第八，九周作业参考解答及补充

作业

1. (习题 3.1.1)

设 K 是特征零的域, $f(x) \in K[x]$ 是次数大于零的首项系数为 1 的多项式, $d(x) = (f(x), f'(x))$ 是 $f(x)$ 与 $f'(x)$ 的最大公因子. 令

$$f(x) = d(x) \cdot g(x).$$

证明: $g(x)$ 与 $f(x)$ 有相同的根且 $g(x)$ 没有重根.

proof

我们总可以在 $f(x)$ 的分裂域上考虑因式分解. 由 2.4.3 可知, a 是 $f(x)$ 和 $f'(x)$ 的公共根当且仅当 a 是 $f(x)$ 的重根. 而 $f(x)$ 和 $f'(x)$ 的公共根当且仅当是 $d(x)$ 的根, 从而 $f(x)$ 的单根为 $g(x)$ 的根. 且若 a 是 $k(>1)$ 重根, 则按定义有 $f(x) = (x-a)^k f_1(x)$, $f_1(a) \neq 0$. 那么 $f'(x) = (x-a)^{k-1}(kf_1(x) + (x-a)f_1'(x))$, 记 $h(x) = kf_1(x) + (x-a)f_1'(x)$, 有 $h(a) = kf_1(a) \neq 0$. 即有 $(x-a)^{k-1} \mid d(x)$ 但 $(x-a)^k \nmid d(x)$, 因此 $g(x)$ 有单因子 $(x-a)$, 即重根 a 是 $g(x)$ 的单根. $\square$

2. (习题 3.1.2)

设 $K \subseteq L$ 是域扩张, $\alpha \in L$ 是域 K 上的代数元. 令 $K[x] \xrightarrow{\psi_\alpha} L$, $f(x) \mapsto f(\alpha)$, 表示多项式在 $x = \alpha$ 的取值映射. 试证明:

(1) $\ker(\psi_\alpha)$ 由极小多项式 $\mu_\alpha(x)$ 生成;

(2) ψ_α 诱导了域同构 $\mathbb{K}[x]/(\mu_\alpha(x)) \cong K[\alpha]$.

proof

(1) 回忆 2.2.6 和 2.3.2,

$$\ker(\psi_\alpha) = \{f \in K[x] \mid f(\alpha) = 0\}$$

是一个理想. 类似 2.2.6, 有 $(\mu_\alpha(x)) \subseteq \ker(\psi_\alpha)$ 且 $(\mu_\alpha(x))$ 是极大理想 (由 $K[x]$ 是 PID, 2.3.2), 且 $\ker(\psi_\alpha) \neq K[x]$, 因此只能是 $\ker(\psi_\alpha) = (\mu_\alpha(x))$.

(2) 由 2.3.2, $\overline{x}$ 为 μ_α 在扩域 $K[x]/(\mu_\alpha(x))$ 中的一个根. 那么映射

$$\varphi : K[x]/(\mu_\alpha(x)) \to K[\alpha], \quad \overline{x} \mapsto \alpha$$

是同构, 这是因为 $\psi_\alpha(K[x]) = K[\alpha] = K(\alpha)$(见注记), 那么由同态基本定理就得到同构.

□

注:

教材出现了有限生成扩张 (p7-8) 但并未单独列出这个的定义, 这里需要用一下所以先把这个定义提一下.

定义 设 $K \subseteq L$ 是一个域扩张, $S \subseteq L$ 是一个子集, $K(S)$ 称为由 F 和 S 生成的子域, 即包含 F 和 S 的最小域:

$$K(S) := \cap\{E \subseteq L \mid F \cup S \subseteq E\}$$

若 $T \subseteq L$ 是另一个子集, 则定义 $K(S)(T) := K(S \cup T)$.
若存在有限子集 S 使得 $L = K(S)$, 即存在有限个 $u_1, u_2, \cdots, u_n \in L$ 使得 $L = K(u_1, u_2, \cdots, u_n)$, 则称该扩张是有限生成的 (finitely generated).

$$K(u_1, u_2, \cdots, u_n) := \cap\{E \subseteq L \mid K \subseteq E,\ u_1, u_2, \cdots, u_n \in E\}$$

$n = 1$ 时称为单扩张 (simple extension).
下面要验证的事实是, 当 $u_1, u_2, \cdots, u_n$ 都是 K 上代数元的时候,
$K(u_1, u_2, \cdots, u_n) = K[u_1, u_2, \cdots, u_n]$, 且此时该扩张是有限扩张, 否则是无限扩张. 即对域扩张而言:

$$\text{algebraic} + \text{finitely generated} = \text{finite}$$

反过来是非常简单的, 有限扩张 $\implies$ 代数扩张, 利用 $1, \alpha, \cdots, \alpha^n$ 线性相关即可, $n = \dim_K L$. 有限扩张 $\implies$ 有限生成, 取一组基就行.
对任意的单扩张 $K \subseteq K(\alpha)$, 很自然的想法就是用 2.3.7 的赋值映射来讨论. 对包含 $K \overset{i}{\hookrightarrow} K(\alpha)$ 用泛性质, 存在唯一的同态

$$\psi_\alpha : K[x] \to K(\alpha), \quad f(x) \mapsto f(\alpha).$$

由同态基本定理, $K[x]/\ker(\psi_\alpha) \cong \psi_\alpha(K[x]) = K[\alpha] \subseteq K(\alpha)$. 由于 $K(\alpha)$ 按定义是域, 因此是整环. 而 $K[\alpha]$ 是子环, 从而也是整环, 因此 $\ker(\psi_\alpha)$ 是素理想. 而 $K[x]$ 是一个 PID, 因此只有两种情况.

Case 1 $\ker(\psi_\alpha) = \{0\}$, 此时 ψ_α 是单射. 这意味着 $\{f(x) \in K[x] \mid f(\alpha) = 0\} = \{0\}$, 即零多项式是唯一使得 $f(\alpha) = 0$ 的多项式, 换言之 α 是 K 上的超越元. 注意 $K(x)$ 是 $K[x]$ 的分式域, 由分式域 (或者说 localization) 的泛性质 (单独放在后面), 存在唯一的同态使得图表交换:

$$\begin{tikzcd}
K(x) \arrow[rr, "\varphi_\alpha"] & & K(\alpha) \\
& K[x] \arrow[ul, hook] \arrow[ur, "\psi_\alpha"'] &
\end{tikzcd}$$

即

$$\varphi_\alpha : K(x) \to K(\alpha), \quad \frac{p(x)}{q(x)} \mapsto \frac{p(\alpha)}{q(\alpha)}$$

这是一个单射 (因为 $K(x)$ 是域). 考虑 φ_α 的像, 它一定是一个域, 且包含 K 和 α, 因此按定义就有 $K(\alpha) \cong \varphi_\alpha(K(x)) \cong K(x)$, 那么 $K \subseteq K(\alpha)$ 扩张次数为无穷 $(1, \alpha, \alpha^2, \cdots$ 线性无关). 如 $\mathbb{Q}(\pi) \cong \mathbb{Q}(x)$.

Case 2 $\ker(\psi_\alpha) = (p(x))$, $p(x)$ 是一个不可约多项式. 注意到 $\alpha = \psi_\alpha(x)$, 此时 $K[\alpha] = \psi_\alpha(K[x]) \cong K[x]/(p(x))$ 是包含 α 的域, 而根据 ψ_α 的构造, $K[\alpha] \subseteq K(\alpha)$, 由 $K(\alpha)$ 的定义, 只能是 $K[\alpha] = K(\alpha) \cong K[x]/(p(x))$. 此时是有限扩张, 扩张次数为 $\deg(p(x))$, 且 $p(x)$ 和 α 的极小多项式 $\mu_\alpha(x)$ 是相伴的 ($(p(x)) = (\mu_\alpha(x))$, 即就差一个常数, $p(x)$ 除掉首项系数就是 $\mu_\alpha(x)$). 在这个域同构下 $\overline{x} \in K[x]/(p(x))$ 的像就是 α, 这就是为什么 2.3.2 在最后提到, $\overline{x}$ 是多项式 $p(x)$ 在扩域 $K[x]/(p(x))$ 上的根.

多元的情形由归纳法即可,

$$\begin{aligned} K(u_1, u_2, \cdots, u_n) &= K(u_1, u_2, \cdots, u_{n-1})(u_n) = K[u_1, u_2, \cdots, u_{n-1}](u_n) \\ &= K[u_1, u_2, \cdots, u_{n-1}][u_n] = K[u_1, u_2, \cdots, u_n] \end{aligned}$$

, 且

$$\begin{aligned} &[K[u_1, u_2, \cdots, u_n] : K] \\ &\quad = [K[u_1, u_2, \cdots, u_n] : K[u_1, u_2, \cdots, u_{n-1}]] \cdot [K[u_1, u_2, \cdots, u_{n-1}] : K] < \infty. \end{aligned}$$

值得注意的是多元的时候, 这里只是说明可以由 $u_1, u_2, \cdots, u_n$ 通过多项式生成, 但仍有可能由更少的代数元生成, 如 1.1.3, $\mathbb{Q}$ 加上 $\sqrt{2}$ 和 $\sqrt{3}$ 后仍是一个单扩张. 又比如 $\mathbb{Q}[\sqrt{2}, \sqrt[4]{2}] = \mathbb{Q}[\sqrt[4]{2}]$.
上面提到的 localization 可以理解成分式域的推广. 设 A 是交换环, $S \subseteq A$ 是一个乘法封闭子集 (multiplicatively closed subset), 即 $\forall s, t \in S \implies st \in S$ 并要求 $1 \in S$. 换句话说, S 是 $(A, \cdot)$ 的一个子幺半群. 则 $A \times S$ 上有一个等价关系:

$$(a, s) \sim (a', s') \iff \exists u \in S, (as' - a's)u = 0$$

记商集 $A \times S/\sim$ 为 $S^{-1}A$, 可以验证这是一个环, A 是它的子环, 称为 A 对 S 的分式环. 它是包含 A 的并使得 S 中元素都可逆的“最小”的环. 这个构造通常称为环的局部化 (localization). 当 A 是整环且取 $S = A \setminus \{0\}$ 时就是分式域, 如 $\mathbb{Q}$, $K(x)$. 若 $0 \in S$ 则得到零环, 因此一般尽量排除这种平凡的情况. 当 $\mathfrak{p} \subseteq A$ 是素理想时, 按素理想的定义可以验证 $S = A \setminus \mathfrak{p}$ 是乘法封闭的 (事实上反过来也是对的). 此时 $S^{-1}A$ 一般记作 $A_\mathfrak{p}$, 这是一个局部环 (2.3.1), 如 $\mathbb{Z}_p$(p-adic integers).

上述的“最小”对应它的泛性质:
$S^{-1}A$ 的元素记为 $\frac{a}{s}$, 我们有一个自然的同态

$$f_S : A \to S^{-1}A, \quad a \mapsto \frac{a}{1}$$

$f(s) = \frac{s}{1}$ 在 $S^{-1}A$ 中都是可逆的, 逆是 $\frac{1}{s}$. 若环同态 $\varphi : A \to B$ 满足对任意的 $s \in S$, $\varphi(s)$ 在 B 中可逆, 那么存在唯一的环同态 $\varphi_S : S^{-1}A \to B$ 使得图表交换:

$$\begin{tikzcd} S^{-1}A \arrow[rr, "\varphi_S"] & & B \\ & A \arrow[ul, "f_S"] \arrow[ur, "\varphi"'] & \end{tikzcd}$$

$\varphi_S(\frac{a}{s}) = \varphi(a)\varphi(s)^{-1}$. 注意一般情况下 f_S 不一定是单的, 事实上是非整环的情形有零因子导致的, 因此 A 是整环的时候且不考虑 $0 \in S$, 等价关系 $\sim$ 简化为和分式域的情况一样, 即

$$(a, s) \sim (a', s') \iff as' = a's$$

3. (习题 3.1.3)

设 $E = \mathbb{Q}[u], u^3 - u^2 + u + 2 = 0$. 试将 $(u^2 + u + 1)(u^2 - u)$ 和 $(u - 1)^{-1}$ 表示成 $au^2 + bu + c(a, b, c \in \mathbb{Q})$ 的形式.

proof

利用 $u^3 = u^2 - u - 2$ 消去次数大于 2 的项.

$(u^2+u+1)(u^2-u) = (u^3-1)u = (u^2-u-3)u = u^2-u-2-u^2-3u = -4u-2.$

第二个可以用形式级数处理

$$\begin{aligned} (u-1)^{-1} = \frac{1}{u-1} &= -(1 + u + u^2 + u^3(1 + u + u^2 + \cdots)) \\ &= -(1 + u + u^2 + \frac{u^2 - u - 2}{1 - u}) \\ &= -(1 + u^2 - \frac{2}{1 - u}) \end{aligned}$$

因此 $\frac{1}{u-1} = -\frac{1}{3}(1 + u^2)$. □

4. (习题 3.1.4)

求 $\left[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}\right]$(提示: 证明 $\left[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\sqrt{3}]\right] = 2$).

proof

参考 1.4.8, $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$, 即不存在 $\mathbb{Q}[\sqrt{2}]$ 上的一次多项式使得 $\sqrt{3}$ 是根, 因此 x^2-3 是 $\mathbb{Q}[\sqrt{2}]$ 上的不可约多项式. 更详细的说, 若 x^2-3 在 $\mathbb{Q}[\sqrt{2}]$ 上可约, 则按定义 $x^2-3=(x-\alpha_1)(x-\alpha_2)$, 其中 $\alpha_i = a_i + b_i\sqrt{2}$, $a_i, b_i \in \mathbb{Q}$. 右边展开对比系数一样得到矛盾.
$\sqrt{3}$ 是 x^2-3 的根, 因此它是 $\sqrt{3}$ 对于 $\mathbb{Q}[\sqrt{2}]$ 的极小多项式. 从而有

$$\left[\mathbb{Q}[\sqrt{2},\sqrt{3}] : \mathbb{Q}[\sqrt{2}]\right] = \left[\mathbb{Q}[\sqrt{2}][\sqrt{3}] : \mathbb{Q}[\sqrt{2}]\right] = \deg(x^2-3) = 2.$$

故

$$\left[\mathbb{Q}[\sqrt{2},\sqrt{3}] : \mathbb{Q}\right] = \left[\mathbb{Q}[\sqrt{2},\sqrt{3}] : \mathbb{Q}[\sqrt{2}]\right] \cdot \left[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}\right] = 4$$

□

5. (习题 3.1.5)

设 p 是一个素数, $z \in \mathbb{C}$ 满足 $z^p = 1$ 且 $z \neq 1$, 试证明 $[\mathbb{Q}[z] : \mathbb{Q}] = p-1$.

proof

注意到 $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$. 由于 $z \neq 1$, 因此 z 是多项式 $\Phi_p(x) = x^{p-1} + \cdots + x + 1$ 的根, 这是一个不可约多项式 (教材例 2.3.4), 从而是 z 的极小多项式. 因此 $[\mathbb{Q}[z] : \mathbb{Q}] = \deg(\Phi_p) = p-1$. □

注:

这是分圆多项式中 n 为素数的情况.

6. (习题 3.1.6)

证明:

(1) $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ 是一个循环群;

(2) $z = \cos\frac{\pi}{6} + i\sin\frac{\pi}{6}$ 是 U_{12} 的一个生成元, 但 $[\mathbb{Q}[z] : \mathbb{Q}] = 4$;

(3) 求 $z = \cos\frac{\pi}{6} + i\sin\frac{\pi}{6}$ 在 $\mathbb{Q}$ 上的极小多项式.

proof

(1) $\zeta_n = e^{\frac{2\pi i}{n}}$ 是 U_n 的生成元.

(2) $z=\cos\frac{\pi}{6}+i\sin\frac{\pi}{6}=e^{\frac{2\pi i}{12}}=\zeta_{12}$, 即 (1) 中提到的生成元. 而

$$\begin{aligned}
x^{12}-1&=(x^4-1)(x^8+x^4+1)\\
&=(x^2-1)(x^2+1)(x^4+x^2+1)(x^4-x^2+1)\\
&=(x-1)(x+1)(x^2+1)(x^2-x+1)(x^2+x+1)(x^4-x^2+1)
\end{aligned}$$

是不可约分解, 其中 x^4-x^2+1 是 $\Phi_{12}(x)$, 它的根是 12 次本原单位根 $\zeta_{12},\zeta_{12}^5,\zeta_{12}^7,\zeta_{12}^{11}$, $x-1$ 为 $\Phi_1(x)$, 根是 $1=\zeta_{12}^0$; $x+1$ 为 $\Phi_2(x)$, 根是 $-1=\zeta_{12}^6$; x^2+1 为 $\Phi_4(x)$, 根是 $i=\zeta_{12}^3,-i=\zeta_{12}^9$; x^2+x+1 为 $\Phi_3(x)$, 根是 $\zeta_{12}^4,\zeta_{12}^8$; x^2-x+1 为 $\Phi_6(x)$, 根是 $\zeta_{12}^2,\zeta_{12}^{10}$. 故 x^4-x^2+1 是 ζ_{12} 的极小多项式, $[\mathbb{Q}[z]:\mathbb{Q}]=\deg(\Phi_{12}(x))=4$.

(3) 见 (2).

□

注:

1. 教材循环群的定义为由一个元素生成的 (自由) 群 $\langle a\rangle=\{a^n\mid n\in\mathbb{Z}\}$, 等价的说就是和 $\mathbb{Z}/n\mathbb{Z}$ 同构的群 ($n=0$ 时为 $\mathbb{Z}$ 本身). 对于 $\mathbb{Z}/n\mathbb{Z}$ 有一个和初等数论有关的结论就是 Euler 函数 $\phi(n)=|(\mathbb{Z}/n\mathbb{Z})^{\times}|$, 其中 $(\mathbb{Z}/n\mathbb{Z})^{\times}$ 是单位群 $U(\mathbb{Z}/n\mathbb{Z})=\{\overline{m}\in\mathbb{Z}/n\mathbb{Z}\mid(m,n)=1\}$. 即 $\phi(n)$ 是 0 到 $n-1$ 中和 n 互素的元素个数. Fermat 小定理的推广便是

$$(a,n)=1\implies a^{\phi(n)}\equiv 1\pmod{n}$$

且有恒等式

$$n=\sum_{\substack{d\mid n\\ d>0}}\phi(d)$$

2. 易见 $U_n\cong\mathbb{Z}/n\mathbb{Z}$, U_n 中的 1 对应 $\mathbb{Z}/n\mathbb{Z}$ 中的 0, ζ_n 对应 1, 若 $(k,n)=1$, k 就是生成元, 对应 U_n 中的 $\zeta_n^k=e^{\frac{2k\pi i}{n}}$. U_n 的生成元称为 n 次本原单位根. 分圆多项式 $\Phi_n(x)$ 是 ζ_n 的极小多项式, 事实上

$$\Phi_n(x)=\prod_{0\leqslant k<n,(n,k)=1}(x-\zeta_n^k)$$

且有恒等式

$$x^n-1=\prod_{\substack{d\mid n\\ d>0}}\Phi_d(x)$$

因此可以递归的计算出 $\Phi_n(x)$,

$$\Phi_n(x)=\frac{x^n-1}{\prod\limits_{\substack{d|n\\0<d<n}}\Phi_d(x)}$$

7. (习题 3.1.7)

设 $E=K[u]$ 是一个代数扩张, 且 u 的极小多项式的次数是奇数. 证明: $E=K[u^2]$.

proof

由于 $K[u^2]\subseteq K[u]$, 即 $K[u^2]$ 是中间域, 设 $\mu_u(x)\in K[x]$ 是 u 的极小多项式, 则

$$\deg(\mu_u(x))=[K[u]:K]=\left[K[u]:K[u^2]\right]\cdot\left[K[u^2]:K\right]$$

是奇数. 而 u 是多项式 $x^2-u^2\in K[u^2][x]$ 的根, 因此 $\left[K[u]:K[u^2]\right]\leqslant 2$. 但由于奇数不可能有因子 2, 故 $\left[K[u]:K[u^2]\right]=1$, 即 $K[u^2]=K[u]$. $\square$

8. (习题 3.1.8)

设 E_1,E_2 是域扩张 $K\subseteq L$ 的中间域 (即: $K\subseteq E_i\subseteq L$), 且 $[E_i:K]<+\infty$. 令 $E=K(E_1,E_2)\subseteq L$ 是由 E_1,E_2 生成的子域. 证明:

$$[E:K]\leqslant[E_1:K]\cdot[E_2:K].$$

注:

按正确的记号应该是用圆括号表示生成, 见 3.1.2 的注记.

proof

设 $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ 是 E_1 的一组 K-基, $\{\beta_1,\beta_2,\cdots,\beta_m\}$ 是 E_2 的一组 K-基, 并要求 $\alpha_1=\beta_1=1$(总是可以乘上一个 α_1^{-1} 或 β_1^{-1}, 而这一组元素仍是基). 只需说明 $S=\{\alpha_i\beta_j\}$ 可以生成 $E=K(E_1,E_2)=K(E_1\cup E_2)$. 按定义, 若 $e_1\in E_1,e_2\in E_2$, $e_1=\sum\limits_{i=1}^{n}k_i\alpha_i$, $e_2=\sum\limits_{j=1}^{m}l_j\beta_j$. 由于取 $\alpha_1=\beta_1=1$, 因此 $\alpha_i,\beta_j\in S$, 那么 $e_1\pm e_2,e_1e_2,e_i^{-1}$(若不为零) 都可以由 S 生成. $\square$

9. (习题 3.1.9)

设 $K\subseteq L$ 是代数扩张, $E\subseteq L$ 是中间子环 (即: $K\subseteq E\subseteq L$). 证明: $E\subseteq L$ 必为子域 (所以任何有限扩张 $K\subseteq L$ 的中间子环必为域).

proof

按定义说明 E 中非零元可逆即可. 设 $0 \neq u \in E \subseteq L$, 则 u 在 L 上代数, 那么 $K(u) = K[u] \subseteq E$ 是域 (包含关系由泛性质得到, 2.3.7), 则 $u \in K[u]$ 可逆. □

10. (习题 3.1.10)

设 $L = K(u)$, u 是 K 上的超越元, $E \neq K$ 是 $K \subseteq L$ 的中间域. 证明: u 是 E 上的代数元.

proof

任取 $v \in E \setminus K$, 那么按定义 $v = \dfrac{p(u)}{q(u)}$, 则 $p(u) - vq(u) = 0$, 即 u 是多项式 $p(x) - vq(x) \in E[x]$ 的根. □

11. (习题 3.1.11)

设 p 是素数, $K \subseteq L$ 是 p 次扩张. 证明: $K \subseteq L$ 必为单扩张(即: 存在 $u \in L$, 使 $L = K[u]$).

注:

单扩张见 3.1.2 的注记, 由于 3.3.14 又写成单扩张了, 干脆把这里的“单纯”也改成“单”.

proof

任取 $u \in L \setminus K$, 和 3.1.7 的讨论类似,

$$p = [L : K] = [L : K[u]] \cdot [K[u] : K]$$

由 p 是素数, 且 $[K[u] : K] \neq 1$(因为 $u \notin K$), 可知 $[L : K[u]] = 1$, $[k[u] : K] = p$, 即 $L = K[u]$. □

12. (习题 3.1.12)

设域扩张 $K \subseteq L$ 满足条件:

(1) $[L : K] < +\infty$;

(2) 对任意两个中间域 $K \subseteq E_1 \subseteq L$, $K \subseteq E_2 \subseteq L$, 必有 $E_1 \subseteq E_2$ 或者 $E_2 \subseteq E_1$.

证明: $K \subseteq L$ 必为单扩张(即: 存在 $u \in L$, 使 $L = K[u]$).

proof

由 3.1.2 的注记, 有限扩张是有限生成代数扩张, 故存在代数元 $u_1, u_2, \cdots, u_n$, $L = K[u_1, \cdots, u_n]$, 那么 $K[u_i]$ 都是中间域, 若 $K[u_i] \subseteq K[u_j]$, 则 $K[u_i, u_j] = K[u_j][u_i] = K[u_j]$. 那么存在某个 $u \in \{u_1, \cdots, u_n\}$ 使得 $K[u] = \bigcup_{i=1}^{n} K[u_i] = K[u_1, \cdots, u_n] = L$. □

13. (习题 3.1.14)

设 $K = \mathbb{Q}[\sqrt[3]{3}]$, 证明: $x^5 - 5$ 在 $K[x]$ 中不可约.

proof

只需说明 $x^5 - 5$ 是 $\sqrt[5]{5}$ 在 K 上的极小多项式. 我们证明 $\left[\mathbb{Q}[\sqrt[3]{3}, \sqrt[5]{5}] : \mathbb{Q}[\sqrt[3]{3}]\right] = 5$ 即可.
由 Eisenstein 判别法容易说明 $x^3 - 3$ 和 $x^5 - 5$ 在 $\mathbb{Q}$ 上不可约, 从而有 $\left[\mathbb{Q}[\sqrt[3]{3}] : \mathbb{Q}\right] = 3$, $\left[\mathbb{Q}[\sqrt[5]{5}] : \mathbb{Q}\right] = 5$. 由于

$$\left[\mathbb{Q}[\sqrt[3]{3}, \sqrt[5]{5}] : \mathbb{Q}\right] = \left[\mathbb{Q}[\sqrt[3]{3}, \sqrt[5]{5}] : \mathbb{Q}[\sqrt[3]{3}]\right] \cdot \left[\mathbb{Q}[\sqrt[3]{3}] : \mathbb{Q}\right]$$

那么只需说明 $\left[\mathbb{Q}[\sqrt[3]{3}, \sqrt[5]{5}] : \mathbb{Q}\right] = 15$. 记 $\alpha = \sqrt[3]{3}$, $\beta = \sqrt[5]{5}$. 则 $\mathbb{Q}[\alpha]$ 的基为 $\{1, \alpha, \alpha^2\}$, $\mathbb{Q}[\beta]$ 的基为 $\{1, \beta, \beta^2, \beta^3, \beta^4\}$. 由 3.1.8, 说明 $\{\alpha^i \beta^j \mid 0 \leqslant i \leqslant 2, 0 \leqslant j \leqslant 4\}$ 是 $\mathbb{Q}$-线性无关的即可, 这是比较容易看出来的 (虽然很明显但是没想到优雅的证明先挖个坑). □

注:

3.1.4 是直接证不可约得到扩张次数, 这里是用扩张次数来得到不可约.

14. (习题 3.1.15)

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 $[L : K] = p^2$.

注:

代数无关是多元的超越, $a_1, a_2, \cdots, a_n$ 代数无关指不存在满足它们的代数方程, 即不存在多项式 $f(x_1, x_2, \cdots, x_n) \in k[x_1, x_2, \cdots, x_n]$ 使得 $f(a_1, a_2, \cdots, a_n) = 0$.

proof

x, y 代数无关, 按定义 x, y 就是超越元, 根据 3.1.2 的注记, K 和 L 视为有理函数域处理即可. 考虑中间域 $k(x, y^p)$, 由 Eisenstein 判别法, x^p 是 $k[x^p, y^p]$ 的不可约元, 则 $t^p - x^p \in k[x^p, y^p][t]$ 是不可约多项式, 而 K 是 $k[x^p, y^p]$ 的分式

域, 从而在 $K[t]$ 内也不可约 (教材推论 2.3.1). 那么 $t^p - x^p$ 是 $x \in k(x, y^p)$ 在 K 上的极小多项式. $[k(x, y^p) : K] = \deg(t^p - x^p) = p$. 同理 $[L : k(x, y^p)] = p$. 因此 $[L : K] = [L : k(x, y^p)] \cdot [k(x, y^p) : K] = p^2$. □

注:

证明过程没有用到特征 p, 因此该结论对任意域都是是对的.

课上的补充内容

基本上都在 3.1.2 里.