

题目 1. 设 R 是域 F 的子环, 且对任意 $a \in F$, 都存在首一多项式 $f \in R[x]$, 使得 $f(a) = 0$. 证明 R 是域.

证明. 设 $a \in R$, $a \neq 0$. 则 $\frac{1}{a} \in F$, 知存在首一多项式 $f(x) \in R[x]$, 使得 $f\left(\frac{1}{a}\right) = 0$. 设 $f(x) = x^n + g(x)$, 其中 $\deg g \leq n$. 则 $\frac{1}{a} = a^{n-1}g\left(\frac{1}{a}\right) \in R$. 由 a 任意性, R 是域. \square

题目 2. 设 p 是素数, $n \geq 2$ 为正整数, $R = \mathbb{Z}/p^n$. 证明:

1. R 的元素要么可逆, 要么幂零.
2. R 只有一个素理想 P , 并求这个素理想.
3. R/P 是有限域.

证明. (1) 设 $a \in \mathbb{Z}$. 若 $a \in p\mathbb{Z}$, 则 $a^n \equiv 0 \pmod{p^n}$. 若 $a \notin p\mathbb{Z}$, 则 $(a, p^n) = (1)$, 进而 $aR = R$. 于是 a 在 R 中的像要么幂零, 要么可逆.

(2) 由素理想对应, R 的素理想一一对应于 \mathbb{Z} 的包含 (p^n) 的素理想, 从而仅有 $P = (p)$.

(3) $R/P \cong \mathbb{Z}/p = \mathbb{F}_p$ 为有限域. □

题目 3. 证明 $R = \mathbb{Z}[\sqrt{3}]$ 为欧几里得整环.

证明. 在 $K = \mathbb{Q}(\sqrt{3})$ 上令范数 $N(a + b\sqrt{3}) = a^2 - 3b^2$ ($a, b \in \mathbb{Q}$), 令欧几里得赋值 $\delta(x) = |N(x)|$. 不难验证 N 保持乘积, 进而 δ 保持乘积.

任取 $x = a + b\sqrt{3} \in K$. 设 a', b' 分别为离 a, b 最近的整数, $x' = a' + b'\sqrt{3} \in R$. 则 $|a - a'|, |b - b'| \leq \frac{1}{2}$. 从而 $\delta(x - x') = \left| (a - a')^2 - 3(b - b')^2 \right| \leq \frac{3}{4}$. 这说明, 对任何 $x \in K$, 存在 $x' \in R$ 使得 $\delta(x - x') \leq \frac{3}{4}$.

现在任取 $x, y \in R$, $y \neq 0$. 则存在 $p \in R$ 使得 $\delta\left(\frac{x}{y} - p\right) \leq \frac{3}{4}$. 从而 $\delta(x - yp) < \delta(y)$. 由 x, y 任意性, 知 δ 确为欧几里得赋值, 从而 R 为欧几里得整环. \square

注 3.1. 注意到, $\delta(a + b\sqrt{3}) = a^2 + 3b^2$ 不是欧几里得赋值. 事实上, $\delta(2) = \delta(1 + \sqrt{3}) = 4$, 但不存在 $p \in R$ 使得 $\delta(1 + \sqrt{3} - 2p) < 4$.

题目 4. 下面论断是否成立？试证明或给出反例。

1. Q 的 2 次扩张都同构。
2. R 的 2 次扩张都同构。
3. 有限域的 2 次扩张都同构。

证明。 (1) 不成立。

注意到, $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ 均为 2 次扩张。又不难验证, $x^2 - 3$ 在 $\mathbb{Q}(\sqrt{2})$ 中没有零点, 从而这两个扩域不同构。

(2) 成立。

证法 1: 注意到 \mathbb{C} 是 \mathbb{R} 的一个代数闭包, 从而由延拓定理, \mathbb{R} 的代数扩张都到 \mathbb{C} 有 \mathbb{R} 同态。比较次数知 \mathbb{R} 的 2 次扩张到 \mathbb{C} 的同态都为同构, 从而 \mathbb{R} 的 2 次扩张都同构于 \mathbb{C} 。

证法 2: 注意到 \mathbb{R} 的 2 次扩张都是 2 次根式扩张, 从而形如 $\mathbb{R}(\alpha)$, 其中 $\alpha^2 = a \in \mathbb{R}$ 不是平方。于是 $a < 0$, 进而 $\alpha \mapsto \sqrt{a}$ 给出了 \mathbb{R} 同态 $\mathbb{R}(\alpha) \rightarrow \mathbb{C}$, 且比较次数知这是同构。从而 \mathbb{R} 的 2 次扩张都同构于 \mathbb{C} 。

(3) 成立。

设 F 是有限域, 下证 F 的 2 次扩张都同构。设 $|F| = q$ 。

注意: 需要证明这些域作为 F 的扩张同构, 即它们 F -同构。

证法 1: F 的 2 次扩张为 q^2 阶有限域, 从而为 $x^{q^2} - x$ 在 F 上的分裂域。知它们均同构。

证法 2: 由 ppt 结论知 q^2 阶有限域均同构。设 K_1, K_2 为 F 的两个 2 次扩张。 $\varphi : K_1 \rightarrow K_2$ 为同构。则由 F 为 \mathbb{F}_p 的 Galois 扩张, 知 $\varphi|_F$ 为 F 的自同构。由 K_1 也是 \mathbb{F}_p 的 Galois 扩张, 知 $\varphi|_F$ 延拓为自同构 $\psi : K_1 \rightarrow K_1$ 。进而 $\varphi \circ \psi^{-1} : K_1 \rightarrow K_2$ 为 F 同构。

证法 3: 若 $\text{char } F \neq 2$, 则 F 的二次扩张 K 形如 $F(\alpha)$, 其中 $\alpha^2 \in F - F^2$ 。但 F^\times 为循环群, 从而任两个非平方元相差一个平方元。这说明若还有二次扩张 $L = F(\beta)$, $\beta^2 \in F - F^2$, 则 $F(\alpha) \cong F(\beta)$ 。故 F 的 2 次扩张都同构。

若 $\text{char } F = 2$, 令 $\kappa(a) = a^2 - a$ 。则 κ 在任何特征 2 的域上为加法群的自同态, 且满足 $\ker \kappa = \{0, 1\}$ 。于是对有限域 F , $\kappa(F)$ 为 F 加法群的指数为 2 子群。

则 F 的二次扩张 K 形如 $F(\alpha)$, 其中 $\kappa(\alpha) \in F - \kappa(F)$ 。若还有 $L = F(\beta)$, $\kappa(\beta) \in F - \kappa(F)$, 则 $\kappa(\alpha)$ 与 $\kappa(\beta)$ 相差 $\kappa(F)$ 的一个元素, 从而

$F(\alpha) \cong F(\beta)$. 故 F 的 2 次扩张都同构.

□

题目 5. 设 F 为域, E/F 为 n 次多项式 $f \in F[x]$ 的分裂域. 证明 $[E : F] \mid n!$.

证明. 这是作业题.

对 n 归纳. 不妨设 $n > 1$.

若 $f = f_1 f_2$ 可约, 令 K 为 f_1 在 F 上分裂域, E 为 f_2 在 K 上分裂域, 则 E 是 f 在 F 上的分裂域. 设 $\deg f_i = n_i$. 从而 $[E : F] \mid [K : F][E : K] \mid n_1!n_2! \mid n!$.

若 f 不可约, 取 $\alpha \in E$ 为 f 的根. 则令 $g(x) = \frac{f(x)}{x - \alpha} \in F(\alpha)[x]$, 则 E 也为 g 在 $F(\alpha)$ 上的分裂域. 由归纳假设 $[E : F(\alpha)] \mid (n - 1)!$. 又 $[F(\alpha) : F] = n$, 从而 $[E : F] \mid n!$. \square

注 5.1. 很容易注意到, $\text{Gal}_f \leq S_n$, 从而 $|\text{Gal}(E/F)| \mid n!$. 但这不能说明 $[E : F] \mid n!$, 因为 f 可能不可分.

此外, 有少量同学不加思考地背诵并默写了存在跳步的作业参考答案. 在可约的情形中, 确实有 $E = E_1 E_2$, 其中 E_i 为 f_i 在 F 上的分裂域. 但是 $[E : F] \mid [E_1 : F][E_2 : F]$ 是需要证明的. 这需要用到 E_i 是 F 的正规扩张.

题目 6. 设 \mathbb{F}_2 为 2 阶有限域, $\mathbb{F}_2(t)$ 为有理函数域. 证明 $\mathbb{F}_2(t)/\mathbb{F}_2(t^2)$ 为正规不可分扩张.

证明. 注意到 $t \in K = \mathbb{F}_2(t)$ 在 $F = \mathbb{F}_2(t^2)$ 上的最小多项式为 $f(x) = x^2 - t^2$. 它是不可分多项式, 从而 K/F 不可分. 而 K 又为 f 在 F 上的分裂域, 从而正规. \square

题目 7. 设 $f(x) = x^4 - 16x^2 + 4 \in \mathbb{Q}[x]$. 设 E 是 f 在 \mathbb{Q} 上的分裂域.

1. 计算 $[E : \mathbb{Q}]$.

2. 求 f 的 Galois 群 Gal_f .

3. 求 E/\mathbb{Q} 的所有中间域 L , 及对应的子群 $\text{Gal}(E/L)$, 并判断它们是否是正规的.

证明. 证法 1: 注意到 $\pm\sqrt{3} \pm \sqrt{5}$ 为 f 的零点, 从而 $E = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

(1) 由作业题, $[E : \mathbb{Q}] = 4$.

(2) 注意到 $(x, y) \in \mathbb{Z}/2 \times \mathbb{Z}/2$ 作用在 E 上,

$$\sigma_{x,y}(\sqrt{3}) = (-1)^x \sqrt{3},$$

$$\sigma_{x,y}(\sqrt{5}) = (-1)^y \sqrt{5}.$$

则 σ 定义了同态 $\mathbb{Z}/2 \times \mathbb{Z}/2 \rightarrow \text{Gal}(E/\mathbb{Q})$, 不难验证这是单射, 进而是同构.

令

$$\alpha_1 = \sqrt{3} + \sqrt{5}, \alpha_2 = \sqrt{3} - \sqrt{5}, \alpha_3 = -\sqrt{3} + \sqrt{5}, \alpha_4 = -\sqrt{3} - \sqrt{5}.$$

则 $\sigma_{1,0}$ 作用为 (13)(24), $\sigma_{0,1}$ 作用为 (12)(34). 于是

$$\text{Gal}_f = \{e, (12)(34), (13)(24), (14)(23)\}.$$

(3) E/\mathbb{Q} 的全体中间域及对应的 Galois 群为

$$\{e\} \leftrightarrow E = \mathbb{Q}(\sqrt{3}, \sqrt{5}),$$

$$\langle \sigma_{1,0} \rangle \leftrightarrow \mathbb{Q}(\sqrt{5}),$$

$$\langle \sigma_{0,1} \rangle \leftrightarrow \mathbb{Q}(\sqrt{3}),$$

$$\langle \sigma_{1,1} \rangle \leftrightarrow \mathbb{Q}(\sqrt{15}),$$

$$\text{Gal}(E/\mathbb{Q}) \leftrightarrow \mathbb{Q}.$$

由于 $\text{Gal}(E/\mathbb{Q})$ 交换, 它的子群都是正规子群, 从而 E/\mathbb{Q} 的中间域都是 \mathbb{Q} 的正规扩张.

证法 2: 不难验证 f 没有零点. 进而设 $f(x) = (x^2 + ax + b)(x^2 - ax + c)$, 则 $a = 0$ 或 $b = c$, 均易验证无解. 从而 f 不可约.

设 $\pm\alpha, \pm\beta$ 为 f 的所有零点. 则 $\alpha^2\beta^2 = 4$. 从而不妨设 $\alpha\beta = 2$. 这说明 $E = \mathbb{Q}(\pm\alpha, \pm\beta) = \mathbb{Q}(\alpha)$.

(1) 由 $E = \mathbb{Q}(\alpha)$, 知 $[E : \mathbb{Q}] = 4$.

(2) $\text{Gal}(E/\mathbb{Q})$ 的元素被 α 的像唯一决定, 且这个像的取值范围为 f 的全体零点, 即 $\pm\alpha, \pm\beta$. 令

$$\alpha_1 = \alpha, \alpha_2 = -\alpha, \alpha_3 = \beta = \frac{2}{\alpha}, \alpha_4 = -\beta.$$

则 4 个 Galois 变换为

$$e, (12)(34), (13)(24), (14)(23).$$

它们构成的群即为 Gal_f .

(3) E/\mathbb{Q} 的全体中间域及对应的 Galois 群为

$$\begin{aligned} \{e\} &\leftrightarrow E = \mathbb{Q}(\alpha), \\ \langle(12)(34)\rangle &\leftrightarrow \mathbb{Q}(\alpha^2), \\ \langle(13)(24)\rangle &\leftrightarrow \mathbb{Q}(\alpha + \beta), \\ \langle(14)(23)\rangle &\leftrightarrow \mathbb{Q}(\alpha - \beta), \\ \text{Gal}(E/\mathbb{Q}) &\leftrightarrow \mathbb{Q}. \end{aligned}$$

由于 $\text{Gal}(E/\mathbb{Q})$ 交换, 它的子群都是正规子群, 从而 E/\mathbb{Q} 的中间域都是 \mathbb{Q} 的正规扩张.

当然, 若已经取定 $\alpha\beta = 2$, 可得 $(\alpha + \beta)^2 = 20$, $(\alpha - \beta)^2 = 12$. 又有 $(\alpha^2 - 8)^2 = 60$. 于是这三个中间域分别为 $\mathbb{Q}(\sqrt{15}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{3})$. \square

题目 8. 判断 $f(x) = x^5 - 15x^2 + 9$ 是否在 \mathbb{Q} 上根式可解.

证明. 不可解.

注意到 $f(x+1)$ 为关于 5 的爱森斯坦多项式, 从而不可约. 而 $f'(x)$ 恰有 2 实根, 且 f 在这两个实根间变号. 从而 f 恰有 3 个实根.

由 ppt 结论, 知 $\text{Gal}_f = S_5$ 不可解.

(结论的证明: 注意到, Gal_f 传递, 进而有 5 轮换. 而 f 恰有 2 虚根, 这说明复共轭给出了 Gal_f 中的对换. 现在 $\text{Gal}_f \leq S_5$ 含有一个对换和一个 5 轮换, 只能为整个 S_5 .) \square