

1, 设 Q 是有理数域, x^3-a 是 $Q[x]$ 中的不可约元, α 是 x^3-a 的一个根, 试证明 $Q(\alpha)$ 不是 x^3-a 在 Q 上的分裂域,

证明: 因为 α 是 x^3-a 的一个根, 所以 x^3-a 的另外两个根为 $\alpha\omega, \alpha\omega^2$

若 $Q(\alpha)$ 是 x^3-a 在 Q 上的分裂域, 则 $\alpha\omega, \alpha\omega^2$ 属于 $Q(\alpha)$,

从而有 ω 属于 $Q(\alpha)$, 于是 $Q(\alpha)$ 包含 $Q(\omega)$,

因此 $|Q(\alpha) : Q| = |Q(\alpha) : Q(\omega)| |Q(\omega) : Q|$

因为 $|Q(\alpha) : Q| = 3, |Q(\omega) : Q| = 2$, 所以矛盾, 故 $Q(\alpha)$ 不是 x^3-a 在 Q 上的分裂域

2, 设 α 是属于 $Q[x]$ 的 $f(x) = x^2 + x + 1$ 的根

求 $f(x)$ 在 Q 上的分裂域及 $f(x)$ 在分裂域中的因子分解,

解: 因为 $f(x)$ 是二次多项式, 因此若 α 是 $f(x)$ 的根,

$-1-\alpha$ 是 $f(x)$ 的另一个根, 且 $f(x) = (x-\alpha)(x+1+\alpha)$,

$f(x)$ 在 Q 上的分裂域为 $Q(\alpha)$,

3, 求多项式 $f(x) = x^3 - x^2 - x - 2$ 在有理数域上的分裂域,

解: 因为 $f(x) = x^3 - x^2 - x - 2 = (x^2 + x + 1)(x - 2) = (x - \omega)(x - \bar{\omega})(x - 2)$,

所以 $f(x)$ 在有理数域上的分裂域为 $Q(\omega, \bar{\omega}, 2) = Q(\omega)$,

4, 设 p 是素数, 求 $x^{p^n} - 1$ 在 Z_p 上的分裂域,

解: 因为 $f(x) = x^{p^n} - 1 = (x - 1)^{p^n}$, 故 $f(x) = x^{p^n} - 1$ 在 Z_p 上的分裂域为 Z_p

5, 试证明包含 Q 的扩张 $Q(\sqrt[4]{9})$ 是正规扩张,

证明: 由于 $\sqrt[4]{9} = \sqrt{3}$ 在 Q 上的极小多项式是 $x^2 - 3$,

而 $x^2 - 3$ 在 Q 上的分裂域为 $Q(\sqrt[4]{9})$,

所以包含 Q 的 $Q(\sqrt[4]{9})$ 是正规扩张

6, 试证明扩张次数为 2 的扩张是正规扩张,

证明: 设 $|E:F|=2$, 取属于 $E-F$ 的 α ,

则由 $|E:F|=|E:F(\alpha)||F(\alpha):F|$, 知 $|F(\alpha):F|=2$, $|E:F(\alpha)|=1$, $E=F(\alpha)$,

设 α 在 F 上的极小多项式为 x^2+ax+b , 则 x^2+ax+b 的根为 $\alpha, \beta=-a-\alpha$,

x^2+ax+b 在 F 上的分裂域为 $F(\alpha, \beta)=F(\alpha)$,

所以包含 F 的 E 是正规扩张,

7, 试证明 $Q(\sqrt[3]{5})$ 不是 Q 的正规扩张,

证明: $Q[x]$ 中不可约元 $f(x)=x^3-5$ 的根为 $\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5}$, 其中 $\omega=\frac{1-\sqrt{3}i}{2}$

显然 $\omega\sqrt[3]{5}, \omega^2\sqrt[3]{5}$ 不属于 $Q(\sqrt[3]{5})$, 故 $Q(\sqrt[3]{5})$ 不是 Q 上的正规扩张,

8, 求属于 $Z_2[x]$ 的多项式 $f(x)=x^2+x+1$ 在 Z_2 上的分裂域,

解: 因为 $f(x)=(x-1)(x^2+x+1)$, 且 x^2+x+1 是 Z_2 上的不可约多项式,

所以 $f(x)$ 在 Z_2 上的分裂域为 $Z_2(\alpha)$, 其中 α 是 x^2+x+1 的一个根,

习题 1 设 F 为域, E 是 $F[x]$ 中 n 次多项式 $f(x)$ 在 F 上的分裂域, 求证 $|E:F|=n!$

证明: 对 n 用数学归纳法, 显然, $n=1$ 时结论成立,

假设结论对 $n-1$ 次多项式成立,

设 $f(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, 其中 a 属于 $F, \alpha_1, \alpha_2, \dots, \alpha_n$ 属于 E

令 $f_{n-1}(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{n-1})$, 则 $f_{n-1}(x)$ 是 $F(\alpha_n)$ 上多项式

且在 $F(\alpha_n)$ 上的分裂域为 $F(\alpha_n)(\alpha_1, \alpha_2, \dots, \alpha_{n-1})=E$

由归纳假设知 $|E:F(\alpha_n)|=(n-1)!$

由 α_n 是 $F[x]$ 中 n 次多项式 $f(x)$ 的根可知 $|F(\alpha_n):F|=n!$

因此, $|E:F|=|E:F(\alpha_n)||F(\alpha_n):F|=n!$

习题 2 求 $f(x)=x^3-2$ 在有理数域上的分裂域 E , 并求 $|E:Q|$,

解: 因为 $f(x)=(x-\sqrt[3]{2})(x-\sqrt[3]{2}\omega)(x-\sqrt[3]{2}\bar{\omega})$

所以 $f(x)$ 在有理数域上的分裂域为 $Q(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\bar{\omega})=Q(\sqrt[3]{2}, \sqrt{3}i)$,

扩张次数为 $|Q(\sqrt[3]{2}, \sqrt{3}i):Q|=|Q(\sqrt[3]{2}, \sqrt{3}i):Q(\sqrt[3]{2})||Q(\sqrt[3]{2}):Q|=6$,

习题 3 求 $f(x)=x^4-10x^2+1$ 在有理数域上的分裂域 E , 并求 $|E:Q|$,

解: 因为 $f(x)=(x^4-2x^2+1)-8x^2=(x^2-2\sqrt{2}x-1)(x^2+2\sqrt{2}x-1)$

$= (x-\sqrt{2}-3)(x-\sqrt{2}+3)(x+\sqrt{2}-3)(x+\sqrt{2}+3)$,

所以 $f(x)$ 在 Q 上的分裂域为 $Q(\sqrt{2}\pm\sqrt{3})=Q(\sqrt{2}, \sqrt{3})=Q(\sqrt{2}+\sqrt{3})$, $|E:Q|=4$,

习题 4 求 $f(x)=x^5+x^3-2x^2-2$ 在有理数域上的分裂域 E , 并求 $|E:Q|$,

解: 因为 $f(x)=(x-i)(x+i)(x-\sqrt[3]{2})(x-\sqrt[3]{2}\omega)(x-\sqrt[3]{2}\bar{\omega})$

所以 $f(x)$ 在有理数域上的分裂域为 $Q(i, \sqrt{3}, \sqrt[3]{2})$, $|E:Q|=12$,

习题 5 将 Z_2 上多项式 $f(x)=x^3+x+1$ 表示成分裂域上一次因式的乘积的形式,

解: 易知 $f(x)$ 是 $Z_2[x]$ 中不可约多项式, $f(x)$ 在 $Z_2[x]/\langle f(x) \rangle$ 中有根 \bar{x}

而 $Z_2(\bar{x}) \cong Z_2[x]/\langle f(x) \rangle$, $Z_2(\bar{x}) = \{a\bar{x}^2 + b\bar{x} + c \mid a, b, c \in Z_2\}$,

容易验证 \bar{x}^2 , $\bar{x}^2 + \bar{x}$ 是 $f(x)$ 的根, 所以分裂域为 $Z_2(\bar{x})$, $f(x) = (x-\bar{x})(x-\bar{x}^2)(x-\bar{x}^2-\bar{x})$

习题 6 设 $f(x)=x^{p^n}-x$ 在 Z_p 上的分裂域为 E , 证明 $|E|=p^n$, 并求 $|E:Z_p|$,

证明: 设 F 是 $f(x)$ 在 E 中所有根的集合, 则对属于 F 的任意 a, b ,

我们有 $(a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b$, $(ab^{-1})^{p^n} = a^{p^n} (b^{p^n})^{-1} = ab^{-1}$

即 $a-b, ab^{-1}$ 属于 F , 因而 F 是 E 的子域,

又因为 $f(x)$ 无重根 ($f'(x)=-1$), 所以 F 的阶为 p^n

若 c 属于 Z_p , 则 $c=c^p$, 从而 $c=c^{p^n}$, 即 c 属于 F

从而 $E=Z_p(F) \subseteq F \subseteq E$, 即 $E=F$, 易知, $|E:Z_p|=n$

习题 7 求 $f(x)=x^6+\bar{2}x^3+\bar{2}$ 在 Z_3 上的分裂域 E , 并求 $|E:Z_3|$,

解: 因为 $f(x)=x^6+\bar{2}x^3+\bar{2}=(x^2+\bar{2}x+\bar{2})^3$, 而 $x^2+\bar{2}x+\bar{2}$ 在 Z_3 上不可约,

所以 $f(x)$ 在 Z_3 上的分裂域为 $Z_3(\alpha)$, 其中 α 是 $x^2+\bar{2}x+\bar{2}$ 的一个根,

易知 $|Z_3(\alpha):Z_3|=2$,

习题 8 设 F 是域, E 是属于 $F[x]$ 的多项式 $f(x)$ 在 F 上的分裂域,

K 是包含 F 的 E 的中间域, 试证明 E 是 $f(x)$ 在 K 上的分裂域,

证明: 设 $f(x)$ 在 E 中的根为 $\alpha_1, \dots, \alpha_n$ 则 $E=F(\alpha_1, \dots, \alpha_n)$,

从而 $f(x)$ 在 K 上的分裂域为 $K(\alpha_1, \dots, \alpha_n)$, 而 $E \supseteq K(\alpha_1, \dots, \alpha_n) \supseteq F(\alpha_1, \dots, \alpha_n) = E$

所以 E 是 $f(x)$ 在 K 上的分裂域,

习题 9 证明 $Q(\sqrt[4]{2})$ 不是 Q 的正规扩张,

证明: $Q[x]$ 中不可约元 $f(x)=x^4-2$ 的根为 $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$

由于 $Q(\sqrt[4]{2})$ 包含于 R , 但是 $i\sqrt[4]{2}$ 不属于 R , 故 $Q(\sqrt[4]{2})$ 不是 Q 的正规扩张,