群与 Galois 理论

作业 8

陈宏泰

2024011131

清华大学数学科学系

cht24@mails.tsinghua.edu.cn

2026 年 1 月 2 日

目录

A. X^6-3X^2-1 的 Galois 群

1. 证明, $P(X)=X^3-3X-1\in\mathbb{Q}[X]$ 有 3 个实根 $\alpha_1,\alpha_2,\alpha_3$ 满足 $\alpha_1>0>\alpha_2>\alpha_3$ 并且对任意 $\alpha\in\{\alpha_1,\alpha_2,\alpha_3\}$, $2-\alpha^2$ 是 P 的根。

证明： 注意到 $P(-2)=-3<0$, $P(-1)=1>0$, $P(0)=-1<0$, $P(1)=-3<0$, $P(2)=3>0$, 由介值定理可知, P 在区间 $(-2,-1),(-1,0),(1,2)$ 上各有一个实根, 记为 $\alpha_3,\alpha_2,\alpha_1$, 则 $\alpha_1>0>\alpha_2>\alpha_3$.

任取 $\alpha\in\{\alpha_1,\alpha_2,\alpha_3\}$, 有

$$\begin{aligned}P(2-\alpha^2)&=(2-\alpha^2)^3-3(2-\alpha^2)-1\\&=8-12\alpha^2+6\alpha^4-\alpha^6-6+3\alpha^2-1\\&=-\alpha^6+6\alpha^4-9\alpha^2+1\\&=-(3\alpha+1)^2+6\alpha(3\alpha+1)-9\alpha^2+1\\&=-9\alpha^2-6\alpha-1+18\alpha^2+6\alpha-9\alpha^2+1\\&=0.\end{aligned}$$

从而, $2-\alpha^2$ 是 P 的根. □

2. 令 K 为 P 在 $\mathbb{Q}$ 上的分裂域。证明, $K=\mathbb{Q}(\alpha_1)$ 并且 $\mathbf{Gal}(K/\mathbb{Q})\simeq\mathbb{Z}/3\mathbb{Z}$。

证明： $K=\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$. 而容易推理出 $2-\alpha_2^2=\alpha_1$, 进一步有 $2-\alpha_1^2=\alpha_3$, $2-\alpha_3^2=\alpha_2$. 于是 $K=\mathbb{Q}(\alpha_1)$.

设 $\sigma\in\mathbf{Gal}(K/\mathbb{Q})$, 则 σ 由 $\sigma(\alpha_1)$ 唯一确定. 由于 σ 是 $\mathbb{Q}$-自同构, 所以 $\sigma(\alpha_1)$ 也是 P 的根, 因此 $\sigma(\alpha_1)\in\{\alpha_1,\alpha_2,\alpha_3\}$. 这说明 $|\mathbf{Gal}(K/\mathbb{Q})|=3$. 由于任何阶为 3 的群都是循环群, 所以 $\mathbf{Gal}(K/\mathbb{Q})\simeq\mathbb{Z}/3\mathbb{Z}$。 □

3. 对每个 $i=1,2,3$, 选定 $\beta_i\in\mathbb{C}$, 使得 $\beta_i^2=\alpha_i$ 并且 $\beta_1\beta_2\beta_3=1$。计算 $[K(\beta_1):K]$。

解：

$\alpha_1,\alpha_2,\alpha_3\notin K$ 从而也 $\notin K^2$. 所以 $\beta_i\notin K$. 因此, $X^2-\alpha_i$ 在 K 上不可约, 从而 $[K(\beta_i):K]=2$. 特别地, $[K(\beta_1):K]=2$. □

4. 证明, $L=\mathbb{Q}(\beta_1,\beta_2)$ 是 $\mathbb{Q}$ 上的 Galois 扩张并计算 $[L:\mathbb{Q}]$。自此往后, 令 $G=\mathbf{Gal}(L/\mathbb{Q})$。

证明： 由于 $\beta_1,\beta_2\in L$, 所以 $\beta_3=\frac{1}{\beta_1\beta_2}\in L$. 因此, L 是 X^6-3X^2-1 在 $\mathbb{Q}$ 上的分裂域, 从而是 Galois 扩张.($\mathbb{Q}$ 的特征为 0, 所以总是可分扩张)

由于 $[K:\mathbb{Q}]=3$, $[\mathbb{Q}(\beta_1):K]=2$, $[L:\mathbb{Q}(\beta_1)]=2$, 所以 $[L:\mathbb{Q}]=3\times2\times2=12$. 其中 $L\neq\mathbb{Q}(\beta_1)$ 因为 $\beta_2\in\mathbb{C}\backslash\mathbb{R}$, 而 $\mathbb{Q}(\beta_1)\subset\mathbb{R}$. 即有如下扩张列:

$$\mathbb{Q}\ \overset{3}{\text{——}}\ K=\mathbb{Q}(\alpha_1)\ \overset{2}{\text{——}}\ \mathbb{Q}(\beta_1)\ \overset{2}{\text{——}}\ L=\mathbb{Q}(\beta_1,\beta_2)$$

□

5. G 有几个的 Sylow 2-子群？证明, 它们都同构于 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$。

证明： 设 n_2 为 G 的 Sylow 2-子群的个数。由 Sylow 定理, 有 $n_2 \equiv 1 \pmod 2$ 且 $n_2 \mid 3$. 因此, $n_2 = 1$ 或 3.

又 Galois 对应定理, $K/\mathbb{Q}$ 是一个三次扩张, 所以对应着 G 的一个指数为 3 的子群 H, 即 $|H| = 4$. 又由于 $K/\mathbb{Q}$ 是正规扩张, 故 H 是 G 的一个正规子群. 因此 H 是 G 唯一的 Sylow 2-子群, 即 $n_2 = 1$.

由 Galois 对应定理, $H = \mathrm{Gal}(L/K)$. 设 $\sigma \in H$, 那么 $\sigma(\beta_i^2) = \sigma(\alpha_i) = \alpha_i = \beta_i^2$, 因此 $\sigma(\beta_i) = \pm\beta_i$. 那么 $\mathrm{ord}(\sigma)$ 只能是 1 或 2. 于是 H 不是循环群, 故 $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

6. 证明, 以下 12 个映射所给的 β_1 与 β_2 的像决定了 G 中所有元素：

$$\begin{cases}\beta_1 \mapsto \beta_1,\\ \beta_2 \mapsto \beta_2;\end{cases} \quad \begin{cases}\beta_1 \mapsto \beta_1,\\ \beta_2 \mapsto -\beta_2;\end{cases} \quad \begin{cases}\beta_1 \mapsto -\beta_1,\\ \beta_2 \mapsto \beta_2;\end{cases} \quad \begin{cases}\beta_1 \mapsto -\beta_1,\\ \beta_2 \mapsto -\beta_2;\end{cases} \quad \begin{cases}\beta_1 \mapsto \beta_2,\\ \beta_2 \mapsto \beta_3;\end{cases} \quad \begin{cases}\beta_1 \mapsto \beta_2,\\ \beta_2 \mapsto -\beta_3;\end{cases}$$

$$\begin{cases}\beta_1 \mapsto -\beta_2,\\ \beta_2 \mapsto \beta_3;\end{cases} \quad \begin{cases}\beta_1 \mapsto -\beta_2,\\ \beta_2 \mapsto -\beta_3;\end{cases} \quad \begin{cases}\beta_1 \mapsto \beta_3,\\ \beta_2 \mapsto \beta_1;\end{cases} \quad \begin{cases}\beta_1 \mapsto \beta_3,\\ \beta_2 \mapsto -\beta_1;\end{cases} \quad \begin{cases}\beta_1 \mapsto -\beta_3,\\ \beta_2 \mapsto \beta_1;\end{cases} \quad \begin{cases}\beta_1 \mapsto -\beta_3,\\ \beta_2 \mapsto -\beta_1.\end{cases}$$

证明： 由第 2 问可以知道 $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$. 于是 $\forall\sigma \in G$, $\sigma|_K$ 为 $\mathrm{Gal}(K/\mathbb{Q})$ 中的某个元素 (由 $K/\mathbb{Q}$ 是正规的推出). 那么 σ 作用在 $\{\alpha_1, \alpha_2, \alpha_3\}$ 上只有三种可能性:

$$\begin{cases}\alpha_1 \mapsto \alpha_1,\\ \alpha_2 \mapsto \alpha_2,\\ \alpha_3 \mapsto \alpha_3;\end{cases} \quad \begin{cases}\alpha_1 \mapsto \alpha_2,\\ \alpha_2 \mapsto \alpha_3,\\ \alpha_3 \mapsto \alpha_1;\end{cases} \quad \begin{cases}\alpha_1 \mapsto \alpha_3,\\ \alpha_2 \mapsto \alpha_1,\\ \alpha_3 \mapsto \alpha_2.\end{cases}$$

由于 $\beta_i^2 = \alpha_i$, 所以 $\sigma(\beta_i) = \pm\beta_j$ 其中 j 由上面的映射决定. 因此, σ 作用在 $\{\beta_1, \beta_2, \beta_3\}$ 上共有 12 种可能性, 即题中所列的 12 个映射. 由于 $[L : \mathbb{Q}] = 12$, 所以这 12 个映射对应着 G 中所有元素. □

7. 给出 G 的所有 Sylow 3-子群并证明 $G \simeq \mathfrak{A}_4$。

证明： 设 n_3 为 G 的 Sylow 3-子群的个数。由 Sylow 定理, 有 $n_3 \equiv 1 \pmod 3$ 且 $n_3 \mid 12$. 因此, $n_3 = 1$ 或 4.

可以直接给出所有的 Sylow 3-子群:

$$\left(\begin{cases}\beta_1\mapsto\beta_1,\\ \beta_2\mapsto\beta_2;\end{cases}\quad\begin{cases}\beta_1\mapsto\beta_2,\\ \beta_2\mapsto\beta_3;\end{cases}\quad\begin{cases}\beta_1\mapsto\beta_3,\\ \beta_2\mapsto\beta_1.\end{cases}\right)$$

$$\left(\begin{cases}\beta_1\mapsto\beta_1,\\ \beta_2\mapsto-\beta_2;\end{cases}\quad\begin{cases}\beta_1\mapsto-\beta_2,\\ \beta_2\mapsto-\beta_3;\end{cases}\quad\begin{cases}\beta_1\mapsto-\beta_3,\\ \beta_2\mapsto\beta_1.\end{cases}\right)$$

$$\left(\begin{cases}\beta_1\mapsto-\beta_1,\\ \beta_2\mapsto\beta_2;\end{cases}\quad\begin{cases}\beta_1\mapsto\beta_2,\\ \beta_2\mapsto-\beta_3;\end{cases}\quad\begin{cases}\beta_1\mapsto-\beta_3,\\ \beta_2\mapsto-\beta_1.\end{cases}\right)$$

$$\left(\begin{cases}\beta_1\mapsto-\beta_1,\\ \beta_2\mapsto-\beta_2;\end{cases}\quad\begin{cases}\beta_1\mapsto-\beta_2,\\ \beta_2\mapsto\beta_3;\end{cases}\quad\begin{cases}\beta_1\mapsto\beta_3,\\ \beta_2\mapsto-\beta_1.\end{cases}\right)$$

于是 $n_3=4$.

G 是非交换的, 而非交换的阶为 12 的群只有 D_6, $\mathfrak{A}_4$ 和 $\mathbb{Z}/3\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z}$. 由于 G 只有单位元, (3 个) 2 阶元和 (8 个) 3 阶元. 因此 $G\simeq\mathfrak{A}_4$. □

注：如果不想知道 12 阶群的分类, 而想直接地看出 $G\simeq\mathfrak{A}_4$, 那么 G 中元素可以实现为第 8 小问中 $\{\theta_1,\theta_2,\theta_3,\theta_4\}$ 的置换.

8. 令 $\theta_1=\beta_1+\beta_2+\beta_3,\theta_2=-\beta_1+\beta_2-\beta_3,\theta_3=\beta_1-\beta_2-\beta_3,\theta_4=-\beta_1-\beta_2+\beta_3$。证明, 以下给出了 $L/\mathbb{Q}$ 的所有非平凡中间域：

$$\left\{\mathbb{Q}\left(\beta_1^2\right),\mathbb{Q}\left(\beta_1\right),\mathbb{Q}\left(\beta_2\right),\mathbb{Q}\left(\beta_3\right),\mathbb{Q}\left(\theta_1\right),\mathbb{Q}\left(\theta_2\right),\mathbb{Q}\left(\theta_3\right),\mathbb{Q}\left(\theta_4\right)\right\}$$

证明：由 Galois 对应定理, L 的中间域与 G 的子群一一对应.

由第 5 问可知, G 有一个 4 阶子群对应着 $\mathbb{Q}(\beta_1^2)$. 由第 6 问可知, G 有 3 个 2 阶元, 从而有 3 个 2 阶子群分别对应着 $\mathbb{Q}(\beta_1),\mathbb{Q}(\beta_2),\mathbb{Q}(\beta_3)$. 再由第 7 问可知, G 有 4 个 3 阶子群分别对应着 $\mathbb{Q}(\theta_1),\mathbb{Q}(\theta_2),\mathbb{Q}(\theta_3),\mathbb{Q}(\theta_4)$.(可以轻松验证 θ_i 在对应的 3 阶子群下不变)

综上所述, L 的所有非平凡中间域如题所示. □

B. 一个 6 次多项式分裂域的 Galois 群的计算

1. 证明, X^2+X+1 是 $\mathbb{F}_2[X]$ 中唯一一个二次不可约多项式。

证明： 设 $P(X)$ 为 $\mathbb{F}_2[X]$ 中任意一个二次多项式. 如果 $P(X)$ 可约, 则 $P(X)$ 可以写成 $(X+a)(X+b)$ 的形式, 其中 $a,b\in\mathbb{F}_2$. 通过枚举, 可以验证 $P(X)$ 只能是 X^2, X^2+1, X^2+X. 因此, $\mathbb{F}_2[X]$ 中唯一的二次不可约多项式是 X^2+X+1. □

2. 证明, $\mathbb{F}_2[X]$ 中每个三次不可约多项式都整除 X^8+X。

证明： 设 $P(X)$ 为 $\mathbb{F}_2[X]$ 中任意一个三次不可约多项式. 考虑域扩张 $\mathbb{F}_2[X]/(P(X)) =: K(\alpha)$, 其中 α 是 $P(X)$ 的一个根. 由有限域的结论可知 $|K|=2^3=8$. 那么 $|K^\times|=7$. 根据第一次作业知 $K^\times$ 是一个 7 阶循环群, 因此, $\forall x\in K^\times$, $x^7=1$. 于是, $\forall x\in K$, $x^8=x$. 也即 x 是多项式 X^8-X 的根. 将 X^8-X 视为 $\mathbb{F}_2$ 上的多项式, 也即 X^8+X. 由于 $P(\alpha)=0$, 所以 $P(X)$ 整除 X^8+X. □

3. 证明, 在 $\mathbb{F}_2[X]$ 中, X^2+X+1 整除 X^8+X+1。计算 $P_2(X)=\frac{X^8+X+1}{X^2+X+1}$ 并证明 $P_2(X)$ 是不可约的。

证明： 直接计算可得

$$P_2(X)=X^6+X^5+X^3+X^2+1.$$

因此在 $\mathbb{F}_2[X]$ 中, X^2+X+1 整除 X^8+X+1.

下面证明 $P_2(X)$ 是不可约的. 如果 $P_2(X)$ 可约, 则有三种可能:

- $P_2(X)$ 有一个一次因子. 由于 $\mathbb{F}_2$ 中只有两个元素 0 和 1, 所以只需验证 $P_2(0)$ 和 $P_2(1)$ 是否为 0. 计算可得 $P_2(0)=1, P_2(1)=1$. 因此, $P_2(X)$ 没有一次因子.
- $P_2(X)$ 可以被一个二次不可约多项式整除. 由于 $\mathbb{F}_2[X]$ 中唯一的二次不可约多项式是 X^2+X+1, 但是 $P_2(X)=(X^2+X+1)(X^4+X^2)+1$, 于是 X^2+X+1 不能整除 $P_2(X)$.
- $P_2(X)$ 可以被三次不可约多项式整除. 设 $Q(X)$ 为 $\mathbb{F}_2[X]$ 中任意一个三次不可约多项式, 且 $Q|P_2$. 那么 $Q|P_2|X^8+X+1$, 但又由第 2 小问可知 $Q|X^8+X$, 于是 $Q|1$, 矛盾.

综上所述, $P_2(X)$ 是不可约的. □

4. 令 $T(X)=X^2+1\in\mathbb{Z}[X], F_0(X)=X, F_n(X)=T\left(F_{n-1}(X)\right)$, 其中, $n\geqslant 1$。证明, 在 $\mathbb{Z}[X]$ 中, $T(X)-X$ 整除 $F_n(X)-F_{n-1}(X)$, 其中, $n\geqslant 1$；进一步证明, 在 $\mathbb{Z}[X]$ 中, $T(X)-X$ 整除 $F_3(X)-X$。

证明： 注意到 $T(X)-X=F_1(X)-F_0(X)$. 那么只需证明 $F_n(X)-F_{n-1}(X)|F_{n+1}(X)-F_n(X)$

即可. 计算可得

$$\begin{aligned} F_{n+1}(X) - F_n(X) &= T(F_n(X)) - F_n(X) \\ &= (F_n(X))^2 + 1 - F_n(X) \\ &= (F_n(X))^2 + 1 - (F_{n-1}(X)^2 + 1) \\ &= (F_n(X) - F_{n-1}(X))(F_n(X) + F_{n-1}(X)). \end{aligned}$$

于是, $F_n(X) - F_{n-1}(X) | F_{n+1}(X) - F_n(X)$. 进一步, $T(X) - X | F_2(X) - F_1(X) | \cdots | F_n(X) - F_{n-1}(X)$.

特别地, $T(X) - X | F_2(X) - F_1(X) | F_3(X) - F_2(X)$. 于是

$$F_3(X) - X = (F_3(X) - F_2(X)) + (F_2(X) - F_1(X)) + (F_1(X) - F_0(X)) \qquad (*)$$

从而可知 $T(X) - X$ 整除 $F_3(X) - X$. □

5. 证明, 在 $\mathbb{Z}[X]$ 中, 计算 $P(X) = \frac{F_3(X)-X}{T(X)-X}$（你可以用 $P(10) = 1143745$ 来检验答案的正确性）并证明 $P(X)$ 是 $\mathbb{Z}[X]$ 中的不可约多项式。

提示：如果一个多项式在 $\mathbb{Z}[X]$ 中可约, 那么它在 $\mathbb{F}_p[X]$ 中也是可约的。

证明：利用带余除法直接计算可知

$$P(X) = X^6 + X^5 + 4X^4 + 3X^3 + 7X^2 + 4X + 5.$$

(可以用 $P(10) = 1143745$ 来“检验”答案的正确性).

下面证明 $P(X)$ 在 $\mathbb{Z}[X]$ 中不可约. 注意到 $P(X)$ 在 mod 2 意义下的像恰为 $P_2(X)$, 而由第 3 问可知 $P_2(X)$ 在 $\mathbb{F}_2[X]$ 中不可约, 于是 $P(X)$ 在 $\mathbb{Z}[X]$ 中不可约. □

6. 令 $\mathcal{R} = \{x \in \overline{\mathbb{Q}} \mid P(x) = 0\}$ 为 P 根的集合, L 为 P 在 $\mathbb{Q}$ 上的分裂域 (不妨假设 $L \subset \overline{\mathbb{Q}} \subset \mathbb{C}$), $G := \mathrm{Gal}(L/\mathbb{Q})$ 为其 Galois 群。证明, $\mathcal{R}$ 可以如下描述：

$$\mathcal{R} = \{x \in \overline{\mathbb{C}} \mid T(T(T(x))) = x, \text{但是} T(x) \neq x\}.$$

证明：这是 4、5 小问的直接推论. □

7. 证明, 对任意的 $x \in \mathcal{R}$, 我们有 $T(x) \in \mathcal{R}$, 从而, 以下映射是良好定义的：

$$T : \mathcal{R} \longrightarrow \mathcal{R}.$$

证明：设 $x \in \mathcal{R}$. 由第 6 问可知 $T(T(T(x))) = x$. 那么

$$T(T(T(T(x)))) = T(x).$$

并且 $T(x) \neq x$. 另一方面, 根据 $(*)$ 式, 有

$$T(T(T(x))) - x = (T(T(T(x))) - T(T(x))) + (T(T(x)) - T(x)) + (T(x) - x).$$

如果 $T(T(x))=T(x)$, 并且 $T(T(X))-T(X)=F_2(X)-F_1(X)|F_3(X)-F_2(X)=T(T(T(X)))-T(T(X))$, 那么 $T(T(T(x)))=T(T(x))$. 从而上式左边为 0, 右边前两个式子也为 0, 而 $T(x)\neq x$, 矛盾. 于是, $T(T(x))\neq T(x)$.

综上所述, $T(x)\in\mathcal{R}$. □

8. 证明, $|\mathcal{R}|=6$ 并且可以将 $\mathcal{R}$ 中的元素记作是

$$\mathcal{R}=\{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6\}=\underbrace{\{\alpha_1,\alpha_3,\alpha_5\}}_{\mathcal{R}_1}\cup\underbrace{\{\alpha_2,\alpha_4,\alpha_6\}}_{\mathcal{R}_2}.$$

使得 $T(\alpha_1)=\alpha_3, T(\alpha_3)=\alpha_5, T(\alpha_5)=\alpha_1$ 而 $T(\alpha_2)=\alpha_4, T(\alpha_4)=\alpha_6, T(\alpha_6)=\alpha_2$。特别地, 如果将 $\mathfrak{S}_{\mathcal{R}}$ 与 $\mathfrak{S}_6$ 等同, 其中, $\alpha_i\in\mathcal{R}$ 对应着指标 i, 那么, T 可以被视作是 $(1,3,5)(2,4,6)\in\mathfrak{S}_6$。

证明： 设 $x\in\mathcal{R}$. 由第 6 问可知 $T(T(T(x)))=x$. 由于 T 在 $\mathcal{R}$ 上是一个映射, 所以 T 在 $\mathcal{R}$ 上是一个置换. 由于 $P(X)$ 是 6 次不可约多项式, 所以 $|\mathcal{R}|=6$. 于是, T 在 $\mathcal{R}$ 上有两个不相交的 3 循环. 任取 $\alpha_1\in\mathcal{R}$, 定义 $\alpha_3=T(\alpha_1), \alpha_5=T(\alpha_3)$. 再任取 $\alpha_2\in\mathcal{R}\backslash\{\alpha_1,\alpha_3,\alpha_5\}$, 定义 $\alpha_4=T(\alpha_2), \alpha_6=T(\alpha_4)$. 于是, $\mathcal{R}$ 可以写成题中所示的形式, 并且 T 可以视作 $(1,3,5)(2,4,6)\in\mathfrak{S}_6$. □

9. 令 $C_T=\{g\in\mathfrak{S}_6\mid g\cdot T=T\cdot g\}$ 为 T 在 $\mathfrak{S}_6$ 中的中心化子。证明, 对任意的 $g\in C_T$, 我们有 $g(\mathcal{R}_1)=\mathcal{R}_1, g(\mathcal{R}_2)=\mathcal{R}_2$ 或者 $g(\mathcal{R}_1)=\mathcal{R}_2, g(\mathcal{R}_2)=\mathcal{R}_1$。据此, 证明以下映射是**满的**群同态：

$$\varepsilon: C_T\to\{\pm1\},\quad \varepsilon(g)=\begin{cases}1, & \text{如果} g(\mathcal{R}_1)=\mathcal{R}_1;\\ -1, & \text{如果} g(\mathcal{R}_1)=\mathcal{R}_2.\end{cases}$$

其中, $\{\pm1\}$ 是 2 阶循环群。

证明： 设 $g\in C_T$. 由于 $gT=Tg$, 也即 $gTg^{-1}=T$. 于是, g 的共轭作用将 T 的两个 3 循环要么分别映射到自己, 要么互相交换. 也即, $g(\mathcal{R}_1)=\mathcal{R}_1, g(\mathcal{R}_2)=\mathcal{R}_2$ 或者 $g(\mathcal{R}_1)=\mathcal{R}_2, g(\mathcal{R}_2)=\mathcal{R}_1$.

下面证明 ε 是满的群同态. 设 $g_1,g_2\in C_T$. 如果 $g_1(\mathcal{R}_1)=\mathcal{R}_1, g_2(\mathcal{R}_1)=\mathcal{R}_1$, 那么 $(g_1g_2)(\mathcal{R}_1)=\mathcal{R}_1$. 如果 $g_1(\mathcal{R}_1)=\mathcal{R}_1, g_2(\mathcal{R}_1)=\mathcal{R}_2$, 那么 $(g_1g_2)(\mathcal{R}_1)=\mathcal{R}_2$. 如果 $g_1(\mathcal{R}_1)=\mathcal{R}_2, g_2(\mathcal{R}_1)=\mathcal{R}_1$, 那么 $(g_1g_2)(\mathcal{R}_1)=\mathcal{R}_2$. 如果 $g_1(\mathcal{R}_1)=\mathcal{R}_2, g_2(\mathcal{R}_1)=\mathcal{R}_2$, 那么 $(g_1g_2)(\mathcal{R}_1)=\mathcal{R}_1$. 综上所述, $\varepsilon(g_1g_2)=\varepsilon(g_1)\varepsilon(g_2)$, 也即 ε 是群同态 (这完全是显然的). 另外, 设 $g\in\mathfrak{S}_6$ 为 $(1,2)(3,4)(5,6)$, 那么 $g\in C_T$ 且 $g(\mathcal{R}_1)=\mathcal{R}_2$. 于是, ε 是满的.

综上所述, ε 是满的群同态. □

10. 证明, $|C_T|=18$。

证明： 考虑 $g\in C_T$ 在 $\{\alpha_1,\alpha_2\}$ 上的作用, 这已经可以决定 g 在 $\mathcal{R}$ 上的作用. 因为如果 $g(\alpha_1)=\alpha_i$, 那么 $g(\alpha_3)=g(T(\alpha_1))=T(g(\alpha_1))=T(\alpha_i)$, $g(\alpha_5)=g(T(\alpha_3))=T(g(\alpha_3))=T^2(\alpha_i)$. 同理, 如果 $g(\alpha_2)=\alpha_j$, 那么 $g(\alpha_4)=T(\alpha_j), g(\alpha_6)=T^2(\alpha_j)$.

先考虑 $g(\alpha_1)$, 其可以是任意 $\alpha_i, 1 \leqslant i \leqslant 6$. 再考虑 $g(\alpha_2)$, 由于第 9 小问, $g(\alpha) \in \mathcal{R}\backslash\{g(\alpha_1), T(g(\alpha_1)), T^2(g(\alpha_1))\}$. 因此, $g(\alpha_2)$ 有 3 种选择. 综上所述, $|C_T| = 6 \times 3 = 18$.

□

11. 我们可以将 $G \coloneqq \mathrm{Gal}(L/\mathbb{Q})$ 视作是 $\mathfrak{S}_{\mathcal{R}} = \mathfrak{S}_6$ 的子群。证明, $G < C_T, \varepsilon|_G : G \to \{\pm 1\}$ 也是满射并且 $|G| = 6$ 或 18。

证明： 设 $\sigma \in G$. 由于 σ 是 $L/\mathbb{Q}$ 的自同构, 所以 G 可以作用在 $\mathcal{R}$ 上. 而

$$\sigma(T(\alpha)) = \sigma(\alpha^2 + 1) = \sigma(\alpha)^2 + 1 = T(\sigma(\alpha)),$$

也即 $\sigma T = T\sigma$. 于是, $G < C_T$.

下面证明 $\varepsilon|_G$ 是满射. 设 $\alpha_1 \in \mathcal{R}$. 由于 $P(X)$ 在 $\mathbb{Q}$ 中不可约, 所以 G 在 $\mathcal{R}$ 上的作用是传递的. 于是存在 $\tau \in G$ 使得 $\tau(\alpha_1) = \alpha_2$. 那么 $\tau(\alpha_2) = \tau(T(\alpha_1)) = T(\tau(\alpha_1)) = T(\alpha_2) = \alpha_4$, $\tau(\alpha_4) = \tau(T(\alpha_2)) = T(\tau(\alpha_2)) = T(\alpha_4) = \alpha_6$, $\tau(\alpha_6) = \tau(T(\alpha_4)) = T(\tau(\alpha_4)) = T(\alpha_6) = \alpha_2$. 于是, $\tau(\mathcal{R}_1) = \mathcal{R}_2$. 因此, $\varepsilon|_G$ 是满射.

由于 $G < C_T$, 所以 $|G|$ 整除 $|C_T| = 18$. 又由于 $\varepsilon|_G$ 是满射, 所以 $|G|$ 是 2 的倍数. 又 $|G| \geqslant \deg P = 6$. 综上所述, $|G| = 6$ 或 18. □

12. 令 $\xi = \alpha_1 + \alpha_3 + \alpha_5, \eta = \alpha_2 + \alpha_4 + \alpha_6$, 证明, $Q(X) = (X - \xi)(X - \eta) \in \mathbb{Q}[X]$。注意, 不能使用本题后面的结论。

证明： 设 $\sigma \in G$, 由第 9、10 小问, $\sigma(\mathcal{R}_1) = \mathcal{R}_1, \sigma(\mathcal{R}_2) = \mathcal{R}_2$ 或 $\sigma(\mathcal{R}_1) = \mathcal{R}_2, \sigma(\mathcal{R}_2) = \mathcal{R}_1$. 那么

$$\sigma(\xi) = \sum_{\alpha \in \mathcal{R}_1} \sigma(\alpha) = \begin{cases} \xi, & \text{如果} \sigma(\mathcal{R}_1) = \mathcal{R}_1; \\ \eta, & \text{如果} \sigma(\mathcal{R}_1) = \mathcal{R}_2. \end{cases}$$

$$\sigma(\eta) = \sum_{\alpha \in \mathcal{R}_2} \sigma(\alpha) = \begin{cases} \eta, & \text{如果} \sigma(\mathcal{R}_2) = \mathcal{R}_2; \\ \xi, & \text{如果} \sigma(\mathcal{R}_2) = \mathcal{R}_1. \end{cases}$$

于是, σ 作用在 $Q(X) = (X - \xi)(X - \eta)$ 上时, 仅仅是交换 ξ 和 η 或者不变. 也即, $\sigma(Q(X)) = Q(X)$. 由于 $\sigma \in G$ 是任意的, 由 Galois 对应定理, $Q(X)$ 的系数都在 $L^G = \mathbb{Q}$ 中, 所以 $Q(X) \in \mathbb{Q}[X]$. □

13. 证明, $Q(X) = X^2 + X + 3 \in \mathbb{Z}[X]$。

证明： 由第 12 小问可知 $Q(X) \in \mathbb{Q}[X]$. 计算可得

$$\xi + \eta = (\alpha_1 + \alpha_3 + \alpha_5) + (\alpha_2 + \alpha_4 + \alpha_6) = \sum_{i=1}^{6} \alpha_i = -1,$$

$$\begin{aligned} \xi\eta &= (\alpha_1 + \alpha_3 + \alpha_5)(\alpha_2 + \alpha_4 + \alpha_6) \\ &= \sum_{i<j} \alpha_i\alpha_j - (\alpha_1\alpha_3 + \alpha_3\alpha_5 + \alpha_5\alpha_1) - (\alpha_2\alpha_4 + \alpha_4\alpha_6 + \alpha_6\alpha_2) \end{aligned}$$

再计算 $\alpha_1\alpha_3+\alpha_3\alpha_5+\alpha_5\alpha_1$ 和 $\alpha_2\alpha_4+\alpha_4\alpha_6+\alpha_6\alpha_2$,

$$\begin{aligned}\alpha_1\alpha_3+\alpha_3\alpha_5+\alpha_5\alpha_1 &= \alpha_1\alpha_3+(\alpha_1^2+1)((\alpha_1^2+1)^2+1)+((\alpha_1^2+1)^2+1)\alpha_1\\ &= \alpha_1^6+\alpha_1^5+3\alpha_1^4+3\alpha_1^3+4\alpha_1^2+3\alpha_1+2,\\ &= -(\alpha_1^4+3\alpha_1^2+\alpha_1+3)\\ &= -(\alpha_1+\alpha_3+\alpha_5)\\ &= -\xi,\\ \alpha_2\alpha_4+\alpha_4\alpha_6 &= -\eta\\ \Rightarrow \xi\eta &= \sum_{i<j}\alpha_i\alpha_j+\xi+\eta = 4-1=3.\end{aligned}$$

从而 $Q(X)=X^2+X+3$. □

14. 令 $H\coloneqq \mathrm{Ker}\,(\varepsilon|_G: G\to\{\pm1\})$, 证明, L^H 是 $L/\mathbb{Q}$ 的唯一 2 次的中间域。进一步给出整数 d, 使得该中间域为 $\mathbb{Q}(\sqrt{d})$。

证明： 由第 11 小问可知, $|G|=6$ 或 18. 由于 $\varepsilon|_G$ 是满射, 易知 $\#\{g\mid\varepsilon(g)=1\}=\#\{g\mid\varepsilon(g)=-1\}$, 所以 $|H|=\frac{|G|}{2}=3$ 或 9. 从而 H 总是 G 的 Sylow-3 子群, 又有 $H\triangleleft G$, 于是 H 是 G 唯一阶为 $|H|=\frac{|G|}{2}$ 的子群. 于是由 Galois 对应定理可知, L^H 是 $L/\mathbb{Q}$ 唯一的 2 次中间域.

下面给出整数 d 使得 $L^H=\mathbb{Q}(\sqrt{d})$. 由于 $[L^H:\mathbb{Q}]=2$, 所以存在 $d\in\mathbb{Z}$ 使得 $L^H=\mathbb{Q}(\sqrt{d})$. 由第 13 小问可知, $\mathbb{Q}[X]/Q(X)$ 是 $L/\mathbb{Q}$ 的 2 次中间域, 从而是唯一的 2 次中间域 L^H. $Q(X)=X^2+X+3$ 在 $\mathbb{Z}[X]$ 中不可约, 所以 $\xi,\eta\notin\mathbb{Q}$. 于是, ξ,η 都是 L^H 的生成元. 计算可得

$$(\xi-\eta)^2=(\xi+\eta)^2-4\xi\eta=(-1)^2-4\times3=-11.$$

于是, $L^H=\mathbb{Q}(\sqrt{-11})$. 因为 ξ 和 η 可以表示为

$$\xi=\frac{-1+\sqrt{-11}}{2},\quad \eta=\frac{-1-\sqrt{-11}}{2}.$$

□

15. 利用 GaloisGPT 软件, 得到 P 的判别式 $\mathrm{Disc}(P)=-33$, 请问它的结果是否正确并给出理由。

证明： 设 $P(X)=\prod_{i=1}^6(X-\alpha_i)$. 那么

$$\mathrm{Disc}(P)=-\prod_{1\leqslant i<j\leqslant6}(\alpha_i-\alpha_j)^2.$$

从而我们可以考虑 $\delta=\prod_{1\leqslant i<j\leqslant6}(\alpha_i-\alpha_j)=\sqrt{33}$. 那么 δ 在 $G\cap\mathfrak{A}_6$ 作用下不变, 而在 G 中奇置换下变号. 于是, $\delta\notin\mathbb{Q}$, 但是 $\delta^2\in\mathbb{Q}$. 由第 14 小问可知, $\mathbb{Q}(\delta)=L^H=\mathbb{Q}(\sqrt{-11})$. 于是, δ 可以表示为 $a+b\sqrt{-11}$, 其中 $a,b\in\mathbb{Q}$. 但由于 $\sqrt{33}$ 是无理数, 可以推出矛盾. 于是, P 的判别式 $\mathrm{Disc}(P)=-33$ 不正确. □

16. 令

$$\begin{cases}\gamma_1=\alpha_1\alpha_2+\alpha_3\alpha_4+\alpha_5\alpha_6,\\ \gamma_2=\alpha_1\alpha_4+\alpha_3\alpha_6+\alpha_5\alpha_2,\\ \gamma_3=\alpha_1\alpha_6+\alpha_3\alpha_2+\alpha_5\alpha_4,\end{cases}\qquad \begin{cases}\delta_1=\alpha_1\alpha_2+\alpha_3\alpha_6+\alpha_5\alpha_4\\ \delta_2=\alpha_1\alpha_4+\alpha_3\alpha_2+\alpha_5\alpha_6\\ \delta_3=\alpha_1\alpha_6+\alpha_3\alpha_4+\alpha_5\alpha_2\end{cases}$$

令 $A(X)=(X-\gamma_1)(X-\gamma_2)(X-\gamma_3), B(X)=(X-\delta_1)(X-\delta_2)(X-\delta_3)$。

证明, $A(X), B(X)\in\mathbb{Q}[X]$。注意, 不能使用本题后面的结论。

证明：以 $A(X)$ 为例, $B(X)$ 的证明类似. 首先注意到在置换 $(\alpha_1,\alpha_3,\alpha_5)$ 和 $(\alpha_2,\alpha_4,\alpha_6)$ 下, $A(X)$ 不变. 另外, 可以将 $\{\gamma_1,\gamma_2,\gamma_3\}$ 表示为

$$\begin{cases}\gamma_1=\alpha_1\alpha_2+T(\alpha_1)T(\alpha_2)+T^2(\alpha_1)T^2(\alpha_2),\\ \gamma_2=\alpha_1T(\alpha_2)+T(\alpha_1)T^2(\alpha_2)+T^2(\alpha_1)\alpha_2,\\ \gamma_3=\alpha_1T^2(\alpha_2)+T(\alpha_1)\alpha_2+T^2(\alpha_1)T(\alpha_2).\end{cases}$$

由第 10 小问的证明过程可知, $\sigma\in G$ 的作用完全由 $\sigma(\alpha_1)$ 和 $\sigma(\alpha_2)$ 决定. 于是, $\forall\sigma\in G$, 有

$$\begin{aligned}\sigma(\gamma_1)&=\sigma(\alpha_1)\sigma(\alpha_2)+T(\sigma(\alpha_1))T(\sigma(\alpha_2))+T^2(\sigma(\alpha_1))T^2(\sigma(\alpha_2)),\\ \sigma(\gamma_2)&=\sigma(\alpha_1)T(\sigma(\alpha_2))+T(\sigma(\alpha_1))T^2(\sigma(\alpha_2))+T^2(\sigma(\alpha_1))\sigma(\alpha_2),\\ \sigma(\gamma_3)&=\sigma(\alpha_1)T^2(\sigma(\alpha_2))+T(\sigma(\alpha_1))\sigma(\alpha_2)+T^2(\sigma(\alpha_1))T(\sigma(\alpha_2)).\end{aligned}$$

可以设 $\sigma(\alpha_1)=\alpha_i,\sigma(\alpha_2)=\alpha_j$, 其中 $\alpha_j\notin\{\alpha_i,T(\alpha_i),T^2(\alpha_i)\}$. 那么由于 $\{\alpha_1,\alpha_3,\alpha_5\}$ 和 $\{\alpha_2,\alpha_4,\alpha_6\}$ 的对称性, 只需考虑 $i=1,j=2$ 和 $i=2,j=1$ 两种情况. 计算可得

- 如果 $i=1,j=2$, 那么 $\sigma(\gamma_1)=\gamma_1,\sigma(\gamma_2)=\gamma_2,\sigma(\gamma_3)=\gamma_3$.
- 如果 $i=2,j=1$, 那么 $\sigma(\gamma_1)=\gamma_1,\sigma(\gamma_2)=\gamma_3,\sigma(\gamma_3)=\gamma_2$.

于是, σ 作用在 $A(X)=(X-\gamma_1)(X-\gamma_2)(X-\gamma_3)$ 上时不变. 也即, $A^\sigma(X)=A(X)$. 由于 $\sigma\in G$ 是任意的, 由 Galois 对应定理, $A(X)$ 的系数都在 $L^G=\mathbb{Q}$ 中, 所以 $A(X)\in\mathbb{Q}[X]$. □

利用 Mathematica 软件可以算得（正确的结果）

$$A(X)=X^3-3X^2-6X-28,\quad B(X)=X^3-3X^2-6X-1.$$

17. 证明, $\mathrm{Disc}(A)=-2^2\cdot3^6\cdot11$ 而 $\mathrm{Disc}(B)=3^6$。我们可以利用如下公式：对于多项式 X^3+aX+b, $\mathrm{Disc}\left(X^3+aX+b\right)=-4a^3-27b^2$.

证明：注意到判别式在平移下不变, 于是

$$\begin{aligned}A(X+1)&=X^3-9X-36,\\ B(X+1)&=X^3-9X-9.\end{aligned}$$

由判别式公式可知

$$\begin{aligned}\mathrm{Disc}(A) &= -4(-9)^3 - 27(-36)^2 = -2^2 \cdot 3^6 \cdot 11,\\ \mathrm{Disc}(B) &= -4(-9)^3 - 27(-9)^2 = 3^6.\end{aligned}$$

□

18. 证明, $G \simeq C_T$。

证明：我们可以较为轻松地判断 A 和 B 都是 $\mathbb{Q}[X]$ 中的不可约多项式. 于是我们可以考虑域扩张 $\mathbb{Q}(\gamma_1)/\mathbb{Q}$ 和 $\mathbb{Q}(\delta_1)/\mathbb{Q}$ 的 Galois 群 G_A 和 G_B.

回忆 12.23 课上例子 (也可参考期末复习题 14), 对于 3 次多项式 $A(B)$ 有

$$\mathrm{Gal}(\mathbb{Q}(\gamma_1)/\mathbb{Q}(\mathbb{Q}(\delta_1)/\mathbb{Q})) < \mathfrak{A}_3 \Leftrightarrow \mathrm{Disc}(A(B)) \in \mathbb{Q}^2.$$

那么由第 17 小问可知, $\mathrm{Disc}(A) \notin \mathbb{Q}^2$ 而 $\mathrm{Disc}(B) \in \mathbb{Q}^2$. 于是, $G_A \neq G_B$, 那么结合第 14 题中的推理知 $|G| \neq 6$. 于是, 由第 11 小问可知, $|G| = 18$. 由于 $G < C_T$ 且 $|C_T| = 18$, 所以 $G \simeq C_T$. □