第十五次习题课

方法提要、小测讲解、习题讲解和内容扩充

助教：邓先涛

2023 年 12 月 25 日

重点知识提要

重点知识提要

- Galois 理论：特征 0 域上的多项式 f 可根式解等价于 f 的 Galois 群可解.
- 一般的五次多项式不可根式解：了解一般五次多项式不可根式的证明思路；能够计算一些五次多项式的 Galois 群.

小测讲解

小测第 1 题

构造 25 元有限域 $\mathbb{F}_{25}$，指出所有本原元.

极大理想的性质

注

$\mathbb{F}_{25}$ 确实是 $x^{25}-x$ 在 $\mathbb{F}_5$ 上的分裂域，但是不能写作 $\mathbb{F}_5[x]/(x^{25}-x)$.

思维拓展

找出 $\mathbb{F}_{25}^{\times}$ 的全部生成元.

证明

- 构造 25 元有限域等价于找 $\mathbb{F}_5[x]$ 中的次数为 2 的不可约多项式生成的极大理想.
- 注意到 x^2+2 在 $\mathbb{F}_5$ 上没有根，因此不可约.
- $\mathbb{F}_{25}=\mathbb{F}_5[x]/(x^2+2)=\{a+b\overline{x}|a,b\in\mathbb{F}_5\}$.
- 本原元：$\alpha\in\mathbb{F}_{25}$ 使得 $\mathbb{F}_{25}=\mathbb{F}_5(\alpha)$.
- 素数阶扩张任意 $\alpha\in\mathbb{F}_{25}-\mathbb{F}_5$ 均是本原元.
- 原根/生成元：$\alpha\in\mathbb{F}_{25}$ 使得 $\mathbb{F}_{25}^{\times}=<\alpha>$.

小测第 2 题

设 $F=\mathbb{Q}\left(\sqrt[3]{2},\sqrt{-1}\right)$，对 $F/\mathbb{Q}$ 的每一个中间域 M，找一个 $\beta\in F$ 使得 $M=\mathbb{Q}(\beta)$，指出在 $\mathbb{Q}$ 上为正规扩张的所有非平凡中间域.

域扩张中的元素分析

思维拓展

任给素数 p 和正整数 n，找出 $F=\mathbb{Q}\left(\sqrt[p]{2},\zeta_{2^n}\right)$ 的所有中间域.

证明

- $[F:\mathbb{Q}]=6$，$F/\mathbb{Q}$ 只有 2 次和 3 次子域 M.
- 若 $[M:\mathbb{Q}]=3$，则 $M\cap\mathbb{Q}\left(\sqrt[3]{2}\right)$ 为 $\mathbb{Q}$ 或 M.
- 若是 $\mathbb{Q}$，则 x^3-2 在 M 上可约，等价于有根，这与 $M\subset F$ 矛盾.
- 若是 M，则 $M=\mathbb{Q}\left(\sqrt[3]{2}\right)$，不是正规扩张.
- 若 $[M:\mathbb{Q}]=2$，则 $\sqrt{-1}\in M$，否则 $[M(\sqrt{-1}):\mathbb{Q}]=4$ 与 $M\subset F$ 矛盾.
- 此时 $M=\mathbb{Q}(\sqrt{-1})$，是正规扩张.

小测第 3 题

设 $\alpha=\sqrt{2+\sqrt{2}}$，$\beta=\sqrt{2-\sqrt{2}}$，$m(x)$ 为 α 在 $\mathbb{Q}$ 上的极小多项式，证明 $\mathbb{Q}(\alpha)$ 为 $m(x)$ 在 $\mathbb{Q}$ 上的分裂域，求 $m(x)$ 在 $\mathbb{Q}$ 上的 Galois 群.

单扩张的 Galois 群的计算

思维拓展

试用四次方程 Galois 群的判定方法证明该结论.

证明

- α 的零化多项式为 x^4-4x^2+2 在 $\mathbb{Q}$ 上不可约，因此 $m(x)=x^4-4x^2+2$.
- 可验证 $\pm\alpha$ 和 $\pm\beta$ 是 $m(x)$ 的全部不同根.
- $\beta=\frac{\alpha^2-2}{\alpha}\in\mathbb{Q}(\alpha)$，因此 $\mathbb{Q}(\alpha)$ 包含了 $m(x)$ 全部根，为 $m(x)$ 的分裂域.
- $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ 中的元素由 α 的像完全决定，因此是一个四阶群.
- $\sigma(\alpha)=\beta$，则 $\sigma^2(\alpha)=-\alpha$，因此 σ 为四阶元，这意味着 $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ 是四阶循环群.

第八章习题

第八章第 37 题

设 E/F 为素数 p 次循环扩张，L/F 为任一域扩张．证明：复合域 EL 或者是 L 上的 p 次循环扩张或者 $EL = L$.

正规扩张的性质

思维拓展

举例说明题中循环扩张的条件是必要的.

证明

- 素数次扩张总是可以令 $E = F(\alpha)$，α 在 F 上的极小多项式为 $m(x)$.
- 若 $\alpha \in L$，则 $EL = L$.
- 若 $\alpha \notin L$，则令 $h(x)$ 为 α 在 L 上的极小多项式，有 $h(x) \mid m(x)$.
- $m(x)$ 在 E 中完全分解，因此 $h(x)$ 的系数属于 E.
- 若 $h(x) \neq m(x)$，则存在 $h(x)$ 的系数 $a \in (E - F) \cap L$，因此 $E = F(a) \subset L$ 矛盾.

Galois 群计算实例

补充题

证明：$f(x)=x^5-20x+16$ 在 $\mathbb{Q}$ 上的群为 S_5.

S_p 的基本性质

证明

- 注意到 $x^5-20x+16$ 有三个实根和一对复根.
- $\sigma: a+bi\to a-bi$ 是 $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ 中的二阶元素，可以看作 S_5 中的元素 (12).
- $f(x-1)$ 在 $\mathbb{Q}$ 上不可约，因此 $f(x)$ 不可约推出 $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ 有 5 阶子群，即 5 阶元.
- 5 阶元表明 $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ 有元素可以看作大群 S_5 中的 (12345).
- 因此 $S_5=<(12),(12345)>\subset \mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})\subset S_5$ 推得命题成立.

第八章第 39 题

证明：$f(x)=x^5+20x+16$ 在 $\mathbb{Q}$ 上的群为 A_5

教材 258 页定理 5：G_f 只含有偶置换的充要条件是 $D(f)$ 在 $\mathbb{Q}$ 内可开方.

证明第一步：$G_f\subset A_5$

- 设 x_i 为 $F(x)=x^5+ax+b$ 的根，$D(F)=\prod_{1\le i<j\le 5}(x_i-x_j)^2$ 是关于 x_i 的 20 次齐次对称多项式.
- 令 $\sigma_k=\sum_{1\le i_1<\cdots<i_k\le 5} x_{i_1}\cdots x_{i_k}$ 为初等对称多项式. 则 $\sigma_1=\sigma_2=\sigma_3=0$，$\sigma_4=a$，$\sigma_5=-b$.
- $D(F)$ 可以表为初等对称多项式的多元函数，因此写作 $D(f)=k_1\sigma_4^5+k_2\sigma_5^4$，其中 k_1 和 k_2 的值与 a 和 b 的选择无关.
- 取 $a=-1$ 和 $b=0$，有 $D(F)=-256=-k_1$，因此 $k_1=4^4$.
- 取 $a=-5$ 和 $b=4$，则 F 有重根，有 $D(F)=0=-k_1\cdot 5^5+k_2 4^4$，因此 $k_2=5^5$.
- $D(f)=4^4\cdot 20^5+5^5\cdot 16^4=4^8 5^6$ 可在 $\mathbb{Q}$ 中开方，推出 $G_f\subset A_5$.

第八章第 39 题

证明：$f(x)=x^5+20x+16$ 在 $\mathbb{Q}$ 上的群为 A_5

多项式模 p 法 (294 页定理 20)：设 p 是与 $D(f)$ 互素的素数，则 $f(x)$ 在 $\mathbb{F}_p$ 上的群是 G_f 的子群.

证明第二步：$|G_f|\geq 15$

- 前一问结论为 $D(f)=2^{16}\cdot 5^6$.
- 现令 $p=3$，验证 $f(x)$ 在 $\mathbb{F}_p$ 上不可约，因此 $f(x)$ 在 $\mathbb{F}_3$ 上的群为 5 阶循环群.
- 令 $p=7$，$f(x)\equiv(x+3)(x+2)(x^3+2x+5x+5) \bmod 7$，故 $f(x)$ 在 $\mathbb{F}_7$ 上的群为 3 阶循环群.
- 因此 G_f 中至少有一个 3 阶循环子群与 5 阶循环子群的半直积，元素个数大于等于 15.

第八章第 39 题

证明：$f(x) = x^5 + 20x + 16$ 在 $\mathbb{Q}$ 上的群为 A_5

群在集合上的作用：

证明第三步：$|G_f| = A_5$

- 前两问的结论为：$D(f) = 2^{16} \cdot 5^6$ 和 $[A_5 : G_f] \leq 4$.
- 设 $g_1, \cdots, g_s (s \leq 4, g_1 = 1)$ 为 A_5 关于 G_f 的陪集分解.
- 定义 A_5 在 $\{g_1, \cdots, g_s\}$ 上的作用，$gg_i = g_j \iff gg_iG_f = g_jG_f$，有同态 $\psi : A_5 \to S_4$.
- $\ker(\psi)$ 为 A_5 的正规子群，因此 $\ker(\psi)$ 要么是 $\{1\}$ 要么是 A_5.
- 前者与两群的阶数相矛盾；后者表明 $G_f = A_5$，因此结论成立.

总结

任给正整数 n 和 $m < n$，A_n 中不存在指数为 m 的子群.

补充题

证明 $f(x) = x^5 - x - 1$ 在 $\mathbb{Q}$ 上的 Galois 群是 S_5.

多项式模 p 法：设 p 是与 $D(f)$ 互素的素数，则 $f(x)$ 在 $\mathbb{F}_p$ 上的群是 G_f 的子群.

证明

- 计算多项式的判别式 $D(f) = 5^5 - 4^4 = 2869$，因此模 p 法可以取 $p = 2, 3, 5$.
- $p = 2$，验证 $f(x) \equiv (x^2 + x + 1)(x^3 + x^2 + 1) \bmod 2$，因此 G_f 有一个 6 阶循环子群.
- $p = 3$，验证 $f(x)$ 在 $\mathbb{F}_3[x]$ 中不可约，因此 G_f 有一个 5 阶循环子群.
- 注意到 S_5 中的元素可以写作不相交的轮换乘积，6 阶元总是形如 $(12)(345)$.
- 因此 $[(12)(345)]^3 = (12) \in G_f$，且 $(12345) \in G_f$，推出 $G_f = S_5$.

补充题

任给素数 $p \geq 3$，构造一个在 $\mathbb{Q}$ 上 Galois 群为 S_p 的 p 次不可约多项式 $f(x) \in \mathbb{Z}[x]$.

多项式模 p 法：设 p 是与 $D(f)$ 互素的素数，则 $f(x)$ 在 $\mathbb{F}_p$ 上的群是 G_f 的子群.

证明

- 令 $f_1(x)$ 为 $\mathbb{F}_2[x]$ 中的 p 次不可约多项式.
- 令 $f_2(x)$ 是 $\mathbb{F}_p[x]$ 中次数为 2 的不可约多项式.
- 令 $f(x) = pf_2(x) + 2(x-1)\cdots(x-(p-2))f_2(x)$，则 $f(x)$ 在 $\mathbb{F}_2$ 和 $\mathbb{F}_p$ 上无重根，在 $\mathbb{Q}$ 上不可约.
- $f(x)$ 在 $\mathbb{Q}$ 上的群中有一个 p 阶元和一个 2 阶元，因此 $G_f = S_p$.

思维拓展

任给正整数 n，构造在 $\mathbb{Q}$ 上的群为 S_n 的 n 次不可约多项式 $f(x) \in \mathbb{Z}[x]$(见教材 295 页定理 21).

本学期抽象代数习题课到此结束

感谢各位同学对我助教工作的积极配合

祝各位同学期末取得满意成绩

该系列课件适合做完习题的同学查阅核对，对将要学习抽象代数的同学无益，请勿传至学弟学妹.