq L$. Serge Lang《Algebra》§V.2 Theorem 2.5

若该命题成立, 那么根据上面的讨论, 任何域都存在代数闭包, 唯一性见 3.3.6.

这个命题的证明是构造性的, 构造方法属于 Artin, 需要用到 2.1.6 注记里补充的命题. 基本的思路就是构造一个域扩张 $K \subseteq K_1$ 使得 $K[x]$ 中所有非常数多项

式在 K_1 中都有至少一个根, 这个操作做可数次之后就能得到一个代数闭域. 类似 2.3.2 和 3.1.2 中说的那样, 令 $S=\{X_f \mid f\in K[x]\setminus K\}$, 即用 $K[x]$ 里的非常数多项式来编号, 得到一个无穷的未定元构成的集合, 然后考虑多项式环 $K[S]$. 此时记 $K[S]$ 的一个理想 $I=(f(X_f))_{f\in K[x]\setminus K}=\sum_{f\in K[x]\setminus K}(f(X_f))$, 即所有这种形式的 $K[S]$ 里的多项式生成的理想 (2.1.6 的注记), 如果商掉这个理想, 那么和 2.3.2 一样, $\overline{X_f}$ 就是 f 的一个根, 但 I 不一定是极大理想, 因此需要用到 2.1.6 注记里补充的命题 (新增加的), 即考虑 $I\subseteq\mathfrak{m}$, 其中 $\mathfrak{m}$ 是极大理想. 不过需要先验证 $I\neq(1)$, 这是容易的, 若 $I=(1)$, 意味着 $1=\sum_{i=1}^{n}a_if_i(X_{f_i})$, 而这是不可能的, 因为我们可以用 n 次 3.1.2 得到扩张 $K\subseteq E$ 让这里的 f_i 都有根, 赋值 (这里用的是多元的 2.4.5) 之后就得到 $1=0$, 矛盾. 因此这样我们得到了 $K_1=K[S]/\mathfrak{m}$. 然后做可数次 $K\subseteq K_1\subseteq\cdots\subseteq K_i\subseteq\cdots$. 最终得到的代数闭域就是 $L=\bigcup_{i=1}^{\infty}K_i$.

3. (习题 3.3.3)

设 L 是 n 次多项式 $f(x)\in K[x]$ 的分裂域, 证明: $[L:K]\leqslant n!$.

proof

对 n 归纳.

$n=1$ 或 f 已经在 K 上分裂, 都有 $[L:K]=1$. 假设结论对 n 成立, 现考虑 $\deg(f)=n+1$, 且 f 在 K 上不分裂, 那么存在 f 的不可与因子 g 满足 $\deg(g)>1$(否则 f 在 K 上分裂). 设 $u\in L$ 是 $g(x)$ 的一个根, 由 3.1.2, $K[u]\cong K[x]/(g(x))$ 是中间域, $[K[u]:K]=\deg(g)\leqslant\deg(f)=n+1$, 且在 $K[u][x]$ 上有分解 $f(x)=(x-u)h(x)$, $\deg(h)=n$. 由归纳假设, 此时 L 是 n 次多项式 $h(x)\in K[u][x]$ 的分裂域, 有 $[L:K[u]]\leqslant n!$, 从而 $[L:K]=[L:K[u]]\cdot[K[u]:K]\leqslant(n+1)!$. □

4. (习题 3.3.4)

构造 $x^5-2\in\mathbb{Q}[x]$ 的一个分裂域 L, 并求 $[L:\mathbb{Q}]$.

proof

仍使用 3.1.14 分析 degree 的方法, x^5-2 的根为 $\sqrt[5]{2}\zeta_5^k$, $k=0,1,2,3,4$. $L=\mathbb{Q}\left[\sqrt[5]{2}\zeta_5^i\right]=\mathbb{Q}\left[\sqrt[5]{2},\zeta_5\right]$. 借助中间域 $\mathbb{Q}[\sqrt[5]{2}]$. 一方面, $\left[\mathbb{Q}[\sqrt[5]{2}]:\mathbb{Q}\right]=5$(3.1.14); 另一方面, $[\mathbb{Q}[\zeta_5]:\mathbb{Q}]=4$(3.1.5). 因此 $5,4\mid[L:\mathbb{Q}]$, 由于 $(4,5)=1$, 因此 $4\cdot 5=20\mid[L:\mathbb{Q}]$, 另一方面 $x^5-2\in\mathbb{Q}[\zeta_5][x]$ 仍是 $\sqrt[5]{2}$ 的化零多项式, 又有 $[L:\mathbb{Q}]\leqslant 20$, 故 $[L:\mathbb{Q}]=20$. □

5. (习题 3.3.5)

确定多项式 $x^{p^n}-1\in\mathbb{F}_p[x]$ 在 $\mathbb{F}_p$ 上的分裂域 ($n\in\mathbb{N}$).

proof

特征 p 的域的多项式环上 Frobenius(2.1.2) 也是成立的, 故有 $x^{p^n}-1=x^{p^n}-1^{p^n}=(x-1)^{p^n}$. 从而 x^{p^n} 在 $\mathbb{F}_p$ 上分裂, 分裂域即 $\mathbb{F}_p$. $\square$

6. (习题 3.3.7)

令 $f(x)=(x^2-2)(x^2-3)$, $K=\mathbb{Q}[x]/(x^2-2)=\mathbb{Q}[u_1]$, 此处 $u_1=\overline{x}\in\mathbb{Q}[x]/(x^2-2)$. 试证明:

(1) K 是一个域, 且 x^2-3 在 $K[x]$ 中不可约;

(2) $L=K[x]/(x^2-3)=K[u_2]$(此处 $u_2=\overline{x}\in K[x]/(x^2-3)$) 是 $f(x)=(x^2-2)(x^2-3)$ 的分裂域, 且 $[L:\mathbb{Q}]=4$.

proof

(1) K 是域是因为 (x^2-2) 是极大理想, 见 3.1.2 和 3.1.14. x^2-3 在 K 中不可约在 3.1.4 已证.

(2) 根据 3.1.2 和 (1), $L=\mathbb{Q}[u_1,u_2]$ 是域. 且有分解 $f(x)=(x-u_1)(x+u_1)(x-u_2)(x+u_2)$, 因此 L 是 $f(x)$ 的分裂域 (3.3.1). 且有 $[L:\mathbb{Q}]=[L:K]\cdot[K:\mathbb{Q}]=2\cdot 2=4$.

$\square$