Homework 7

冯熙喆

2025 年 12 月 20 日

A $X^6 - 3X^2 - 1$ 的 Galois 群

A1)

考虑到 $P(0) = 0, P(\sqrt{3}) = -1, P(-\sqrt{3}) = -1, P(-1) =, P(2) = 1, P(-2) = -3$ 就得到了根的分布].

如果 α 是一个根, 下面验证 $P(2 - \alpha^2) = 0$:

$\alpha^4 = 3\alpha^2 + \alpha$，$\alpha^6 = 9\alpha^2 + 6\alpha + 1$

$P(2 - \alpha^2) = (2 - \alpha^2)^3 - 3(2 - \alpha^2) - 1 = (8 - 12\alpha^2 + 6\alpha^4 - \alpha^6) - (6 - 3\alpha^2) - 1 = 0$。

因此 $2 - \alpha^2$ 也是 $P(X)$ 的根。

A2)

因为 α_2, α_3 都可以被 α_1 和 $\mathbb{Q}$ 中元素用加减乘除得到 (由 A1), 就可以知道分裂域确实是 $\mathbb{Q}(\alpha_1)$

据此, 这是一个可分扩张, 且由 mod2 判别法可知 $P(X)$ 是不可约多项式, 因此 Galois 群的阶数就等于多项式的 deg, 也就是 3. 据 3 阶群的唯一性我们就知道它就是 3 阶循环群.

A3)

$X^6-3X^2-1\in Ann(\beta_1)$, 因此 $[K(\beta_1):Q]|6$, 又因为 $\mathbb{Q}(\alpha_1)\subseteq K(\beta_1)$, 可知 $3|[K(\beta_1):Q]$, 因此 $[K(\beta_1):K]$ 等于 1 或者 2

下证明 $[K(\beta_1):K]$ 等于 2, 为此, 我们证明 $\beta_1\notin K$:

反设 $\beta_1\in K$, 那么就有 $\alpha_1=\beta_1^2$, 取 $\sigma\neq id\in Gal(K/\mathbb{Q})$ 那么 $\sigma(\alpha_1)=(\sigma(\beta_1))^2$, 然而 $\sigma(\alpha_1)<0$, 这说明 $\sigma(\beta_1)\notin\mathbb{R}$, 这与 K 是实数的子域矛盾.

因此,$[K(\beta_1):K]=2$

A4)

由前所述, 我们知道 $[\mathbb{Q}(\beta_1):\mathbb{Q}]=6$, 且 β_2 在 $\mathbb{Q}(\beta_1)[X]$ 中有 2 次零化多项式, 据此, 我们知道 $[\mathbb{Q}(\beta_1,\beta_2):\mathbb{Q}]=6$或12, 下证明 $\mathbb{Q}(\beta_1,\beta_2)\neq\mathbb{Q}(\beta_1)$:

由于 $\alpha_2<0$ 可知 $\beta_2\in\mathbb{C}-\mathbb{R}$, 从而一定有 $\mathbb{Q}(\beta_1,\beta_2)\neq\mathbb{Q}(\beta_1)$

进一步, 我们知道 $\beta_3\in\mathbb{Q}(\beta_1,\beta_2)$, 也就是说 $L/\mathbb{Q}$ 是一个正规扩张, 计算判别式可知它还是可分扩张, 从而 $[L:\mathbb{Q}]=|Gal(L/\mathbb{Q})|=12$

A5)

$Gal(L/\mathbb{Q})$ 的 Sylow 2-子群是 4 阶的, 并且 Sylow 2-子群的个数可能为 1 或 3

由于 $\mathbb{Q}(\alpha_1)/\mathbb{Q}$ 是一个 3 次正规扩张,Galois 对应定理指出 $Gal(L/\mathbb{Q})$ 存在指数为 3 的 (4 阶的) 正规子群, 从而 Sylow 2-子群的个数只能为 1.

进一步, 记这个群为 $H=Gal(L/K)$, 任取 $\sigma\in H,\beta_i(i=1,2,3)$, 总有 $\sigma(\beta_i^2)=\sigma(\alpha_i)=\alpha_i\Leftrightarrow\sigma(\beta_i)=\pm\beta_i$

据此 H 中元素全为至多 2 阶元素, 也就是说,$H\simeq K_4$

A6)

据定义, 这 12 个映射是两两不等的, 而且他们确实是 L 的 Q-自同构, 结合 $Gal(L/\mathbb{Q})$ 的阶数就得到了证明

A7)

由 Sylow 定理可知,G 的 Sylow 3-子群可能有 1 个或 4 个.

考虑如下由映射的像给出的自同构 $\varphi:(\beta_1,\beta_2,\beta_3)\mapsto(\beta_2,\beta_3,\beta_1)$ 以及自同构 $\psi:(\beta_1,\beta_2,\beta_3)\mapsto(\beta_3,\beta_2,\beta_1)$

我们知道 $\langle\varphi\rangle,\langle\psi\rangle$ 都是 Sylow 3-子群, 并且他们不相等, 从而 Sylow 3 子群至少有 2 个, 那么它的个数是 4.

进一步, 我们知道 G 中有 1 个单位元素, 一个 2 阶元素,7 个互不相等的 3 阶元素,2 个 4 阶元素, 这些元素构成了 G, 从而 $G\simeq\mathfrak{A}_4$

A8)

根据 A7 的分析, 我们知道 G 所有真子群分别是 3 个阶为 2 的子群,4 个阶为 3 的子群,1 个阶为 4 的子群.

阶为 2 的子群对应的就是 6 次扩张 $\mathbb{Q}(\beta_i)/(Q),(i=1,2,3)$

我们知道 $\theta_i,(i=1,2,3,4)$ 分别被 4 个阶为 3 的子群保持, 从而 $\mathbb{Q}(\theta_i)/\mathbb{Q}$ 是中间域扩张, 他们的阶数整除 4, 又因为 G 没有 6 阶子群, 我们就知道他们一定对应的是阶为 3 的子群

阶为 4 的子群对应的就是 $K/\mathbb{Q}$

由 Galois 对应定理, 我们知道前面的讨论给出了所有的中间域.

B

B1)

$\mathbb{F}_2[X]$ 中的二次多项式只有三个:X^2,X^2+1,X^2+X+1

前两个多项式在 $\mathbb{F}_2$ 中是分裂的, 而 X^2+X+1 在 $\mathbb{F}_2$ 之中没有根, 从而它不能写成两个 $\mathbb{F}_2[X]$ 中一次多项式的乘积, 从而它是不可约的.

B2)

先找到所有三次不可约多项式: 它们分别是 X^3+X+1,X^3+X^2+1

这两个多项式的乘积恰好为 $X^6+X^5+X^4+X^3+X^2+X+1$, 而 $X^8+X=X(X+1)(X^6+X^5+X^4+X^3+X^2+X+1)$

因此这些不可约多项式确实整除 X^8+X

B3)

直接计算可知 $(X^6+X^5+X^3+X^2+1)(X^2+X+1)=X^8+X+1$, 从而 $P_2(X)=X^6+X^5+X^3+X^2+1$

因为 $P_2(X)=X^6+X^5+X^3+X^2+1$ 无法被前面所述的 2 次和 3 次不可约多项式整除, 因此它是不可约的.

B4)

由于 $F_{n+1}(X)-F_n(X)=(F_n(X))^2-(F_{n-1}(X))^2=(F_n(X)-F_{n-1}(X))(F_n(X)+F_{n-1}(X))$

因此我们知道 $F_{n+1}(X)-F_n(X)$ 被 $F_n(X)-F_{n-1}(X)$ 整除, 进一步, 它就被 $T(X)-X=F_1(X)-F_0(X)$ 整除

更进一步, 对 $F_{n+1}(X)-F_n(X)(0\leq n\leq N-1)$ 求和就知道 $F_N(X)-X$ 被 $T(X)-X=F_1(X)-F_0(X)$ 整除

B5)

直接计算就知道 $P(X)=X^6+X^5+4X^4+3X^3+7X^2+4X+5$

利用 mod2 法, 它在 $\mathbb{F}_2$ 中就是 $P_2(X)=X^6+X^5+X^3+X^2+1$, 从而它不可约

B6)

注意到 $T^3(x)-x=F_3(x)-x$

$\mathcal{R}$ 中的元素实际上就是在代数闭域中, 全体适合 $P(X)(X^2-X+1)$ 且不适合 X^2-X+1 的元素, 因此, 他就是 $P(X)$ 的全体根的集合.

B7)

若 $x \in \mathcal{R}$, 只需要验证 $T(x)$ 满足 $\mathcal{R}$ 的两点要求:

1.$T^3(T(x)) = T(x)$, 已知等式 $T^3(x) = x$,T 同时作用于等式两端就得到验证;

2.$T \circ T(x) \neq T(x)$, 这是因为 $T \circ T(x) - T(x) = (T(x) + x)(T(x) - x)$, 已知 $T(x) - x \neq 0$, 只需验证 $T(x) + x \neq 0$, 若不然, 则 $T(x) = -x$, 也就是 $x^2 + 1 = -x$, 从而 $T^2(x) = -x, T^3(x) = -x \ldots$

又已知 $T^3(x) = x$, 这和 $T^3(x) = -x$ 共同导出 $x = 0$, 然而 $T(0) = 1 \neq -x = 0$, 这就导出了矛盾,

因此 2.$T \circ T(x) \neq T(x)$ 必然成立.

B8)

因为 $P(X)$ 是 6 次多项式, 它在分裂域上的根自然是 6 个.

因为 T 可以被视作 $\mathfrak{S}_6$ 中的元素, 并且 T 的阶数是 3, 就知道它要么是 3-循环, 要么是两个不交 3-循环的乘积.

同时, 据定义,T 在 $\mathcal{R}$ 上没有不动点, 因此它必须是两个不交三循环之积.

同时, 考虑到考虑到 $P(X)$ 的根均不在 $\mathbb{R}$ 中, 我们可以假定 $\alpha_2 = \overline{\alpha_1}, \alpha_3 = T(\alpha_1), \alpha_4 = \overline{\alpha_3}, \alpha_5 = T(\alpha_3), \alpha_6 = \overline{\alpha_5}$, 这个标号就给出了 $T = (135)(246)$

B9)

因为 $g(\mathcal{R}_1) = g \cdot T(\mathcal{R}_1) = T \cdot g(\mathcal{R}_1)$, 所以 $g(\mathcal{R}_1)$ 是一个含 3 个元素, 且被 T 保持的集合, 也就是说,$g(\mathcal{R}_1) = \mathcal{R}_1$ 或 $\mathcal{R}_2$, 此时必然有 $g(\mathcal{R}_2) = \mathcal{R}_2$ 或 $\mathcal{R}_1$

下面证明 ε 是同态:

考虑 C_T 在 $R = \{\mathcal{R}_1, \mathcal{R}_2\}$ 上的作用,ε 就是 C_T 到 $\mathfrak{S}_R \simeq \mathfrak{S}_2$ 的嵌入映射, 因此它确实是一个同态.

考虑 $g = (12)(34)(56)$, 这个元素自然被映射到 -1, 因此 ε 确实是满的.

B10)

先考虑所有满足 $\varepsilon(g)=1$ 的元素, 这样的元素属于 $\mathfrak{S}_{\mathcal{R}_1}\times\mathfrak{S}_{\mathcal{R}_2}$, 直接考察这个群里面的元素, 就知道和 $(135)(246)$ 交换的元素恰好是 $\langle(135)\rangle\times\langle(246)\rangle$ 中的所有元素, 这样的元素一共 9 个.

据此 $|C_T|=|\mathrm{Ker}\varepsilon||\mathrm{Im}\varepsilon|=18$

B11)

为此, 我们证明任意 G 中的元素 σ 都和 T 交换:

这是因为 $\sigma\circ T(x)=\sigma(x^2+1)=(\sigma(x))^2+1=T\circ\sigma(x)$. 进一步, 我们就知道 $G<C_T$

考虑到 $P(X)$ 的根均不在 $\mathbb{R}$ 中, 我们知道 $L\not\subset\mathbb{R}$ 因此复共轭映射 τ 是一个非平凡的 L-自同构, 而且它是 2 阶的, 又因为它没有不动点, 可知它是 3 个不交对换之积, 因此复共轭映射 τ 被 ε 映射到了 -1 之中, 也就是说 $\varepsilon(G)=\pm1$.

由 A9 的讨论, 我们又知道 $C_T\simeq(\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z})\rtimes\mathbb{Z}/2\mathbb{Z}$ 它的偶数阶子群要么是 $\mathbb{Z}/3\mathbb{Z}\rtimes\mathbb{Z}/2\mathbb{Z}$, 要么是 $(\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z})\rtimes\mathbb{Z}/2\mathbb{Z}$, 因此它的阶数要么是 6, 要么是 18.

B12)

任意 $Gal(L/\mathbb{Q})<C_T$ 中的元素, 要么保持 ξ,η, 要么交换他们

因为任意 $Gal(L/\mathbb{Q})$ 中的元素都保持这个多项式, 所以它是一个 $\mathbb{Q}[X]$ 上的多项式

B13)

直接由 Vieta 定理知道 $Q[X]$ 的一次项就是 1, 我们可以不妨假设 $\xi=-\frac{1}{2}+bi,\eta=-\frac{1}{2}-bi(b\in\mathbb{R})$

先计算 $\alpha_1\alpha_3+\alpha_3\alpha_5+\alpha_5\alpha_1$:

$$\alpha_1(\alpha_1^2+1)+(\alpha_1^2+1)(\alpha_1^4+2\alpha_1^2+2)+(\alpha_1^4+2\alpha_1^2+2)\alpha_1$$

$$=\alpha_1^6+\alpha_1^5+3\alpha_1^4+3\alpha_1^3+4\alpha_1^2+3\alpha_1+2$$

$$=-\alpha_1^4-3\alpha_1^2-\alpha_1-3$$

$$=-\alpha_5-\alpha_3-\alpha_1$$

B14)

我们知道 G 要么是 $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, 要么是 $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$, 因此它指标为 2 的子群是唯一的, 也就是 2 次中间域唯一.

由 B13 的讨论, 我们就知道 ξ 被包含在中间域中, 利用求根公式, 我们就知道 (一个可能的)$d = -11$

B15)

错误的, 取元素 $\delta = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)$, 此时, 我们就知道, 任意 $G \cap \mathfrak{A}_6$ 的元素 (偶置换) 都保持 δ, 而 G 中的奇置换将 δ 映射到-δ, 据此 $\mathbb{Q}(\delta)$ 是一个 2 次扩域, 且 $\delta^2 = Disc(P)$

据此, 我们知道 $\sqrt{disc(P)}$ 应当是 $\mathbb{Q}(\sqrt{d})$ 中的元素, 据此 $disc(P) \neq -33$

B16)

我们考虑 C_T 的生成元在 $\gamma_1, \gamma_2, \gamma_3, \delta_1, \delta_2, \delta_3$ 上面的作用:

1. $\tau = (12)(34)(56)$: 复共轭保持 γ_1, 将 γ_2, γ_3 映射到 γ_3, γ_2, 并且它保持 $\delta_1, \delta_2, \delta_3$

因此 τ 是集合 $\{\gamma_1, \gamma_2, \gamma_3\}$ 和集合 $\{\delta_1, \delta_2, \delta_3\}$ 上的置换

2. $\sigma = (135)$:

$\sigma(\gamma_1) = \gamma_3, \sigma(\gamma_3) = \gamma_2, \sigma(\gamma_2) = \gamma_1$

$\sigma(\delta_1) = \delta_3, \sigma(\delta_3) = \delta_2, \sigma(\delta_2) = \delta_1$

因此 σ 是集合 $\{\gamma_1, \gamma_2, \gamma_3\}$ 和集合 $\{\delta_1, \delta_2, \delta_3\}$ 上的置换

据此,C_T 全体生成元都保持 $A(X), B(X)$, 也就是 G 中的元素都保持 $A(X), B(X)$, 进一步, 他们的系数属于 $L^G = \mathbb{Q}$

B17)

可以适当" 平移" 多项式而不改变多项式的判别式 (因为这不改变分裂域中根的差值):

考虑 $A'(X) = A(X+1)$, 则 $A'(X) = X^3 - 9X - 36$, 那么 $\mathrm{Disc}(A) = \mathrm{Disc}(A') = -4 \cdot (-9)^3 - 27 \cdot (36)^2 = -22 \cdot 36 \cdot 11$

同理, 考虑 $B'(X)=B(X+1)$, 则 $B'(X)=X^3-9X-9$, 那么 $\mathrm{Disc}(B)=\mathrm{Disc}(B')=-4\cdot(-9)^3-27\cdot(-9)^2=3^6$

B18)

因为 $A(X),B(X)$ 没有有理根 (据有理根定理 $A'(X),B'(X)$ 的根分别是整除 36 和 9 的整数, 直接代入可知他们不是根), 他们是 $\mathbb{Q}$ 上的不可约多项式

据此, 考虑域扩张 $\mathbb{Q}(\gamma_1)$ 和域扩张 $\mathbb{Q}(\delta_1)$, 下面说明他们不是同一个域扩张:

考虑判别式,$\mathrm{Disc}(A)$ 不是 $\mathbb{Q}$ 中元素的平方, 因此 $\mathbb{Q}(\gamma_1)$ 不是一个 Galois 扩张, 而 $\mathrm{Disc}(B)$ 是 $\mathbb{Q}$ 中元素的平方, 因此 $\mathbb{Q}(\delta_1)$ 是一个 Galois 扩张, 这说明 $L/\mathbb{Q}$ 有两个不相同的, 次数为 3 的中间域

根据 Galois 对应定理,G 有两个不相同的指数为 3 的子群, 也就是说 $G\not\simeq D_3$, 根据前面的讨论 $G\simeq C_T$