抽代期末辅导

水至月生

2025 年 12 月 29 日

1 如何复习

抽代期末考试题的构筑是 60 分复习题 +60 分 Galois 群计算，前者做复习题就好，后者的题型类似于第八次作业。具体的细节见我的抽代资料云盘中“课堂内容概要”文件。

对于后者，首先要掌握基础的理论，其次要把第八次作业搞明白了，最后要听天由命，我们本次小班辅导便着重解决这两个问题。

2 你需要掌握的理论

首先，你不必掌握讲义上的全部内容;

其次，你不必掌握大定理的证明;

最后，即使是课上讲的内容你也不一定需要全部掌握。

你需要掌握的内容是课堂内容的真子集，课堂内容是讲义内容的真子集。

课堂内容可见我的云盘文件。

2.1 讲义复习范围

5.1 代数扩张

只需去掌握这一节的符号的基础含义以及定义，其它内容不会被考查

5.2 代数闭包

了解代数封闭域，代数闭包的定义.

5.3 环的整扩张

整体跳过

5.4 分裂域和正规扩张

分裂域，正规扩张的定义以及基础性质，正规闭包可以不看；

注意可分的定义和判断方法（不过也可以不看），而完美域，不可分，可分次数不需要看，单扩张可以看一眼本原元素对应定理。

5.5Galois 理论

Galois 扩张的定义，Galois 对应定理的内容，注意判别式的含义。

5.6.2Galois 群在根上的作用一小节可以全部看一下。

5.6.3 正规基,5.6.4 有限域，5.6.5 分圆扩张，5.6.7Kummer 理论可以通通跳过，有余力可以看眼 4，5，6 的大结论

5.7 可解群

跳过

5.8Galois 的经典应用

虽然我认为这是 Galois 理论最美妙的部分，但是考试，所以你可以跳过，并且你不会受到任何处分！

5.9 mod p 理论

只需要关注 Dedekind 理论

第五章之外

如果你群忘的差不多了，那么建议去复习一个 Sylow 子群和正规子群的基础内容。

另外要掌握一些多项式的基础理论，判断重根（导数），不可约等

以及对称多项式的一些计算

2.2 具体知识点

代数元: 设 L/K 是域扩张，$\alpha \in L$。若存在非零多项式 $f(x) \in K[x]$ 使得 $f(\alpha) = 0$，则称 α 是 K 上的**代数元**；否则称 α 是 K 上的**超越元**。

极小多项式: 设 L/K 是域扩张，$\alpha \in L$ 是 K 上的代数元。所有满足 $f(\alpha) = 0$ 的非零多项式 $f(x) \in K[x]$ 中，次数最低的首一多项式称为 α 在 K 上的**极小多项式**，记为 $\min_{K,\alpha}(x)$。

代数扩张: 设 L/K 是域扩张。若 L 中每个元素都是 K 上的代数元，则称 L/K 是**代数扩张**；否则称 L/K 是**超越扩张**。

有限扩张与扩张次数: 设 L/K 是域扩张。若 L 作为 K-线性空间的维数有限，记为 $[L : K] = \dim_K L$，则称 L/K 是**有限扩张**，$[L : K]$ 称为扩张的**次数**；否则称 L/K 是**无限扩张**。

分裂域:

设 K 是域，$f(x) \in K[x]$ 是次数 ≥ 1 的多项式。若存在域扩张 L/K 满足：

1. $f(x)$ 在 $L[x]$ 中可分解为一次因式的乘积：$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ $(c \in K^\times,\ \alpha_i \in L)$；

2. $L = K(\alpha_1, \alpha_2, \cdots, \alpha_n)$（$L$ 由 $f(x)$ 的根生成），

则称 L 是 $f(x)$ 在 K 上的**分裂域**。

正规扩张: 设 L/K 是代数扩张。若每个不可约多项式 $f(x) \in K[x]$ 若在 L 中有根，则必在 $L[x]$ 中分裂为一次因式的乘积，则称 L/K 是**正规扩张**。

正规扩张的基础性质:

1. 有限扩张 L/K 是正规扩张 $\iff$ L 是某个多项式 $f(x) \in K[x]$ 在 K 上的分裂域；

2. 正规扩张的交仍为正规扩张；正规扩张在中间域上的限制未必正规。

可分元与可分扩张: 设 L/K 是域扩张，$\alpha \in L$ 是 K 上的代数元，$\min_{K,\alpha}(x)$ 是其极小多项式。若 $\min_{K,\alpha}(x)$ 在其分裂域中无重根，则称 α 是 K 上的**可分元**；若 L/K 中每个元素都是 K 上的可分元，则称 L/K 是**可分扩张**。

可分性判断方法:

1. 不可约多项式 $f(x) \in K[x]$ 无重根 $\iff$ $f'(x) \neq 0$（形式导数不为零）；

2. 特征为 0 的域上的代数扩张都是可分扩张。

本原元素定理: 设 L/K 是有限可分扩张，则存在 $\alpha \in L$ 使得 $L = K(\alpha)$，称 α 是 L/K 的**本原元素**。

Galois 扩张: 设 L/K 是有限代数扩张。若 L/K 既是可分扩张又是正规扩张，则称 L/K 是 **Galois 扩张**。

Galois 群: 设 L/K 是 Galois 扩张，记 $\mathrm{Gal}(L/K) = \{\sigma : L \to L \mid \sigma \text{ 是域同构且} \sigma|_K = \mathrm{id}_K\}$，称为 L/K 的 **Galois 群**（运算为同构的复合）。

Galois 对应定理: 设 L/K 是有限 Galois 扩张，定义中间域的集合和子群的集合：

$$\mathcal{M} = \{K \subset M \subset L \mid M \text{ 是中间域}\}, \quad \mathcal{S} = \{H < \mathrm{Gal}(L/K) \mid H \text{ 是子群}\},$$

并用包含关系作为 $\mathcal{M}$ 和 $\mathcal{S}$ 上的偏序。那么，我们有如下的反转偏序关系

的 **Galois 对应**（以下映射互为逆）：

$$\mathcal{M} \xrightarrow{1:1} \mathcal{S}, \quad M \mapsto \mathrm{Gal}(L/M), \quad L^H \mapsto H.$$

进一步，扩张 M/K 是正规扩张当且仅当 $\mathrm{Gal}(L/M) \triangleleft \mathrm{Gal}(L/K)$ 是正规子群，并且在此情形下，我们有

$$\mathrm{Gal}(M/K) = \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M).$$

Galois 群在根上的作用： 设 K 是域，$P \in K[X]$ 为可分的多项式，L 是 P 的分裂域。那么，$\mathrm{Gal}(L/K)$ 在根的集合 $Z_P(L)$ 上的作用是忠实的：

$$1 \to \mathrm{Gal}(L/K) \to \mathfrak{S}_{Z_P(L)}.$$

这个作用是传递的当且仅当 P 是不可约多项式。

2.3 讲义之外

1. 可约的判断：

(1). 艾森斯坦判别法：

设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 是一个整系数多项式。如果存在一个素数 p，使得以下三个条件同时成立：

1. 首项系数 a_n 不被 p 整除，即 $p \nmid a_n$；
2. 其余所有系数 $a_{n-1}, a_{n-2}, \ldots, a_0$ 都被 p 整除，即 $p \mid a_i$ 对所有 $0 \le i \le n-1$ 成立；
3. 常数项 a_0 不被 p^2 整除，即 $p^2 \nmid a_0$。

那么多项式 $f(x)$ 在有理数域 $\mathbb{Q}$ 上是不可约的。

(2) 转化到有限域：若在有限域上不可约，则在 $\mathbb{Q}$ 上也不可约

(3) 线性组合反证：例如对于 $x^2 - \alpha$ 在 $\mathbb{Q}(\alpha)$ 上是否可约，可设其可约，之后将其一个根设为 $\{1, \alpha, \alpha^2, \cdots\}$ 的线性组合，之后代入到处矛盾

2. 判别式的性质：

可以去参考复习题

3. 对称多项式：

主要是通过韦达定理得到根的关系，之后用其计算一些对称多项式，或者相对比较对称的多项式

3 例题

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。

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

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 $[K(\beta_1) : K]$。

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 $G = \mathrm{Gal}(L/\mathbb{Q})$。

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

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：

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

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：

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

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。

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

3. 证明，在 $\mathbb{F}_2[X]$ 中，$X^2 + X + 1 \nmid X^8 + X + 1$。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。

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

6. 令 $R=\{x\in\overline{\mathbb{Q}}\mid P(x)=0\}$ 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，R 可以如下描述：

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

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

$$T:\mathcal{R}\to\mathcal{R}$$

8. 证明，$|R|=6$ 并且可以将 R 中的元素记作：

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

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 $\alpha_i\in R$ 对应着指标 i），那么 T 可以被视作是 $(1,3,5)(2,4,6)\in\mathfrak{S}_6$。

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：

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

其中 $\{\pm1\}$ 是 2 阶循环群。

10. 证明，$|C_T|=18$。

11. 我们可以将 $G:=\mathrm{Gal}(L/\mathbb{Q})$ 视作是 $\mathfrak{S}_{\mathcal{R}}=\mathfrak{S}_6$ 的子群。证明，$G<C_T$，$\varepsilon|_G:G\to\{\pm1\}$ 也是满射并且 $|G|=6$ 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。

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

14. 令 $H := (\varepsilon|_G : G \to \{\pm 1\})$，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 $\mathbb{Q}(\sqrt{d})$。

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。

16. 令

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

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。

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，$\mathrm{Disc}(A) = -2^2 \cdot 3^6 \cdot 11$ 而 $\mathrm{Disc}(B) = 3^6$。我们可以利用如下公式：对于多项式 $X^3 + aX + b$，$\mathrm{Disc}(X^3 + aX + b) = -4a^3 - 27b^2$。

18. 证明，$G \cong C_T$。