第十四次习题课

方法提要、习题讲解和内容扩充

助教：邓先涛

2023 年 12 月 18 日

重点知识提要

重点知识提要

- Sylow 定理的应用：了解 Sylow 三定理；能够应用 Sylow 三定理分类一些简单的群.
- 可解群的性质与判定：了解可解群的基本概念；了解可解群的判断方法；了解常见的单群.
- Galois 基本定理的应用：了解 Galois 基本定理的内容；能够应用基本定理给出域扩张的中间域.
- 域的根式扩张：了解根式扩张的基本来源与定义；了解根式扩张与多项式可根式解的关系.

Sylow 定理的应用

Sylow 定理的基本事实

- Sylow 第一定理(Sylow p 子群的存在性)：设 G 是一个有限群，p 为素数，若 $p^k \mid |G| (k \geq 0)$，则群 G 中一定存在 p^k 阶子群.
- Sylow 第二定理：有限群的 Sylow p 子群相互共轭，它的 p 子群一定包含在它的某个 Sylow p 子群. 特别的，有限群的 Sylow p 子群的个数是该有限群的阶数的因子.
- Sylow 第三定理：设 G 是有限群，p 是 $|G|$ 的一个素因子，k 为 G 的全部 Sylow p 子群的个数，则 $k \equiv 1 \mod p$.

第二章第 25 题

设 p 和 q 是不同素数，证明 p^2q 阶群必包含一个正规 Sylow 子群.

Sylow 第二定理和Sylow 第三定理

思维拓展

若素数 p 和 q 满足 $p \nmid q-1$ 和 $q \nmid p^2-1$，则 p^2q 阶群必为交换群.

证明

- 设 Sylow p 子群和 Sylow q 子群的个数分别是 k_p 和 k_q，则 $k_p \mid q$.
- 若 $k_p = 1$ 或 $k_q = 1$，则必存在正规子群.
- 若 $k_p = q$，有 $q \equiv 1 \bmod p$，分以下情况.
- 若 $k_q = p$，则 $p \equiv 1 \bmod q$ 与 $q \equiv 1 \bmod p$ 矛盾.
- 若 $k_q = p^2$，则 $q \mid (p-1)(p+1)$，由上立刻推出 $q \mid p+1$，因此 $p = 2, q = 3$.
- 此时 G 中有 8 个三阶元，于是最多只有一个 4 阶子群，与 $k_p = 3$ 矛盾.

第五章第 20 题

设 p 为素数，则 p^2 阶群 G 必交换.

Sylow 定理的证明技巧：群在有限集合上的作用

思维拓展

任给素数 p，造一个 p^3 阶的非交换群.

证明

- G 在 G 上的共轭作用 $\sigma_g(x) = gxg^{-1}$.
- $H_x = \{g \in G | \sigma_g(x) = x\}$ 为 $x \in G$ 的稳定子群. $O_x = \{y | y = gxg^{-1}, g \in G\}$ 为 x 的轨道.
- 则 $|O_x| = |G/H_x|$，这是因为任给 $y \in O_x$，集合 $\{g | y = gxg^{-1}\}$ 恰是 G 关于 H_x 的一个左陪集类.
- 因此 $|G| = \sum_{x \in G} |O_x|$，$|O_x| = 1$ 的 x 的个数不是 1. 即 G 的中心非平凡.
- 存在 G 的一个循环子群 H 为 G 关于 $Z[G]$ 的陪集代表元全体，因此 G 可交换.

可解群的结构与判定

可解群的基本事实

- 可解群的定义：群 G 称为可解的，若存在有限群链 $\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G$ 使得 G_{i-1} 是 G_i 的正规子群，且 G_i/G_{i-1} 是交换群.
- 可解群的性质：可解群的子群和商群可解.
- 可解群的判定：若有限群 G 中存在正规子群 H 使得 G/H 和 H 均可解，则 G 可解.
- S_n 的可解性：S_n 是可解群当且仅当 $n = 1, 2, 3, 4$.

第二章第 43 题

设 p 和 q 是不同素数，证明 p^2q 阶群 G 必可解.

可解群的判定和Sylow 定理

思维拓展

对任意正整数 n 和素数 p，利用数学归纳法可证明 p^n 阶群均可解.

证明

- 取 H 为 G 的正规 Sylow 子群，则 $|G/H| = q$ 或 p^2.
- 若 $|G/H| = q$，则 G/H 是循环群，且 $|H| = p^2$ 是交换群，因此可解.
- 若 $|G/H| = p^2$，则 G/H 是交换群，且 $|H| = q$ 是循环群，因此可解.

第二章第 45 题

设 H 和 K 是有限群 G 的正规子群，若 G/H 和 G/K 均可解，证明：$G/(H\cap K)$ 可解.

可解群的性质：可解群的子群和商群均可解

思维拓展

找出最小的 n 使得存在 n 阶非交换群. 找出最小的 n 使得存在 n 阶单群.

证明

- 群同态定理表明 $K/(K\cap H)\cong KH/H$，而 KH/H 作为 G/H 的子群是可解的.
- $K/(K\cap H)$ 是 $G/(K\cap H)$ 的正规子群.
- $[G/(K\cap H)]\,/\,[K/(K\cap H)]\cong G/K$，因此商群可解.
- 正规子群和对应的商群可解，因此 $G/(K\cap H)$ 可解.

Galois 基本定理的应用

第八章第 23 题

设 p 为奇素数，则任给正整数 n，$\mathbb{Z}/p^n\mathbb{Z}$ 的单位群 $(\mathbb{Z}/p^n\mathbb{Z})^\times$ 是一个循环群.

$\mathbb{F}_p$ 的性质和简单的数论

总结

$\mathrm{Gal}\,(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ 是一个 $(p-1)p^{n-1}$ 阶的循环群.

证明

- 事实：$\mathbb{F}_p^\times$ 是循环群，记为 $< g_1 >$.
- $m = n-1$ 是使得 $(1+p)^{p^m} \equiv 1 \bmod p^n$ 成立的最小非负整数.
- 令 $g \equiv g_1^{p^{n-1}} \bmod p^n$，则 $g^{p-1} \equiv 1 \bmod p^n$.
- 由于任给 $1 \le m < p-1$，有 $g_1^m \not\equiv 1 \bmod p$，因此 g 是模 p^n 的 $p-1$ 阶元.
- $t = (1+p)g$ 为 $(p-1)p^{n-1}$ 阶元，因此是循环群.

第八章第 24 题

任给正整数 $n > 2$，$\mathbb{Z}/2^n\mathbb{Z}$ 的单位群 $(\mathbb{Z}/2^n\mathbb{Z})^\times$ 是一个 2^{n-2} 阶循环群和 2 阶循环群的直积.

简单的数论

总结

$\mathrm{Gal}\left(\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}\right)(n > 2)$ 是一个 2^{n-2} 阶循环群和 2 阶循环群的直积.

证明

- 5 是模 $2^n (n > 2)$ 的一个 2^{n-2} 阶元.
- 根据有限交换群的结构定理，$(\mathbb{Z}/2^n\mathbb{Z})^\times$ 只有两种结构：循环群或者一个 2^{n-2} 阶循环群和 2 阶循环群的直积.
- $2^{n-1}+1$，$2^{n-1}-1$ 和 -1 均是模 2^n 的二阶元.
- $(\mathbb{Z}/2^n\mathbb{Z})^\times$ 不是循环群，因此结论成立.

补充题

设 G 是一个 2^n 阶交换群，试决定 G 的指数为 2 的子群个数.

有限交换群的结构定理

总结

2^n 阶交换群 G 至多有 2^n-1 个指数为 2 的子群，取等当且仅当G 为 n 个 2 阶循环群的直和.

思维拓展

对于非交换群，指数为 p 的子群的计数问题如何解决？

证明

- 设 $G \cong G_1 \oplus G_2 \oplus \cdots \oplus G_r$ 为有限交换群的标准分解.
- G 的每一个指数为 2 的子群 H 对应一个非平凡群同态 $\phi_H : G \to C_2$.
- $G \to C_2$ 的群同态由 G_i 的生成元的像唯一决定，因此总有 2^r-1 个非平凡的群同态.
- G 的指数为 2 的子群个数由直和项数 r 所决定，为 2^r-1 个.

第八章第 25 题

设 p 为奇素数，令 $p^* = (-1)^{\frac{p-1}{2}} p$，证明：若 n 为正整数，则分圆域 $\mathbb{Q}(\zeta_{p^n})$ 包含唯一的二次子域 $\mathbb{Q}(\sqrt{p^*})$.

Galois 基本定理和Gauss 和

证明

- 设 p 为素数，$\left(\frac{a}{p}\right)$ 为二次剩余符号.
- $\left(\sum_{d=1}^{p-1}\left(\frac{d}{p}\right)\zeta_p^d\right)^2 = \sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(\frac{ab}{p}\right)\zeta_p^{a+b}$ $= \sum_{a=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{c}{p}\right)\zeta_p^{a(1+c)} = p^*$
- 因此 $\sqrt{p^*} \in \mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^n})$.
- 注意到 $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ 是一个循环群，因此只有唯一的指数为 2 的子群，对应唯一的二次子域.

第八章第 26 题

若 $n \geq 3$ 为正整数，则 $\mathbb{Q}(\zeta_{2^n})$ 恰好包含三个二次子域 $\mathbb{Q}(\sqrt{2})$，$\mathbb{Q}(\sqrt{-2})$ 和 $\mathbb{Q}(\sqrt{-1})$.

Galois 基本定理

思维拓展

设 $n = 2^e \cdot p_1^{e_1} \cdots p_k^{e_k}$，试计算分析 $\mathbb{Q}(\zeta_n)$ 中的二次子域的个数.

证明

- 注意到 $\zeta_4 = \pm\sqrt{-1}$，因此 $\mathbb{Q}(\sqrt{-1}) \in \mathbb{Q}(\zeta_4) \subset \mathbb{Q}(\zeta_{2^n})$.
- ζ_8 的极小多项式为
$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1).$$
- 因此 $\zeta_8 + \zeta_8^{-1} = \pm\sqrt{2} \in \mathbb{Q}(\zeta_8)$.
- $\sqrt{-1}, \sqrt{2}, \sqrt{-2} \in \mathbb{Q}(\zeta_{2^n})$.
- $\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}$ 的群为 $C_{2^{n-2}} \oplus C_2$，因此有且仅有 3 个指数为 2 的子群，故恰有三个二次子域.

第八章第 5 题

设 $p_1, \cdots, p_r$ 是 r 个不同的有理素数，决定 $\mathrm{Gal}(K/\mathbb{Q})$，其中 $K = \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_k})$.

Galois 基本定理和指数为 2 的子群的计数

思维拓展

试着抛开 Galois 理论直接证明该问题.

证明

- $[K : \mathbb{Q}] \mid 2^r$，且 $K/\mathbb{Q}$ 为 Galois 扩张，因此 $\mathrm{Gal}(K/\mathbb{Q})$ 是一个 2 的幂次阶群.
- 设 $1 \leq i_j \leq r$，$\mathbb{Q}(\sqrt{p_{i_1} \cdots p_{i_k}})$ 为 K 的二次子域，有 $2^r - 1$ 个这样的不同的二次子域.
- $\mathrm{Gal}(K/\mathbb{Q})$ 有至少 $2^r - 1$ 个不同的指数为 2 的子群，推出 $\mathrm{Gal}(K/\mathbb{Q}) \cong \oplus_{i=1}^{r} C_2$.

根式扩张

根式扩张的基本事实

- 单根式扩张的定义：称 K/F 是一个单根式扩张，若存在 $\alpha \in K$ 满足 $\alpha^n \in F$ 使得 $K = F(\alpha)$.
- 根式扩张的定义：称 K/F 是一个根式扩张，若存在扩张链 $F = E_0 \subset E_1 \subset \cdots \subset E_n = E$ 使得 E_i/E_{i-1} 是单根式扩张.
- 多项式可根式解的刻画：多项式 $f(x)$ 可根式解当且仅当 $f(x)$ 的分裂域包含在某个根式扩张中.
- 注：彭老师讲义中所定义的单根式扩张与教材上并不等价，例子就是 $\mathbb{Q}(\zeta_7)$ 符合讲义上单根式扩张定义，但不符合教材上单根式扩张定义，进一步的甚至不符合教材上根式扩张的定义.
- 注：彭老师讲义中所定义的单根式扩张使用会更加方便，而教材上所定义的单根式扩张会更加符合根式解的原始观察. 可以证明在特征零域上根式解的判断上，两个定义最终是一致的，因为二者的本质区别在于对单位根的处理，而单位根是能够在教材定义基础上证明为可根式解的.

第八章第 28 题

举例说明存在 $\mathbb{Q}$ 上的根式扩张链 $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_r = K$ 使得 $K/\mathbb{Q}$ 的一个中间域 $L/\mathbb{Q}$ 不能写作一个根式扩张链.

可根式解的多项式的分裂域总是一个根式扩张的中间域

证明

- 取 L 为 $f(x) = x^3 - 3x + 1$ 在 $\mathbb{Q}$ 上的分裂域，$D(f) = -4(-3)^3 - 27 = 81$，因此 $[L : \mathbb{Q}] = 3$.
- L 作为三次多项式的分裂域可根式解，因此为某一个根式扩张的中间域.
- 若 L 可写成根式扩张链，只能 $\mathbb{Q} = F_0 \subset F_1 = L$，即存在 $\alpha \in L$ 使得 $L = \mathbb{Q}(\alpha)$，且 $\alpha^n \in \mathbb{Q}$.
- L 是分裂域，因此 α 的所有共轭元均在 L 中，由扩张次数可推出存在至少两个正整数 $k < n$ 使得 $\zeta_n^k \in L$，这与 $L \subset \mathbb{R}$ 矛盾.
- 注：这个现象表明在解多项式方程时需要引入不在分裂域中的元素进行表达.

第八章第 30 题

设 $f(x)$ 是 $\mathbb{Q}$ 上的 n 次不可约多项式 $(n>4)$ 使得 $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q}) \cong S_n$，$\alpha \in \mathbb{Q}(f)$ 为 $f(x)$ 的一个根，则 $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{1\}$，$[\mathbb{Q}(\alpha):\mathbb{Q}] = n$，且 E 是 $\mathbb{Q}(\alpha)$ 的正规闭包.

扩张次数的传递性

证明

- α 的极小多项式为 $f(x)$，次数为 n，推出 $[\mathbb{Q}(\alpha):\mathbb{Q}] = \deg(f(x)) = n$.
- 假设有 $1 \neq \sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$，有 $\sigma(\alpha) = \beta \in \mathbb{Q}(\alpha)$，则 $[\mathbb{Q}(f):\mathbb{Q}(\alpha)] \leq (n-2)!$.
- 扩张次数传递性表明 $|S_n| = [\mathbb{Q}(f):\mathbb{Q}] = [\mathbb{Q}(f):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] \leq n(n-2)!$ 矛盾.

思维拓展

任给正整数 n，满足 $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q}) = S_n$ 的 n 次不可约多项式总是存在吗？

有限域上多项式方程的根式解

设 q 是奇素数 p 的方幂，$\mathbb{F}_q$ 是特征 p 域，任给正整数 $n < p$，证明 $\mathbb{F}_{q^n}$ 是 $\mathbb{F}_q$ 的根式扩张的中间域. 注：该题采用教材定义

有限域的有限扩张

思维拓展

证明 $\mathbb{F}_{3^7}$ 不是 $\mathbb{F}_3$ 的根式扩张的中间域.

证明

- 任给正整数 m，$\mathbb{F}_{q^{2^m}}$ 均是 $\mathbb{F}_q$ 的根式扩张.
- 设 $p_0 = 2, p_1, \cdots, p_r$ 是小于 p 的全体素数，利用归纳法，假设任给 $0 \leq i < r$，以及正整数 $m_0, \cdots, m_i$，$\mathbb{F}_{q^{p_0^{m_0} \cdots p_i^{m_i}}}$ 是根式扩张.
- 存在 $k = p_0^{m_0} \cdots p_i^{m_i}$ 使得 $p_{i+1} \mid q^k - 1$. 令 $\mathbb{F}^{\times}_{q^{p_{i+1}k}} =< \alpha >$，则 $\alpha^{\frac{q^{p_{i+1}k}-1}{p_{i+1}(q^k-1)}p_{i+1}} \in \mathbb{F}_{q^k}$，因此 $\mathbb{F}_{q^{p_{i+1}k}}$ 是 $\mathbb{F}_{q^k}$ 的单根式扩张.
- 以此类推，根据归纳法，任给正整数 m，有 $\mathbb{F}_{q^{p_{i+1}^m k}}$ 是 $\mathbb{F}_q$ 的根式扩张.

问题补充和方法扩张

问题 1

试用 Sylow 定理分类所有阶数 $n \leq 15$ 的有限群.

简要说明

- $n = 1, 2, 3, 5, 7, 11, 13, 15$：循环群 C_n.
- $n = 4$：C_4 和 $C_2 \oplus C_2$. $n = 9$：C_9 和 $C_3 \oplus C_3$.
- $n = 6$：C_6 和 $D_3 = S_3$. $n = 10$：C_{10} 和 D_5. $n = 14$：C_{14} 和 D_4.
- $n = 8$：C_8、$C_4 \oplus C_2$、$C_2 \oplus C_2 \oplus C_2$、$D_4$ 和 Q_8.
- $n = 12$：D_6、A_6 和 $G :=< a, b | b^3 = a^4 = 1, aba^{-1} = b^2 >$

问题 2

$x^n - 1$ 在 $\mathbb{Q}$ 上的根式解如何实现？

简要说明

- 以 $n = 7$ 为例子，考察 $x^7 - 1$ 在 $\mathbb{Q}$ 上的根式解，基本方法是将阶放在扩张次数更低的域扩张中进行实现.
- $(\mathbb{Z}/7\mathbb{Z})^\times$ 有三阶子群 $\{1, 2, 4\}$，该子群固定元素 $s = \zeta_7 + \zeta_7^2 + \zeta_7^4$ 是 $\mathbb{Q}(\zeta_7)$ 的二次子域生成元.
- $s^2 = \zeta_7^3 + \zeta_7^5 + \zeta_7^6 - 1 = -s - 2$，因此 $s = \frac{-1 \pm \sqrt{-7}}{2}$.
- $\zeta_7^3 - s\zeta_7^2 - (s+1)\zeta_7 - 1 = 0$，因此只需要解方程 $x^3 - sx^2 - (s+1)x - 1 = 0$ 即可.