arXiv:2512.14547v1 [math.GR] 16 Dec 2025

与p-极大类群相关的李环

Bettina Eick、Patali Komma 和 Subhrajyoti Saha

2025年12月17日

摘要

Lazard 对应在 p-极大类群与一种由 p-进数域构造的特定类型李环之间建立了密切联系。本文旨在研究这类李环。特别地，我们证明它们总是有限的。由此可知，它们是幂零类较小的幂零李环。这些结果弥补了 (Eick、Komma 和 Saha 2025) 中一个重要的空缺。

1 引言

p-群的极大类分类是群论中一个由来已久的项目。迄今为止，这一领域已经取得了许多有趣而深刻的成果，但仍有许多未解决的问题。对于较小的素数 $p \in \{2, 3\}$，Blackburn [1]已经完成了完整分类。因此，我们在此将重点讨论 $p \geq 5$ 的情形。关于该领域的最新进展、参考文献和背景知识，请参阅 Leedham-Green & McKay [7] 的介绍。

p-群的极大类可以通过其关联的图 $\mathcal{G}(p)$来直观表示：其顶点与无穷多个 p-群极大类的同构类型一一对应，并且当 $H/Z(H) \cong G$ 成立时，两个顶点之间存在一条边 $G \to H$。已知 $\mathcal{G}(p)$由一个孤立点和一棵具有唯一无限路径的无限树 $\mathcal{T}$组成，这条路径称为其主干线。我们用 $S_2 \to S_3 \to \ldots$ 表示这条无限路径，其中 S_i 是一个阶为p^i的群。 i个分支 $\mathcal{B}_i$ 是 $\mathcal{T}$的子树，它由 S_i 的所有后代中不属于 S_{i+1}的后代组成；它是一棵有限树。图 $\mathcal{G}(p)$ 由其孤立点、主干线以及依次排列的分支 $\mathcal{B}_2$、$\mathcal{B}_3$、.....组成。理解这些分支是 p-群极大类分类中的主要问题。

设 G 是 $i \geq p-1$ 的一个分支 $\mathcal{B}_i$ 中的群，并令 $P(G)$ 为其二步中心化子；也就是说，它是 G 中下中心列商 $\gamma_2(G)/\gamma_4(G)$ 的中心化子。于是， $P(G)$ 是 G 的一个极大子群。根据 Shepard [8], , 子群 $P(G)$ 的类至多为 $(p-1)/2$。因此，Lazard 对应适用于 $P(G)$，从而得到李环 $L(P(G))$。一个核心目标是理解这些李环。

致谢： 第二作者获得了亚历山大·冯·洪堡基金会研究奖学金的资助。第三作者感谢英国皇家学会通过研究基金 RGS \R2 \252076 提供的支持。

在 [3] 中证明了，若 G 不是其分支 $\mathcal{B}_i$ 中的叶节点，那么其李环 $L(P(G))$ 源自一种基于 p-进数论的构造，下面将对此作出概述。

1.1 李 p-环的构造

设 $K = \mathbb{Q}_p(\theta)$，其中 $\mathbb{Q}_p$ 表示 p-进有理数域，θ 是一个本原 p 次单位根。设 $\mathcal{O}$ 是 K 中的极大阶，并注意到 $\mathcal{O}$ 有唯一的极大理想 $\mathfrak{p}$，由 $\kappa = \theta - 1$ 生成。环 $\mathcal{O}$ 有唯一的理想链 $\mathcal{O} = \mathfrak{p}^0 > \mathfrak{p}^1 > \mathfrak{p}^2 > \ldots > \{0\}$，其中 $\mathfrak{p}^i$ 由 κ^i 生成，且在 $\mathcal{O}$ 中的指数为 p^i。我们将 $\mathfrak{p}^i \wedge \mathfrak{p}^i$ 视为带有对角作用的 θ-模，并定义

$$H_i = \mathrm{Hom}_\theta(\mathfrak{p}^i \wedge \mathfrak{p}^i, \mathfrak{p}^{2i+1}) \quad \text{and} \quad \hat{H}_i = \{\gamma \in H_i \mid \gamma \text{ surjective }\}.$$

对于 $\gamma \in \hat{H}_i$ 和 $u,\ v,\ w \in \mathfrak{p}^i$，记作

$$J_\gamma(u,v,w) = \gamma(\gamma(u \wedge v) \wedge w) + \gamma(\gamma(v \wedge w) \wedge u) + \gamma(\gamma(w \wedge u) \wedge v).$$

将 $J(\gamma)$ 定义为 $\mathcal{O}$ 中由集合 $\{J_\gamma(u,\ v,\ w) \mid u,\ v,\ w \in \mathfrak{p}^i\}$ 生成的理想。于是存在 $\lambda(\gamma) \in \mathbb{N}_0 \cup \{\infty\}$，使得

$$J(\gamma) = \mathfrak{p}^{\lambda(\gamma)};$$

其中 $\mathfrak{p}^\infty = \{0\}$。我们将 $L_{i,\ m}(\gamma)$ 定义为集合 $\mathfrak{p}^i/\mathfrak{p}^m$，其加法为自然加法，乘法为 $[x + \mathfrak{p}^m, y + \mathfrak{p}^m] = \gamma(x \wedge y) + \mathfrak{p}^m$。若 $m \le \lambda(\gamma)$，则 $L_{i,\ m}(\gamma)$ 是一个李环，其阶为 p^{m-i}。[3] 中的一个中心结果如下所述。

1 定理：（EKS [3]）
设 $p \ge 5$，设 $i > p+1$，并设 G 为 $\mathcal{B}_i$ 中的一个群，且 G 不是叶子。记 P 为 G 中的二步中心化子，并记 $m = \log_p |P| + i$。那么存在 $\gamma \in H_i$，使得

$$L(P) \cong L_{i,m}(\gamma).$$

1.2 李 p-环的研究

现在我们的目标是理解定理 1 中出现的李环 $L_{i,\ m}(\gamma)$。这些满足 $m \le \lambda(\gamma)$，并且是 $L_{i,\ \lambda(\gamma)}(\gamma)$ 的商。第一步是研究 $\lambda(\gamma)$。注意，若 $L_{i,\ \lambda(\gamma)}(\gamma)$ 是有限的，则根据构造，其大小为 $p^{\lambda(\gamma)-i}$。这里的中心结果如下，证明见第 5.3 节，其中包括对 y 的明确界。

2 定理：（主定理 I）
设 $p \ge 5$ 和 $i \ge 1$。则集合 $\{\lambda(\gamma) \mid \gamma \in \hat{H}_i\} \subseteq \mathbb{N}_0$。如果 $L_{i,\ \lambda(\gamma)}(\gamma)$ 是有限的；更准确地说，存在 $y \in \mathbb{N}_0$ 使得 $\lambda = 3i + 13 - 2p + y$，或者等价地，存在 $y \in \mathbb{N}_0$ 使得

$$|L_{i,\lambda}(\gamma)| = p^{2i+13-2p+y}.$$

根据 [3, 定理 1], , $L_{i,\ \lambda}(\gamma)$ 的有限性意味着 $L_{i,\ \lambda}(\gamma)$ 是幂零的；若 $i > p-1$，则 $L_{i,\ \lambda}(\gamma)$ 的类至多为 $p-1$。在后一种情况下，Lazard 对应适用，为每个由此得到的李环 L 定义一个群 $G(L)$。由此得到以下结果。

3 推论： 设 $p \geq 5$ 和 $i > p+1$。记 $\mathcal{L}_i = \{L_{i,m}(\gamma) \mid \gamma \in H_i, m \leq \lambda(\gamma)\}$，并令 $\mathcal{C}_i$ 为 $\mathcal{B}_i$ 中的非叶节点集合。于是，*Lazard* 对应诱导出一个满射

$$\mathcal{L}_i \to \mathcal{C}_i : L \to G(L) \rtimes \langle \theta \rangle,$$

其中 θ 通过在 $\mathcal{O}$ 上进行乘法作用，进而作用于 L 和 $G(L)$。

1.3 特殊情形

对于与 p 互素的 $j \in \mathbb{Z}$，令 σ_j 为将 θ 映射到 θ^j的 K 的伽罗瓦自同构。对于$a \in \{2, \ldots, (p-1)/2\}$，定义 ϑ_a： $K \wedge K \to K$，如下

$$\vartheta_a(x \wedge y) = \sigma_a(x)\sigma_{1-a}(y) - \sigma_{1-a}(x)\sigma_a(y).$$

如 [3, 引理 6]中所述，对于每个 $i \in \mathbb{N}_0$，同态 ϑ_a 张成H_i 在 K上的空间。若 $p = 5$，则只需对某个 $c \in \mathcal{U}$取 $\gamma = c\vartheta_2$，其中 $\mathcal{O}$的单位群。由此得到以下特殊情形。

4 定理：（主定理 II）
设 $p \geq 5$ 和 $i \in \mathbb{N}_0$。设 $\gamma = c\vartheta_a$，其中某个 $c \in \mathcal{U}$ 和 $2 \leq a \leq (p-1)/2$，并记$\lambda = \lambda(\gamma)$。那么 $\gamma \in H_i$ 且 $|L_{i,\lambda(\gamma)}| = p^{2i+3+y}$，其中某个 $y \in \{0, 1, 2\}$。若 $p = 5$，则$y = 0$ 成立。

GAP 实验表明，若 $\gamma = \vartheta_a$，则 $y \in \{0, 2\}$。虽然对于 $p = 5$，情形 $y = 2$ 不会出现，但它会出现在更大的素数情形中。例如：

- 若 $p = 7$，则 $y = 2$，当 $(a, i) \in \{(2, 3), (3, 2), (3, 5)\}$ 时。
- 若 $p = 11$，则 $y = 2$，当 $(a, i) \in \{(4, 10)\}$ 时。
- 如果 $p = 13$，那么 $y = 2$ 如果 $(a,\ i) \in \{(2、4)，(4、2)，(4、5)，(4、8)，(4、11)，(5、4)，(6、3)，(6、9)\}$。

2 数论预备知识

本节回顾一些数论预备知识。与之前一样，设 $K = \mathbb{Q}_p(\theta)$，其中θ 是一个本原 p次单位根，设 $\mathcal{O}$ 是 K 中的极大阶，并设 $\mathfrak{p}$ 表示 $\mathcal{O}$中的唯一极大理想。于是， κ 生成 $\mathfrak{p}$ 作为理想，而 $\mathcal{U} = \mathcal{O} \setminus \mathfrak{p}$ 是 $\mathcal{O}$中的单位元。

5 定义： 对于 $v \in K$，我们将 v 的赋值定义为 $val(v) = n$，若 $v \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$，并定义 $val(0) = \infty$。对于 K 上的向量 v，我们将 $val(v)$ 定义为 v各项赋值的最小值。

$\mathcal{O}$ 的理想 $\mathfrak{p}^i$ 具有自然的 $\mathbb{Z}_p$-基 $\{\theta^j\kappa^i \mid 0 \le j < p-1\}$。在应用中，考虑不同的基通常很有用，如下述注记所示。

6 注记：令 $i \in \mathbb{N}_0$ 和 $d = p-1$ 为 $\mathcal{O}$ 的 $\mathbb{Z}_p$-维数。
(a) 集合 $\{\kappa^j \mid i \le j < i+d\}$ 是 $\mathfrak{p}^i$ 的一个 $\mathbb{Z}_p$-基。(b) 集合 $\{\kappa^j \wedge \kappa^k \mid i \le j < k < i+d\}$ 作为 $\mathbb{Z}_p$-模生成 $\mathfrak{p}^i \wedge \mathfrak{p}^i$。(c) $\kappa^d \equiv -p$ 模 $\mathfrak{p}^{d+1}$。

证明：(a) 和 (b) 是众所周知的，接下来只需证明 (c)。首先注意，对于 $1 \le r \le p-1$ 和 $\sum_{r=0}^{p-1}\binom{p-1}{r} = \binom{p}{r+1}$，有 $\theta^r = (1+\kappa)^r = 1 + r\kappa + \binom{r}{2}\kappa^2 + \cdots + \binom{r}{r}\kappa^r$。由于 $p \in \mathfrak{p}^p$，可得

$$0 = 1 + \theta + \cdots + \theta^{p-1} = p + \binom{p}{2}\kappa + \cdots + \binom{p}{p}\kappa^{p-1} \equiv p + \kappa^{p-1} \bmod \mathfrak{p}^p.$$

由于 $d = p-1$，这就得到了 (c) 的结果。 •

令 $\omega \in \mathbb{Q}_p$ 为单位根（$p-1$ 阶），令 r 为整数（$\mathbb{Z}/p\mathbb{Z}$）乘法群的生成元*，满足 $\omega - r \in \mathfrak{p}$。然后令 $\sigma = \sigma_r$，并注意到 σ 生成 $Gal(K)$。以下内容在第 2] 节的 [6, 中得到证明。

7 定理：
(a) σ 的特征值为 1、ω、.....、ω^{p-2}，且每个特征子空间的维数均为 1。(b) 如果 $v \in K$ 是 σ 的特征向量，那么对应的特征值为 $\omega^{val(v)}$。(c) 对于每个 $n \in \mathbb{Z}$，都存在 σ 的一个特征向量 $v \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$。

以下结果是一个显然的推论。

8 推论： 令 v 为 σ 的特征向量，且满足 $val(v) = n$。那么 v 是 σ^m 的特征向量，其特征值为 ω^{mn}。此外，若 $a \in \{2, \ldots (p-1)/2\}$，其中 $\sigma_a = \sigma^k$，且对于某些整数 k 和 l，有 $\sigma_{1-a} = \sigma^l$，那么

$$\sigma_a(v) = \omega^{kn}v, \quad \sigma_{1-a}(v) = \omega^{ln}v, \quad \sigma_{a^2}(v) = \omega^{2kn}v,$$
$$\sigma_{(1-a)^2} = \omega^{2ln}\omega, \quad \sigma_{a(1-a)}(v) = \omega^{(k+l)n}v.$$

证明：设 v 是 σ 的特征向量，且对应 $val(v) = n$。那么 $\sigma(v) = \omega^n v$，并且 $\sigma^2(v) = \sigma(\omega^n v)$。由于 $\omega \in \mathbb{Q}_p$ 被 σ 固定，因此可得 $\sigma^2(v) = \omega^n\sigma(v) = \omega^{2n}v$。反复应用这一思路，可得 v 是 σ^m 的特征向量，其特征值为 ω^{mn}。利用 l 和 k 的定义，即得所需结论。•

9 引理： 群 $Gal(K)$ 在 $\mathcal{O}/\mathfrak{p}$ 上的作用是平凡的。

证明：每个元素 $c \in \mathcal{O}$ 都可以写成 $c = \sum_{r=0}^{m} a_r\kappa^r$，其中 $m \in \mathbb{N}_0$ 和 $a_r \in \{0, \ldots, p-1\}$。因此 $c \equiv a_0$ 模 $\mathfrak{p}$ 且 $\sigma(c) = \sum_{r=0}^{m} a_r\sigma(\kappa)^r \equiv a_0$ 模 $\mathfrak{p}$。•

3 同态空间的预备知识

全文中，我们假设 $p \geq 5$ 是素数且 $i \in \mathbb{N}_0$。本节旨在介绍该空间的背景

$$\hat{H}_i \subseteq H_i = \mathrm{Hom}_\theta(\mathfrak{p}^i \wedge \mathfrak{p}^i, \mathfrak{p}^{2i+1}).$$

Leedham-Green & McKay 分析了 $\mathrm{Hom}_\theta(\mathcal{O} \wedge \mathcal{O}, \mathcal{O})$ 的结构，见 [7]。基于此，Dietrich & Eick [2] 证明，$\mathrm{Hom}_\theta(\mathcal{O} \wedge \mathcal{O}, \mathcal{O})$ 的每个元素都可以唯一地写成 $\sum_{a=2}^{(p-1)/2} c_a \vartheta_a$，其中系数为 $c_a \in \mathfrak{p}^{4-p}$。下述注记 $\hat{}$ 将其转化为 H_i。

10 注记：

(a) $\gamma \in \mathrm{Hom}_\theta(\mathfrak{p}^i \wedge \mathfrak{p}^i, \mathfrak{p}^{2i+1})$ 通过以下方式诱导出 $\hat{\gamma} \in \mathrm{Hom}_\theta(\mathcal{O} \wedge \mathcal{O}, \mathcal{O})$

$$\hat{\gamma} : \mathcal{O} \wedge \mathcal{O} \to \mathcal{O} : (x \wedge y) \mapsto \kappa^{-(2i+1)} \gamma(\kappa^i x \wedge \kappa^i y).$$

(b) $\delta \in \mathrm{Hom}_\theta(\mathcal{O} \wedge \mathcal{O}, \mathcal{O})$ 通过以下方式诱导出 $\delta \in \mathrm{Hom}_\theta(\mathfrak{p}^i \wedge \mathfrak{p}^i, \mathfrak{p}^{2i+1})$

$$\overline{\delta} : \mathfrak{p}^i \wedge \mathfrak{p}^i \to \mathfrak{p}^{2i+1} : (x \wedge y) \mapsto \kappa^{(2i+1)} \delta(\kappa^{-i} x \wedge \kappa^{-i} y).$$

(c) 这两个映射互为逆映射，因此在 $\mathrm{Hom}_\theta(\mathcal{O} \wedge \mathcal{O}, \mathcal{O})$ 与 $\mathrm{Hom}_\theta(\mathfrak{p}^i \wedge \mathfrak{p}^i, \mathfrak{p}^{2i+1})$ 之间诱导出同构。

11 引理： 每个 $\gamma \in \hat{} H_i$ 都可以唯一地写成 $\gamma = \sum_{a=2}^{(p-1)/2} c_a \vartheta_a$ 的形式，其中 $c_a \in K$ 且 $val(c_a) \geq 5 - p$。

证明：设 $\gamma \in \hat{} H_i$。那么 $\hat{}\gamma = \sum c_a \vartheta_a$ 且 $\gamma = \hat{}\gamma$。由于 $\vartheta_a(\kappa^{-i} x \wedge \kappa^{-i} y) = \kappa^{-2i} u_{a,\,i} \vartheta_a(x \wedge y)$ 对某个单位元 $u_{a,\,i}$ 成立，因此 $\gamma = \sum_a \kappa c_a u_{a,\,i} \vartheta_a$，且此和中系数的赋值为 $val(\kappa c_a u_{a,\,i}) = val(c_a) + 1 \geq 5 - p$。•

$\hat{}$对于 $\gamma \in H_i$，我们记 $val(\gamma) = \min\{val(c_a) \mid 2 \leq a \leq (p-1)/2\}$。引理 11 有如下推论。

$\hat{}$**12 推论：** 设 $\gamma \in H_i$ 满足 $v = val(\gamma)$。

(a) $0 \geq v \geq 5 - p$。(b) $\gamma(\mathfrak{p}^j \wedge \mathfrak{p}^k) \in \mathfrak{p}^{j+k+v}$ 对每个 $j,\ k \geq i$。

证明：令 $\gamma = \sum c_a \vartheta_a$。

(a) 这由引理 11 得出。注意，并非所有系数 c_a 都能属于 $\mathfrak{p}$。(b) 注意，对于所有 $j, k,\ \vartheta_a(\mathfrak{p}^j \wedge \mathfrak{p}^k) \leq \mathfrak{p}^{j+k}$。因此，对于所有 $a, j, k,\ c_a \vartheta_a(\mathfrak{p}^j \wedge \mathfrak{p}^k) \in \mathfrak{p}^{j+k+v}$。 •

4 一个下界

ˆ 在本节中，我们始终假设 $p \geq 5$ 是素数且 $i \in \mathbb{N}_0$。令 $\gamma \in H_i$，并记作 $\gamma = \sum c_a \vartheta_a$ 和 $\lambda = \lambda(\gamma)$。回顾一下， $J(\gamma) = \mathfrak{p}^\lambda$。本节将介绍 λ 的下界。

对于每个 $x \in \mathbb{Z}$，令 e_x 为 σ 的特征向量，满足 $val(e_x) = x$。则 $\sigma(e_x) = \omega^x e_x$。回忆一下，$\omega \in \mathbb{Z}_p$ 是一个 $(p-1)$ 次本原单位根，且 $\omega \equiv r$ 模 p。令 $\sigma_a = \sigma^{k_a}$ 和 $\sigma_{1-a} = \sigma^{l_a}$，其中 k_a, $l_a \in \mathbb{N}$。接下来的三个结果由直接计算得到。

13 引 理： 对于 u、$v \in \mathbb{Z}$，定义 $m_a(u、v) = \omega^{uk_a + vl_a} \in \mathbb{Z}_p$。对于 $c \in K$，可得

$$\vartheta_a(ce_x \wedge e_y) = (\sigma_a(c)m_a(x,y) - \sigma_{1-a}(c)m_a(y,x))e_x e_y.$$

14 引理： 对于 x、$y \in \mathbb{Z}$，定义 $t_a(x、y) = m_a(x、y) - m_a(y、x) \in \mathbb{Z}_p$。则

$$\begin{aligned} & \gamma(\gamma(e_x \wedge e_y) \wedge e_z) \\ = \ & (\sum_{a,b} c_a \sigma_a(c_b) t_b(x,y) m_a(x+y,z) - c_a \sigma_{1-a}(c_b) t_b(x,y) m_a(z,x+y)) e_x e_y e_z. \end{aligned}$$

定义 $l_{a,\ b}(x,\ y,\ z)$ $r_{a,\ b}(x,\ y,\ z) \in \mathbb{Z}_p$ 和 $\Gamma_\gamma(x,\ y,\ z) \in K$ 为

$$\begin{aligned} l_{a,b}(x,y,z) &= t_b(x,y)m_a(x+y,z) + t_b(y,z)m_a(y+z,x) + t_b(z,x)m_a(z+x,y), \\ r_{a,b}(x,y,z) &= t_b(x,y)m_a(z,x+y) + t_b(y,z)m_a(x,y+z) + t_b(z,x)m_a(y,z+x), \\ \Gamma_\gamma(x,y,z) &= \sum_{a,b} c_a \sigma_a(c_b) l_{a,b}(x,y,z) - c_a \sigma_{1-a}(c_b) r_{a,b}(x,y,z). \end{aligned}$$

15 引理： 对于每个 $x, y, z \in \mathbb{N}_0$，可得

$$\begin{aligned} & \gamma(\gamma(e_x \wedge e_y) \wedge e_z) + \gamma(\gamma(e_y \wedge e_z) \wedge e_x) + \gamma(\gamma(e_z \wedge e_x) \wedge e_y) \\ = \ & \Gamma_\gamma(x,y,z) e_x e_y e_z. \end{aligned}$$

以下定理为定理 2 和定理 4 的证明迈出了第一步。

ˆ**16 定理：** 设 $\gamma \in H_i$ 满足 $v = val(\gamma)$，并记 $\lambda = \lambda(\gamma)$。则 $\lambda \geq 3i + 3 + 2v$。因此，一般而言 $\lambda \geq 3i + 13 - 2p$，而当 $\gamma = c\vartheta_a$ 时 $\lambda \geq 3i + 3$。

证明：回顾一下， $J(\gamma) = \mathfrak{p}^\lambda$。由引理 15 可知， $J(\gamma)$作为理想由$\{\Gamma_\gamma(x,y,z)$ $e_x e_y e_z \mid x > y > z \geq i\}$ 生成。因此 $\lambda = \min\{val(\Gamma_\gamma(x,y,z)) + x + y + z \mid x > y > z \geq i\}$。项 $\Gamma_\gamma(x,y,z)$ 由 $\mathbb{Z}_p$ 中的元素、系数 c_a 及其在伽罗瓦群下的像组合而成。回顾推论 12 中的 $5 - p \leq v \leq 0$。因此，所有这些元素都在 $\mathfrak{p}^{2v}$ 中，从而对于所有 x, y, z， $\Gamma_\gamma(x,y,z) \geq 2v$。 x, y, z的最小选择是 $i + i + 1 + i + 2 = 3i + 3$。这就得到了所需结果。•

5 上界

ˆ 在本节中，我们假设 $p \geq 5$ 是素数且 $i \in \mathbb{N}_0$。我们考虑 $\gamma \in H_i$，并记 $\gamma = \sum c_a \vartheta_a$ 和 $\lambda = \lambda(\gamma)$。回顾一下， $J(\gamma) = \mathfrak{p}^\lambda$。本节将证明 λ 是有限的，并给出其上界。

5.1 同态的偏移量

我们的首要目标是分析所有 $j, k \geq i$ 的像 $\gamma(\mathfrak{p}^j \wedge \mathfrak{p}^k)$。我们将 $\rho(j,k) \in \mathbb{Z}$ 定义为

$$\gamma(\mathfrak{p}^j \wedge \mathfrak{p}^k) = \mathfrak{p}^{j+k+\rho(j,k)}.$$

回顾一下， $d = p-1$ 是每个 $\mathfrak{p}^j$ 的 $\mathbb{Z}_p$-维数，并且 $\mathfrak{p}^{j+d} = p\mathfrak{p}^j$ 成立。因此，对每个j, $k \geq i$ ，可得

$$\rho(j,k) = \rho(j+d,k) = \rho(j,k+d).$$

因此，集合 $\{\rho(j,k) \mid j,k \geq i\}$ 中只有有限个不同的值；这将在下述定义的第一部分中用到。此外，回顾一下，每个赋值为 v 的元素 $x \in K$ 都可以（唯一地）写成 $x = \sum_{j \geq v} a_j \kappa^j$，其中 $a_j \in \{0, \ldots, p-1\}$。

ˆ**17 定义：** 设 $\gamma \in H_i$。

(a) 偏移量 $\rho(\gamma)$ 的 γ 是 $\rho(\gamma) = \min\{\rho(j,k) \mid j,k \geq i\}$。

(b) 对于 $j,\ k \geq i$ 令 $a(j,k) \in \{0, \ldots, p-1\}$ 定义为

$$\gamma(\kappa^j \wedge \kappa^k) \equiv a(j,k)\kappa^{j+k+\rho(\gamma)} \bmod \mathfrak{p}^{j+k+\rho(\gamma)+1}.$$

偏移量是一个整数。下面的引理给出了它的一个下界。 .

ˆ**18 引理：** 设 $\gamma \in H_i$。则 $5 - p \leq \rho(\gamma)$。

证明：由引理 11 可将同态 γ 写成 $\gamma = \sum c_a \vartheta_a$，其中 $val(c_a) \geq 5 - p$。由 [3, 引理 6] 可知， $\vartheta_a(\mathfrak{p}^j \wedge \mathfrak{p}^k) = \mathfrak{p}^{j+k+\epsilon}$，其中 $\epsilon \in \{0,1\}$。因此$\gamma(\mathfrak{p}^j \wedge \mathfrak{p}^k) \subseteq \mathfrak{p}^{j+k+5-p}$，于是对每个 $j,\ k$，都有 $\rho(j,\ k) \geq 5-p$。•

作为示例，我们展示了 $p = 7$ 的 $a(j,\ k)$ 数组，以及范围 $0 \leq j,\ k < 6$ 内的两个同态 ϑ_2（左侧）和 ϑ_3（右侧），其中 $i = 0$。

$$\begin{pmatrix} 0 & 4 & 4 & 5 & 6 & 2 \\ 3 & 0 & 6 & 6 & 4 & 2 \\ 3 & 1 & 0 & 2 & 2 & 6 \\ 2 & 1 & 5 & 0 & 3 & 3 \\ 1 & 3 & 5 & 4 & 0 & 1 \\ 5 & 5 & 1 & 4 & 6 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 2 & 2 & 0 & 5 & 5 \\ 5 & 0 & 2 & 2 & 0 & 5 \\ 5 & 5 & 0 & 2 & 2 & 0 \\ 0 & 5 & 5 & 0 & 2 & 2 \\ 2 & 0 & 5 & 5 & 0 & 2 \\ 2 & 2 & 0 & 5 & 5 & 0 \end{pmatrix}$$

我们证明 λ 上界的主要部分在于尽可能充分地理解系数$a(j,k)$。为此迈出的第一步是以下引理。

ˆ**19 引理：** 设 $\gamma \in H_i$，设 $\rho = \rho(\gamma)$，并设 $d = p-1$。
(a) $a(j,j) = 0$ 对所有 $j \geq i$成立。(b) $a(j,k) \equiv -a(k,j)$ 模 p 对所有 $j,k \geq i$成立。(c) $a(j,k) = a(j+d,k) = a(j,k+d)$ 对所有 $j,k \geq i$成立。(d) $a(j,k) \equiv a(j+1,k) + a(j,k+1)$ 模 p 对所有 $j,k \geq i$成立。(e) $a(j,j+1) = a(j,j+2)$ 对所有 $j \geq i$成立。(f) $a(j,j+d-2) = a(j+d-1,j+d-2)$ 对所有 $j \geq i$成立。

证明：在整个证明过程中，令 $j,\ k \geq i$。
(a) 这直接由 $\gamma(\kappa^j \wedge \kappa^j) = 0$得到。(b) 这是通过 $\gamma(\kappa^j \wedge \kappa^k) = -\gamma(\kappa^k \wedge \kappa^j)$得到的。(c) 首先注意到 $\gamma(\kappa^{j+d} \wedge \kappa^k) = \gamma(\kappa^d\kappa^j \wedge \kappa^k)$。接着，$\kappa^d \equiv -p$ 模 $\mathfrak{p}^{d+1}$，见注6。因此模 $\mathfrak{p}^{j+k+d+\rho+1}$进行计算，我们得到如下结果：

$$\begin{aligned} a(j+d,k)\kappa^{j+d+k+\rho} &\equiv \gamma(\kappa^{j+d} \wedge \kappa^k) \\ &\equiv \gamma(-p\kappa^j \wedge \kappa^k) \\ &= -p\gamma(\kappa^j \wedge \kappa^k) \\ &\equiv -pa(j,k)\kappa^{j+k+\rho} \\ &\equiv a(j,k)\kappa^d\kappa^{j+k+\rho} \\ &= a(j,k)\kappa^{j+k+d+\rho}. \end{aligned}$$

因此，$a(j+d,\ k) = a(j,\ k)$ 成立。类似地，$a(j,\ k) = a(j,\ k+d)$ 也成立。
(d) 由于 γ 是双线性的，且 $\theta = \kappa + 1$，因此对 $\alpha,\ \beta \in \mathfrak{p}^i$ 有

$$\begin{aligned} \kappa\gamma(\alpha \wedge \beta) &= \gamma(\theta\alpha \wedge \theta\beta) - \gamma(\alpha \wedge \beta) \\ &= \gamma(\kappa\alpha \wedge \kappa\beta) + \gamma(\kappa\alpha \wedge \beta) + \gamma(\alpha \wedge \kappa\beta). \end{aligned}$$

我们将此应用于 $(\alpha,\ \beta) = (\kappa^j,\ \kappa^k)$。利用 $\gamma(\kappa^{j+1} \wedge \kappa^{k+1}) \in \mathfrak{p}^{j+k+\rho+2}$，可得以下模 $\mathfrak{p}^{j+k+\rho+2}$ 的结果：

$$\begin{aligned} a(j,k)\kappa^{j+k+\rho+1} &\equiv \kappa\gamma(\kappa^j \wedge \kappa^k) \\ &\equiv \gamma(\kappa^{j+1} \wedge \kappa^k) + \gamma(\kappa^j \wedge \kappa^{k+1}) \\ &\equiv (a(j+1,k) + a(j,k+1))\kappa^{j+k+\rho+1}. \end{aligned}$$

由此得到所需结果。
(e) 我们将前面各部分合并，得到 $a(j,j+1) = a(j+1,j+1) + a(j,j+2) = a(j,j+2)$。(f) 再次将前面各部分合并，可得 $a(j+d-1,j+d-2) = a(j+d,j+d-2) + a(j+d-1,j+d-1) = a(j+d,j+d-2) = a(j,j+d-2)$。•

5.2 雅可比元素

令 $\gamma \in \hat{}H_i$。回忆一下，$\mathfrak{p}^\lambda = J(\gamma) = \langle J_\gamma(u,v,w) \mid u,v,w \in \{\kappa^j \mid j \geq i\}\rangle$，其中

$$J_\gamma(u,v,w) = \gamma(\gamma(u \wedge v) \wedge w) + \gamma(\gamma(v \wedge w) \wedge u) + \gamma(\gamma(w \wedge u) \wedge v).$$

我们定义整数 $J(j,k,l) \in \{0,\ldots,p-1\}$，其中 $j,k,l \geq i$，定义如下

$$J(j,k,l) := a(j,k)a(j+k+\rho,l) + a(k,l)a(k+l+\rho,j) + a(l,j)a(l+j+\rho,k) \bmod p.$$

^20 引理： 设 $\gamma \in H_i$ 满足 $\rho = \rho(\gamma)$，并设 j、k、$l \geq i$。则

$$J_\gamma(\kappa^j,\kappa^k,\kappa^l) \equiv J(j,k,l)\kappa^{j+k+l+2\rho} \bmod \mathfrak{p}^{j+k+l+2\rho+1}.$$

证明：我们模 $\mathfrak{p}^{j+k+l+2\rho+1}$ 进行计算：

$$\begin{aligned}\gamma(\gamma(\kappa^j \wedge \kappa^k) \wedge \kappa^l) &\equiv \gamma(a(j,k)\kappa^{j+k+\rho} \wedge \kappa^l)\\ &\equiv a(j,k)\gamma(\kappa^{j+k+\rho} \wedge \kappa^l)\\ &\equiv a(j,k)a(j+k+\rho,l)\kappa^{j+k+l+2\rho}\end{aligned}$$

由此得到所需结果。 •

例如，我们展示了 $p=7$ 对应的 $J(j,j+1,l)$ 数组，以及取值范围为 $0 \leq j,l < 6$ 且满足 $i=0$ 的两个同态：ϑ_2（左侧）和 ϑ_3（右侧）。

$$\begin{pmatrix} 0&0&4&4&4&5\\ 4&0&0&1&1&3\\ 0&1&0&0&6&6\\ 0&5&6&0&0&0\\ 3&3&6&0&0&0\\ 0&5&5&2&3&0 \end{pmatrix} \qquad \begin{pmatrix} 0&0&1&1&0&0\\ 1&0&0&1&1&1\\ 1&1&0&0&0&0\\ 6&0&0&0&0&6\\ 6&6&6&6&0&0\\ 0&0&0&6&6&0 \end{pmatrix}$$

雅可比元素 $J(j,\ k,\ l)$ 将是我们证明 λ 有限并确定其上界的主要工具。下面的定理将为此发挥核心作用。

^21 定理： 设 $\gamma \in H_i$ 并记 $\rho = \rho(\gamma)$ 以及 $d = p-1$。如果存在 j、k、$l \in \{i,\ldots,i+d-1\}$，使得 $J(j、\ k、\ l) \neq 0$，那么 $\lambda = \lambda(\gamma)$ 是有限的，且 $\lambda \leq 3i+3d-6+2\rho$。

证明：如果 $J(j、\ k、\ l) \neq 0$，那么 $J_\gamma(\kappa^j、\ \kappa^k、\ \kappa^l) \neq 0$，从而 $J(\gamma) \neq \{0\}$，如所需。λ 的上界也可以很容易地读出，因为 $J_\gamma(\kappa^j、\ \kappa^k、\ \kappa^l) \equiv J(j、\ k、\ l)\kappa^{j+k+l+2\rho}$ 模 $\mathfrak{p}^{j+k+l+2\rho+1}$，从而 $\lambda \leq j+k+l+2\rho$。如果 $\{j,k,l\}$ 中有两个元素相等，那么根据其定义和引理19，$J(j、\ k、\ l) = 0$。因此，使 $J(j、\ k、\ l) \neq 0$ 成立时，j、k、l 的最大取值为 $i+d-1$、$i+d-2$、$i+d-3$。故上界 $j+k+l+2\rho \leq 3i+3d-6+2\rho$ 得证。•

在本节剩余部分中，我们研究元素 $J(j,\ k,\ l)$，旨在证明其中对于 $i \leq j,\ k,\ l < i+d$ 存在一个非平凡元素。

ˆ**22 引理：** 设 $\gamma \in H_i$ 和 $i \le j$、k、l。记为 $d = p-1$。
(a) $J(j,k,l) = J(l,j,k) \equiv -J(k,j,l)$ 模 p。(b) $J(j,k,l) = J(j+d, k,l) = J(j,k+d,l) = J(j,k,l+d)$。(c) $J(j,k,l) \equiv J(j+1,k,l) + J(j,k+1,l) + J(j,k,l+1)$ 模 p。

证明：部分 (a) 和 (b) 直接由引理19以及 J 的定义得到。下面只需证明 (c)。由引理19可得

$$\begin{aligned} a(j,k)a(j+k+\rho,l) &= a(j,k)a(j+k+1+\rho,l) + a(j,k)b(j+k+\rho,l+1) \\ &= (a(j+1,k)+a(j,k+1))a(j+k+1+\rho,l) \\ &\quad + a(j,k)a(j+k+\rho,l+1). \end{aligned}$$

将 $(j,\ k,\ l)$ 替换为 $(k,\ l,\ j)$ 和 $(l,\ j,\ k)$，并将所得的三项相加，即可得到 (c) 的证明。•

5.3 定理 2 的证明

现在开始证明主要定理 2。下界已经得到证明。因此，还需证明 λ 是有限的。我们还将确定它的一个上界。

ˆ**23 引理：** 设 $\gamma \in H_i$。
(a) 存在 j、$k \in \{i, \ldots, i+d-1\}$，使得 $a(j,\ k) \neq 0$。(b) 若 $a(j,\ k) \neq 0$，则要么 $a(j+1,\ k) \neq 0$，要么 $a(j,\ k+1) \neq 0$。
(c) 存在 $j \in \{i, \ldots, i-d-1\}$，使得 $a(j,\ j+1) \neq 0$。

证明：（a）这直接由 $\rho(\gamma)$ 的定义得到。
(b) 由引理19(d)可得。
(c) 假设所有 $a(j, j+1) = 0$。我们证明这意味着对于所有 j、k，均有 $a(j,k) = 0$，从而与(a)矛盾。根据引理19(b)，我们假设 $j \le k$，并对 $k-j$使用归纳法。该假设断言 $k-j \le 1$ 成立，因此给出了归纳法的初始步骤。现在假设对于所有满足 $k-j \le l$ 的 $i \le j < k$（其中 $l > 1$），该断言均成立。则根据引理19(d)，$0 = a(j,k) \equiv a(j+1,k) + a(j,k+1)$ 模 p。由于 $j+1-k \le l$，归纳法断言 $a(j+1,k) = 0$。因此可推出 $a(j,k+1) = 0$。这完成了归纳步骤。•

ˆ**24 引理：** 设 $\gamma \in H_i$。记 $c(k) = a(k+1,k)$ 为 $k \ge i$。若 $j \ge i$ 且 $t > 0$，则

$$a(j+t,j) \equiv \sum_{u=0}^{\lfloor \frac{t-1}{2} \rfloor} (-1)^u \binom{t-u-1}{u} c(j+u) \bmod p.$$

证明：对于 $t=1$，结论显然成立。设 $t>1$，并记 $A_i=\lfloor\frac{t-i}{2}\rfloor$。我们对 t使用归纳法。引理19表明

$$\begin{aligned}
& a(j+t,j)\\
= \;& a(j+t-1,j)-a(j+t-1,j+1)\\
= \;& \sum_{u=0}^{A_2}(-1)^u\binom{t-u-2}{u}c(j+u)-\sum_{u=0}^{A_3}(-1)^u\binom{t-u-3}{u}c(j+1+u)\\
= \;& c(j)+\sum_{u=1}^{A_2}(-1)^u\binom{t-u-2}{u}c(j+u)-\sum_{u=1}^{A_1}(-1)^{u-1}\binom{t-(u-1)-3}{u-1}c(j+u)\\
= \;& c(j)+\sum_{u=1}^{A_2}(-1)^u(\binom{t-u-2}{u}+\binom{t-u-2}{u-1})c(j+u)\\
& \quad +\delta(-1)^{\frac{\lfloor t-1\rfloor}{2}}\binom{t-A_1-2}{A_3}c(j+A_1),
\end{aligned}$$

其中 $\delta=1$ 若 $A_1>A_2$，且 $\delta=0$ 若 $A_1=A_2$。若 $\delta=0$，则由最后一个等式可得结论。剩下的情况是 $\delta=1$。此时 $A_1=\frac{t-1}{2}$ 且 $A_3=\frac{t-3}{2}$。因此 $t-2-A_1=\frac{t-3}{2}$。于是 $\binom{t-A_1-2}{A_3}=\binom{\frac{t-3}{2}}{\frac{t-3}{2}}=1$。此外，$\binom{t-A_1-1}{A_1}=\binom{\frac{t-1}{2}}{\frac{t-1}{2}}=1$，故

$$\begin{aligned}
& \delta(-1)^{\frac{\lfloor t-1\rfloor}{2}}\binom{t-A_1-2}{A_3}c(j+A_1)\\
= \;& (-1)^{A_1}c(j+A_1)\\
= \;& (-1)^{A_1}\binom{t-A_1-1}{A_1}c(j+A_1).
\end{aligned}$$

因此结论得证。 •

定理 2 的证明。
现在证明存在整数 $j,\ k,\ l\geq i$，使得 $J(j,\ k,\ l)\neq 0$。接着，由引理22可知，对于某些 $i\leq j,\ k,\ l<i+d$，有 $J(j,\ k,\ l)\neq 0$，因此定理21适用，并得出我们所需的定理 2。

反设 $J(j,\ k,\ l)=0$ 对所有 $j,\ k,\ l\geq i$都成立。令 $m\geq i$ 使得$m+\rho\equiv 1$ 模 d。由引理19可知 $c(j)=a(j+1,\ j)=a(j+2,\ j)$，因此我们得到以下模 p的结果：

$$\begin{aligned}
0 \;&=\; J(j+1,j,m)\\
&\equiv\; a(j+1,j)a(j+1+j+\rho,m)\\
&\quad +a(j,m)a(j+m+\rho,j+1)\\
&\quad +a(m,j+1)a(m+j+1+\rho,j)\\
&\equiv\; c(j)a(j+1+j+\rho,m)
\end{aligned}$$

$$
\begin{aligned}
&+a(j,m)a(j+1,j+1)\\
&+a(m,j+1)a(j+2,j)\\
\equiv\ & c(j)(a(2j+1+\rho,m)-a(j+1,m)).
\end{aligned}
\tag{1}
$$

选择 j使得 $m<j<m+d$，并记作 $r=j-m$。则 $2j+1+\rho=2m+2r+1+\rho\equiv m+2r+2$模 d。此外，由引理24可得，存在 $x(1).....$， $x(r-1)\in\{0,\dots,p-1\}$，满足

$$
\begin{aligned}
&a(2j+1+\rho,m)-a(j+1,m)\\
=\ & a(m+2r+2,m)-a(m+r+1,m)\\
=\ & \sum_{u=0}^{\lfloor\frac{2r+1}{2}\rfloor}(-1)^u\binom{2r+2-u-1}{u}c(m+u)-\sum_{u=0}^{\lfloor\frac{r}{2}\rfloor}(-1)^u\binom{r+1-u-1}{u}c(m+u)\\
=\ & (-1)^r\binom{2r+2-r-1}{r}c(m+r)+\sum_{u=1}^{r-1}x(u)c(m+u)\\
=\ & (-1)^r(r+1)c(m+r)+\sum_{u=1}^{r-1}x(u)c(m+u).
\end{aligned}
\tag{2}
$$

结合方程（1）和（2）可得

$$
0=c(m+r)((-1)^r(r+1)c(m+r)+\sum_{u=1}^{r-1}x(u)c(m+u)).
\tag{3}
$$

现在，我们通过对 r进行归纳法证明 $c(m+r)=0$ 对 $0<r\le d-1$ 成立。对于 $r=1$，这可直接由方程（3）得出。令 $r>1$，并假设对 $0<l<r$有 $c(m+l)=0$。那么由方程（3）可得 $c(m+r)=0$。总之，对 $0<r\le d-1$有 $c(m+r)=0$。接下来，我们证明 $c(m)=0$。为此，注意到 $c(m)=-a(m,m+1)=-a(m+p-1,m+1)=-a(m+1+p-2,m+1)$。由引理24可得， $a(m+1+p-2,m+1)$可以写成 $\underline{c(m+1)\ c(m+2)\dots,c(m+\frac{p-3}{2})}$的组合。因此， $c(m)=0$ 得证。总之，我们现在已证明 $c(m)=\cdots=c(m+p-2)=0$。利用 $c(n)=a(n+1,n)=a(n+p,n+p-1)=c(n+p-1)$，可推出对所有 $n\ge i$ 都有 $c(n)=0$。因此，与引理23(c)矛盾。

5.4 单参数情形

本节始终假设 $p\ge5$ 是素数且 $i\in\mathbb{N}_0$。本节考虑 $\gamma\in H_i$ 的特殊情形，其中 $\gamma=c\vartheta$，对某个 $c\in\mathcal{U}$ 和 $a\in\{2,\dots,(p-1)/2\}$。
回顾推论 8， e_x 是 σ 的特征向量，且对每个 $x\in\mathbb{Z}$， σ 具有 $val(e_x)=x$。于是 $\sigma(e_x)=\omega^x e_x$。此外， $\omega\in\mathbb{Z}_p$ 是一个本原 $(p-1)$ 次单位根，且 $\omega\equiv r$ 模 p。令 $\sigma_a=\sigma^{k_a}$ 和 $\sigma_{1-a}=\sigma^{l_a}$，其中 k_a, $l_a\in\mathbb{N}$。

25 定义：对于 x， y， $z\in\mathbb{Z}$ 定义

(a) $t_1(x,\ y,\ z) = c\sigma_a(c)(\omega^{2k_a x}\omega^{(k_a+l_a)y}\omega^{l_a z} - \omega^{(k_a+l_a)x}\omega^{2k_a y}\omega^{l_a z})$, (b) $f(x,\ y,\ z) \in \{0,\dots,p-1\}$ 满足

$$t_1(x,y,z) + t_1(y,z,x) + t_1(z,x,y) = c^2 a^{3i}(1-a)^{2i} f(x,y,z) \bmod \mathfrak{p},$$

(c) $t_2(x,\ y,\ z) = c\sigma_{1_a - a}(c)(-\omega^{(k_a+l_a)x}\omega^{2l_a y}\omega^{k_a z} + \omega^{2l_a x}\omega^{(k_a+l_a)y}\omega^{k_a z})$, (d) $g(x,\ y,\ z) \in \{0,\dots,p-1\}$ 满足

$$t_2(x,y,z) + t_2(y,z,x) + t_2(z,x,y) = c^2 a^{2i}(1-a)^{3i} g(x,y,z) \bmod \mathfrak{p}.$$

26 引理： 设 $x,\ y,\ z \in \mathbb{Z}$ 和 $\gamma = c\vartheta_a$。
(a) $\gamma(\gamma(e_x \wedge e_y) \wedge e_z) = (t_1(x,\ y,\ z) + t_2(x,\ y,\ z))e_x e_y e_z$。
(b)

$$\begin{aligned} t_1(x,y,z) &\equiv c^2(a^{2x}(a(1-a))^y(1-a)^z - (a(1-a))^x(1-a)^{2y}(1-a)^z) \mod \mathfrak{p}, \\ t_2(x,y,z) &\equiv c^2(-(a(1-a))^x(1-a)^{2y}a^z + (1-a)^{2x}(a(1-a))^y a^z) \mod \mathfrak{p}. \end{aligned}$$

证明：(a) 直接计算可得

$$\begin{aligned} & \gamma(\gamma(e_x \wedge e_y) \wedge e_z) \\ = \ & c\sigma_a(c)(\sigma_{a^2}(e_x)\,\sigma_{a(1-a)}(e_y)\,\sigma_{1-a}(e_z) - \sigma_{a(1-a)}(e_x)\,\sigma_{a^2}(e_y)\,\sigma_{1-a}(e_z)) \\ & + c\sigma_{1-a}(c)(-\sigma_{a(1-a)}(e_x)\,\sigma_{(1-a)^2}(e_y)\,\sigma_a(e_z) + \sigma_{(1-a)^2}(e_x)\,\sigma_{a(1-a)}(e_y)\,\sigma_a(e_z)). \end{aligned}$$

推论 8 表明，对于每个 $u \in \mathbb{N}_0$，元素 e_u 是 σ_{a^2}、$\sigma_{a(1-a)}$ 和 $\sigma_{(1-a)^2}$ 各自的特征向量，其特征值分别为 $\omega^{2k_a u}$，$\omega^{(k_a+l_a)u}$ 和 $\omega^{l_a u}$。由此可得$\sigma_{a^2}(e_x)\sigma_{a(1-a)}(e_y)\sigma_{1-a}(e_z) = (\omega^{2k_a x}\omega^{(k_a+l_a)y}\omega^{l_a z})e_x e_y e_z$。以类似方式写出 $\gamma(\gamma(e_x \wedge e_y) \wedge e_z)$ 的其余 3 个加项，即可证明 (a)。

(b) 我们回顾 $\sigma_a = \sigma_r^{k_a} = \sigma_{r^{k_a}}$ 和 $\omega = r$ 模 $\mathfrak{p}$。由 $p\mathcal{O} \le \mathfrak{p}$很容易看出，$a = r^{k_a}$ 模 $\mathfrak{p}$，因此 $a = \omega^{k_a}$ 模 $\mathfrak{p}$；同样地，$1-a = \omega^{l_a}$ 模 $\mathfrak{p}$。最后一部分由在 t_1 和 t_2中应用 $a = \omega^{k_a}$ 模 $\mathfrak{p}$、$1-a = \omega^{l_a}$ 模 $\mathfrak{p}$，并注意到根据引理 9，$c = \sigma_a(c)$ 模 $\mathfrak{p} = \sigma_{1-a}(c)$，即可得到。•

27 引理 ma： 令 $i \in \mathbb{N}_0$ 和 x、y、$z \ge i$。记 $x = i + \bar{x}$、$y = i + \bar{y}$ 和 $z = i + \bar{z}$。于是

$$\begin{aligned} f(x,y,z) = {} & a^{2\bar{x}}(a(1-a))^{\bar{y}}(1-a)^{\bar{z}} - (a(1-a))^{\bar{x}}a^{2\bar{y}}(1-a)^{\bar{z}} + a^{2\bar{y}}(a(1-a))^{\bar{z}}(1-a)^{\bar{x}} \\ & - (a(1-a))^{\bar{y}}a^{2\bar{z}}(1-a)^{\bar{x}} + a^{2\bar{z}}(a(1-a))^{\bar{x}}(1-a)^{\bar{y}} - (a(1-a))^{\bar{z}}a^{2\bar{x}}(1-a)^{\bar{y}} \end{aligned}$$

and

$$\begin{aligned} g(x,y,z) = {} & -(a(1-a))^{\bar{x}}(1-a)^{2\bar{y}}a^{\bar{z}} + (1-a)^{2\bar{x}}(a(1-a))^{\bar{y}}a^{\bar{z}} - (a(1-a))^{\bar{y}}(1-a)^{2\bar{z}}a^{\bar{x}} \\ & + (1-a)^{2\bar{y}}(a(1-a))^{\bar{z}}a^{\bar{x}} - (a(1-a))^{\bar{z}}(1-a)^{2\bar{x}}a^{\bar{y}} + (1-a)^{2\bar{z}}(a(1-a))^{\bar{x}}a^{\bar{y}}. \end{aligned}$$

证明：利用引理 26，经过技术性计算可得

$$\begin{aligned} t_1(x,y,z) \bmod \mathfrak{p} &= c^2(a^{2i+2\bar{x}}(a(1-a))^{i+\bar{y}}(1-a)^{i+\bar{z}} - (a(1-a))^{i+\bar{x}}a^{2i+2\bar{y}}(1-a)^{i+\bar{z}}) \\ &= c^2a^{3i}(1-a)^{2i}(a^{2\bar{x}}(a(1-a))^{\bar{y}}(1-a)^{\bar{z}} - (a(1-a))^{\bar{x}}a^{2\bar{y}}(1-a)^{\bar{z}}). \end{aligned}$$

同理，我们可以得到，

$$t_1(y,z,x) = c^2a^{3i}(1-a)^{2i}(a^{2\bar{y}}(a(1-a))^{\bar{z}}(1-a)^{\bar{x}} - (a(1-a))^{\bar{y}}a^{2\bar{z}}(1-a)^{\bar{x}}) \mod \mathfrak{p},$$

$$t_1(z,x,y) = c^2a^{3i}(1-a)^{2i}(a^{2\bar{z}}(a(1-a))^{\bar{x}}(1-a)^{\bar{y}} - (a(1-a))^{\bar{z}}a^{2\bar{x}}(1-a)^{\bar{y}}) \mod \mathfrak{p}.$$

因此，$t_1(x,y,z) + t_1(y,z,x) + t_1(z,x,y) = c^2a^{3i}(1-a)^{2i}f(x,y,z)$ 模 $\mathfrak{p}$。同理，我们得到 $t_2(x,y,z) + t_2(y,z,x) + t_2(z,x,y) = c^2a^{2i}(1-a)^{3i}g(x,y,z)$ 模 $\mathfrak{p}$。•

28 引理： 设 $i \in \mathbb{N}_0$ 和 $x,y,z \geq i$。那么 $J_\gamma(e_x,e_y,e_z) \in \mathfrak{p}^{x+y+z+1}$ 当且仅当

$$a^{3i}(1-a)^{2i}f(x,y,z) + a^{2i}(1-a)^{3i}g(x,y,z) \equiv 0 \bmod p \tag{4}$$

证明：由引理 27 可得

$$\begin{aligned} & J_\gamma(e_x,e_y,e_z) \\ =& (t_1(x,y,z) + t_2(x,y,z) + t_1(y,z,x) + t_2(y,z,x) + t_1(z,x,y) + t_2(z,x,y))e_xe_ye_z \\ =& c^2(a^{3i}(1-a)^{2i}f(x,y,z) + a^{2i}(1-a)^{3i}g(x,y,z))e_xe_ye_z \mod \mathfrak{p}^{x+y+z+1}. \end{aligned}$$

上述等式的最后一行是由 $val(e_xe_ye_z) = x+y+z$ 这一事实得到的。因此，结论成立。•

定理 4 的证明。
定理 16 表明 $\lambda \geq 3i+3$。由于 $|L_{i,\lambda}(\gamma)| = p^{\lambda-i}$，我们有 $|L_{i,\lambda}(\gamma)| = p^{2i+3+y}$，其中某个 $y \in \mathbb{N}_0$。我们旨在证明 $y \leq 2$。反设 $y \geq 3$。则 $\lambda \geq 3i+6$。因此 $J_i(\gamma) \subseteq \mathfrak{p}^{3i+6}$。回忆定义 25 中的函数 f 和 g。令

$$\begin{aligned} F_1 &= f(i,i+1,i+2), \\ G_1 &= g(i,i+1,i+2), \quad \text{and} \\ E_1 &= a^{3i}(1-a)^{2i}F_1 + a^{2i}(1-a)^{3i}G_1. \end{aligned}$$

Then $E_1 \equiv 0$ 模 p，在公式（4）中取 $(x,\ y,\ z) = (i,\ i+1,\ i+2)$。类似地 ，

$$\begin{aligned} F_2 &= f(i,i+1,i+4), \\ G_2 &= g(i,i+1,i+4), \quad \text{and} \\ E_2 &= a^{3i}(1-a)^{2i}F_2 + a^{2i}(1-a)^{3i}G_2. \end{aligned}$$

因此，在公式（4）中取（$x,\ y,\ z$）=（$i,\ i+1,\ i+4$），可得 $E_2 \equiv 0$ 模 p。此外，我们有 $F_2E_1 - F_1E_2 \equiv 0$ 模 p。另一方面，直接计算可得 $F_2E_1 -$

$F_1E_2 = a^{2i}(1-a)^{3i}\big(F_2G_1 - F_1G_2\big)$。因此，$a^{2i}(1-a)^{3i}\big(F_2G_1 - F_1G_2\big) \equiv 0$ 模 p。现在，直接计算可得 $F_2G_1 - F_1G_2 = a^4(1-a)^4(2a-1)^3(a^2+a-1)(a^2-3a+1)$，并且注意到 a，$1-a$，$2a-1$ 模 p 均非零，因为 $a \in \{2, \ldots (p-1)/2\}$。所以

$$(a^2+a-1)(a^2-3a+1) \equiv 0 \bmod p.$$

由引理 27 直接计算可得

$$F_1 = f(i, i+1, i+2) = a(1-a)^2(2a-1)(a^2+a-1),$$
$$G_1 = g(i, i+1, i+2) = a^2(1-a)(2a-1)(a^2-3a+1).$$

由于 $E_1 = a^{3i}(1-a)^{2i}F_1 + a^{2i}(1-a)^{3i}G_1 \equiv 0$ 模 p，可知若 $a^2-3a+1 \equiv 0$ 模 p，则 $a^2+a-1 \equiv 0$ 模 p。接下来，若 $a^2-3a+1 \equiv 0$ 模 p，则 $a^2+a-1 = (a^2-3a+1) + 2(2a-1) = 2(2a-1) \neq 0$ 模 p。因此 $a^2-3a+1 \neq 0$ 模 p。同理，$a^2+a-1 \neq 0$ 模 p。因此，$(a^2+a-1)(a^2-3a+1) \neq 0$ 模 p。这就产生了矛盾，故 $y \leq 2$。

我们考虑特殊情形 $p = 5$。此时 $a = 2$ 成立。在 F_1 中取 $a = 2$，可得 $f(i, i+1, i+2) = 0$ 模 5，且 $g(i, i+1, i+2) \neq 0$ 模 5。因此，$a^{3i}(1-a)^{2i}f(i, i+1, i+2) + a^{2i}(1-a)^{3i}g(i, i+1, i+2) \neq 0$ 模 p。由公式（4）可知，$J_\gamma(e_i, e_{i+1}, e_{i+2}) \notin \mathfrak{p}^{3i+4}$。因此，$J(\gamma) \not\subseteq \mathfrak{p}^{3i+4}$，进而 $\lambda = 3i+3$。这说明在此特殊情形下，$y = 0$。

参考文献

[1] N. Blackburn，关于一类特殊的 p-群，《数学学报》100 (1958), 45–92。[2] H. Dietrich 和 B. Eick，具有“大”自同构群的极大类有限 p-群，《群论杂志》20 (2017), 227–256。[3] B. Eick、P. Komma 和 S. Saha，与极大类 p-群相关的图的框架 (2025), arXiv:2512.11379。[4] TheGAPGroup，GAP——群、算法与编程，版本 4.14.0 (2025)，https://www.gap-system.org。[5] C. R. Leedham-Green 和 S. McKay，关于极大类 p-群 I，《牛津大学数学季刊》27 (107) (1976), 297–311。[6] C. R. Leedham-Green 和 S. McKay，关于极大类 p-群的分类，《牛津大学数学季刊》35 (139) (1984), 293–304。[7] C. R. Leedham-Green 和 S. McKay，素数幂阶群的结构，伦敦数学会专著·新编，牛津大学出版社 (2002)。

[8] R. Shepherd，p阶最大类群，博士论文，芝加哥大学 (1970).