arXiv:2603.22185v1 [math.RA] 23 Mar 2026

有限域上的忠实分裂元循环群的扭曲群代数

Sanjit Bhowmick* Javier de la Cruz † Edgar Mart´ınez-Moro ‡

2026年3月24日

摘要

设 $\mathbb{F}_\ell$ 为含有 ℓ 个元素的有限域， $G = C_p \rtimes C_m$ 为一个忠实分裂元循环群。本文建立了扭群代数 $\mathbb{F}_\ell^\alpha G$的完整理论。利用 Lyndon–Hochschild–Serre 谱序列，我们证明 G 的第二上同调群同构于 $\mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^m$，并表明所有扭曲仅发生在 C_m 因子上。通过分析弗罗贝尼乌斯自同构与群作用在 C_p特征群上的联合作用，我们确定了本原中心幂等元。利用交叉积理论和有限域的结构，我们得到 $\mathbb{F}_\ell^\alpha G$到矩阵代数的完整 Wedderburn 分解，其中底域 $\mathbb{F}_{\ell^{d_j}}$可被显式确定。最后，也确定了 $\mathbb{F}_\ell$ 上的 G 不可约射影表示。

1 引言

扭曲群代数由 Schur [16, 17, 18] 引入，为射影表示论与环论之间建立了联系。扭曲群代数是群代数的一种推广，其乘法仍由群的乘法诱导，但结果会被一个标量扭曲，而该标量由一个 2-余循环确定。半单情形在许多场景中尤为重要；例如，参见 [12]。此外，已有研究探讨了有限域 $\mathbb{F}_\ell$ 上的某些扭曲群代数的若干方面 [7, 8], ，且这些代数具有实际价值。它们已应用于纠错码 [1, 5, 6, 9, 20] 的研究以及 McEliece密码系统 [4, 13]的设计。此外，还有一些关于线性码何时能实现为群代数理想的结构性结果；例如， [2] 中的作者给出了线性码能实现为有限群代数中的理想的充要条件， [5]证明了扭曲群代数中的理想也有类似结果，而 [6] 中的作者则将这一刻画推广到了交叉积。

*电子邮件：sanjitbhowmick@rnd.iitg.ac.in，电子与电气工程系，古瓦哈提印度理工学院，阿萨姆邦，781039，印度

†电子邮件：jdelacruz@uninorte.edu.co，数学与统计系，北方大学，巴兰基亚，哥伦比亚

‡电子邮件：edgar.martinez@uva.es，数学研究所，巴利亚多利德大学，西班牙巴利亚多利德。部分经费由 SAGACT-1 资助项目 MCIN/AEI/ 10.13039/501100011033 和欧洲区域发展基金“建设欧洲的一种方式” PID2022-138906NB-C212023/2027 提供

本文研究与半直积群$G = C_p \rtimes C_m$相关联的扭曲群代数，其中 $m \mid p-1$。当 $m = 2$时，我们的结果可还原为 Duarte 在 [8]中关于二面体群的定理。特别地，当应用于 $m = 2$时，我们的定理 4.5 可化为 $[8, \text{定理 } 12]$。然而，这一推广不仅涵盖了二面体情形的基本特征，还揭示了由作用于所得简单分量结构的更复杂作用所带来的新现象。我们将以显式形式给出完整 Wedderburn 分解，并用表格总结分析中的所有可能情形。

值得一提的是，本文中的定理 2.3 表明 $H^2(G, \mathbb{F}_\ell^\times) \cong H^2(C_m, \mathbb{F}_\ell^\times)$。这意味着所有上同调扭曲都集中在循环 C_m 因子上。然而，这并不意味着 C_p 因子与代数 $\mathbb{F}_\ell^\alpha G$ 的结构无关。C_m 在 C_p 上的作用会在特征的弗罗贝尼乌斯轨道上诱导一个置换作用，而在扩域 $\mathbb{F}_{\ell^f}$ 上由此产生的交叉积结构可能非常复杂。余循环 α 在 C_p 上的限制是平凡的，但上同调类会通过稳定子 $H \subseteq C_m$ 在域 $\mathbb{F}_{\ell^f}$ 上的作用重新出现在内交叉积中。

本文的组织结构如下。全文中，我们将考虑群 $G = C_p \rtimes C_m$，其中 p 是奇素数，m 是满足 $m \mid p-1$ 的正整数。在第 2 节中，我们介绍扭曲群代数、群的上同调以及群代数 $\mathbb{F}C_p$ 分解的一些结果。第 3 节致力于描述循环群 C_m 在代数 $\mathbb{F}C_p$ 上的作用。在第 4 节中，我们将 $\mathbb{F}_\ell^\alpha G$ 完全约化为简单分量。最后，在第 5 节中，我们给出 $\mathbb{F}_\ell^\alpha G$ 的完整 Wedderburn 分解；第 6 节则给出一些算例，以说明具体实例的 Wedderburn 分解。

2 预备知识

设 G 是一个有限群，A 是一个阿贝尔群。函数 $\alpha : G \times G \longrightarrow A$ 称为*2-余循环*，若对所有 $x, y, z \in G$，它满足

$$\alpha(x,y)\alpha(xy,z) = \alpha(y,z)\alpha(x,yz) \quad \text{and} \quad \alpha(x,1) = \alpha(1,x) = 1.$$

第一个条件称为余循环恒等式，第二个条件确保余循环的规范化。若 $t : G \longrightarrow A$ 是一个满足 $t(1) = 1$ 的映射，则由下式定义的函数 $\Delta(t) : G \times G \longrightarrow A$

$$\Delta(t)(x,y) = t(x)t(y)t(xy)^{-1}$$

称为*2-余边界*。我们用 $Z^2(G, A)$ 表示所有 2-余循环的集合，用 $B^2(G, A)$ 表示所有 2-余边界的集合。G 取值于 A 的**第二上同调群** 定义为

$$H^2(G, A) = Z^2(G, A)/B^2(G, A).$$

给定一个余循环 $\alpha \in Z^2(G, A)$，我们用 $[\alpha]$表示其上同调类。当阿贝尔群取为复数的乘法单位群 $\mathbb{C}^\times$时，我们将 G 的**舒尔乘子** 称为第二上同调群 $M(G) = H^2(G, \mathbb{C}^\times)$。

令 g 为 $C_n = \langle g \rangle$（阶为 n 的循环群）的生成元，并令 $\lambda \in \mathbb{F}_\ell^\times$。映射 $\alpha_\lambda : C_n \times C_n \longrightarrow \mathbb{F}_\ell^\times$ 定义如下：

$$\alpha_\lambda(g^i, g^j) = \begin{cases} 1, & \text{if } i + j < n, \\ \lambda, & \text{if } i + j \geq n. \end{cases}$$

是一个 2-余循环（参见 [10]），它表示与 λ 对应的上同调类，属于 $H^2(C_n,\ \mathbb{F}_\ell^\times) \cong \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^n$。

定义 2.1。设 $\alpha \in Z^2(G,\ \mathbb{F}_\ell^\times)$。扭群代数 $\mathbb{F}_\ell^\alpha G$ 定义为以 $\{u_g\}_{g\in G}$ 为基、定义在 $\mathbb{F}_\ell$ 上的向量空间，其乘法定义如下：

$$u_g u_h = \alpha(g,h)\, u_{gh} \quad \text{for all } g,h \in G.$$

且标量与基元素可交换，即 $u_g d = d u_g$ 对每个 $d \in \mathbb{F}_\ell$ 都成立。

定义 2.2（群 $G = C_p \rtimes_r C_m$）。设 p 是奇素数，m 是满足 $m \mid p-1$ 的正整数。固定一个阶为 m 的 $r \in (\mathbb{Z}/p\mathbb{Z})^\times$，定义

$$G = C_p \rtimes_r C_m = \langle a, b \mid a^p = 1,\ b^m = 1,\ bab^{-1} = a^r \rangle.$$

注意，C_m 对 C_p 的作用是忠实的，因为 $r \not\equiv 1$（模 p）。若该作用是平凡的，则 $G \cong C_p \times C_m$ 将是阿贝尔群；此情形下我们不作讨论。

从现在起，我们用 $\mathbb{F} = \mathbb{F}_\ell$ 表示含有 $\ell \neq p$ 个元素的有限域，用 $A = \mathbb{F}^\times$ 表示 $\mathbb{F}$ 的乘法群，并将其视为平凡的 G-模。

定理 2.3. 设 $G = C_p \rtimes C_m$，其中 $m \mid (p-1)$，且设 $\mathbb{F} = \mathbb{F}_\ell$ 是一个满足 $\ell \neq p$ 的有限域。*Then*

$$H^2(G, \mathbb{F}^\times) \cong H^2(C_m, \mathbb{F}^\times) \cong \mathbb{F}^\times/(\mathbb{F}^\times)^m.$$

证明。考虑与该扩张相关联的 Lyndon–Hochschild–Serre 谱序列

$$1 \longrightarrow C_p \longrightarrow G \longrightarrow C_m \longrightarrow 1,$$

其系数为 $A = \mathbb{F}^\times$，并赋予平凡的 G-作用，则

$$E_2^{i,j} = H^i(C_m, H^j(C_p, A)).$$

由于 $|A| = \ell - 1$ 且 $\gcd(p, \ell-1) = 1$，群 A 没有 p-扭元，因此，对于所有指标 $j \geq 1$，$H^j(C_p, A) = 0$（见推论 6.4）。因此，含有 $i + j = 2$ 的唯一非零项为

$$E_2^{2,0} = H^2(C_m, A).$$

由此可知，谱序列在第 E_2 页退化，且膨胀映射

$$\inf : H^2(C_m, A) \longrightarrow H^2(G, A)$$

是一个同构。最后，由于作用是平凡的，我们有 $H^2(C_m,\ \mathbb{F}^\times) \cong \mathbb{F}^\times/(\mathbb{F}^\times)^m$（参见[3, 第 III 章，第 6] 节）。 □

注 2.4。由于膨胀映射 $H^2(C_m,\ \mathbb{F}^\times) \longrightarrow H^2(G,\ \mathbb{F}^\times)$ 是一个同构，我们总可以选择一个代表 2-余循环 α 使得

$$\alpha|_{C_p \times C_p} = 1 \quad \text{and} \quad \alpha(c_p, c_m) = 1$$

对于所有的 $c_p \in C_p$ 和 $c_m \in C_m$。本文将始终采用这一规范化。

令 $\widehat{C_p} = \mathrm{Hom}(C_p, \mathbb{F}^\times)$ 表示 C_p的特征群。弗罗贝尼乌斯自同构 $\varphi : x \mapsto x^\ell$ 通过以下方式作用于 $\widehat{C_p}$

$$(\varphi \cdot \chi)(a) = \chi(a)^\ell = \chi(a^\ell), \quad \text{for all } a \in C_p.$$

由于 χ 的取值是单位根，这个作用只是置换这些特征标。

定义 2.5。 特征标 $\chi \in C_p$ 的弗罗贝尼乌斯轨道 是集合

$$\{\varphi^k \cdot \chi \mid k \geq 0\},$$

其中 φ 表示弗罗贝尼乌斯自同构。该轨道的大小 是 ℓ 模 χ的阶，即满足以下条件的最小正整数 f

$$\ell^f \equiv 1 \pmod{\mathrm{ord}(\chi)}.$$

命题 2.6。 群代数 $\mathbb{F}C_p$ 分解为

$$\mathbb{F}C_p \cong \bigoplus_{\mathcal{F}} \mathbb{F}(\chi_{\mathcal{F}}),$$

其中求和遍历非平凡特征标的弗罗贝尼乌斯轨道 $\mathcal{F}$，而 $\mathbb{F}(\chi_{\mathcal{F}})$ 表示由 $\mathbb{F}$ 的域扩张，该扩张由轨道中任一特征标的取值生成。对于平凡特征标，我们得到一份 $\mathbb{F}$。

证明。 这由以下事实可得:

$$\mathbb{F}C_p \cong \mathbb{F}[X]/\langle X^p - 1\rangle$$

以及 $X^p - 1$ 在 $\mathbb{F}$ 上分解为分圆多项式的情形。$\mathbb{F}C_p$ 的本原中心幂等元对应于 $\mathbb{F}$ 上不可约特征的伽罗瓦轨道（例如，参见 [19]）。 □

如果 f 是 ℓ 模 p 的阶，即满足 $p \mid \ell^f - 1$ 的最小正整数，那么我们有:

1. 平凡特征给出一个 1 维分量 $\mathbb{F}$。
2. 非平凡特征被划分为大小为 f 的弗罗贝尼乌斯轨道。
3. 此类轨道的数量为 $(p-1)/f$。

对于每个轨道，对应的单分量是域 $\mathbb{F}_{\ell^f}$。由此得到以下结果。

推论 2.7。 设群 C_p 如上所定义，

$$\mathbb{F}C_p \cong \mathbb{F} \oplus (\mathbb{F}_{\ell^f})^{(p-1)/f}.$$

3 C_m 对 $\mathbb{F}C_p$的作用

群 $C_m = \langle b \rangle$ 通过 $\sigma_b(u_a) = u_{a^r}$作用于代数 $\mathbb{F}C_p$。注意，如果在特征标层面考察这一作用，它对应于 $\chi \mapsto \chi^r$，其中 $\chi^r(a) = \chi(a)^r$。

引理 3.1。 C_m 的作用与 *Frobenius* 作用可交换。因此， C_m 置换特征的弗罗贝尼乌斯轨道。

证明。 对于任意特征 χ和任意 k，我们计算得

$$\varphi(\chi^r)(a) = (\chi^r(a))^\ell = (\chi(a)^r)^\ell = \chi(a)^{r\ell} = (\chi(a)^\ell)^r = (\varphi(\chi)(a))^r = (\varphi(\chi))^r(a).$$

因此， $\varphi \circ \sigma_b = \sigma_b \circ \varphi$ 作用于特征。 □

因此，群 C_m 在非平凡特征的弗罗贝尼乌斯轨道集合上有良定义的作用。设 $\mathcal{O}_1, \ldots, \mathcal{O}_s$ 为此作用的轨道， $t_j = |\mathcal{O}_j|$ 为轨道大小。对于每个C_m-轨道（其元素为弗罗贝尼乌斯轨道） $\mathcal{O}_j$ ， 令 e_j 为与 $\mathcal{O}_j$中所有弗罗贝尼乌斯轨道对应的本原幂等元之和，其中 $j = 1, \ldots, s$。

引理 3.2。 沿用上述记号，每个 e_j都是 $\mathbb{F}^\alpha G$ 中的中心幂等元，其中 $j = 1, \ldots, s$。

证明。由于 σ_b 置换 $\mathcal{O}_j$中的弗罗贝尼乌斯轨道，我们有 $\sigma_b(e_j) = e_j$。因此， e_j 与 u_b可交换。由于 α 在 $C_p \times C_p$上是平凡的，子代数 $\mathbb{F}C_p$ 是交换的，并且与自身对易。因此， e_j 与 $\mathbb{F}^\alpha G$中的所有元素都可交换。 □

设 $\mathcal{O}$ 是非平凡特征的弗罗贝尼乌斯轨道的一个 C_m-轨道。我们采用以下记号：

1. 每个弗罗贝尼乌斯轨道的大小为 $f = \mathrm{ord}_p(\ell)$。
2. C_m-轨道 $\mathcal{O}$ 包含 t 个这样的弗罗贝尼乌斯轨道。
3. 设 $K = \mathbb{F}_{\ell^f}$ 为对应于每个弗罗贝尼乌斯轨道的域。
4. 设 $H \subseteq C_m$ 为 $\mathcal{O}$中选定的一个弗罗贝尼乌斯轨道的稳定子，因此 $|H| = h = m/t$.

定义 3.3。 设 R 为一个环， G为一个有限群。设 G通过同态 $\sigma\colon G \longrightarrow \mathrm{Aut}(R)$ 以环自同构的方式作用于 R ，并设 $\alpha\colon G \times G \longrightarrow R^\times$ 为一个归一化二余循环。交叉积代数 $(R,\ G,\ \sigma,\ \alpha)$ 是一个 R-模

$$(R, G, \sigma, \alpha) = \bigoplus_{g \in G} R u_g$$

其乘法由下式确定：

$$\begin{aligned} u_g r &= \sigma_g(r)\, u_g, \qquad r \in R, \\ u_g u_h &= \alpha(g,h)\, u_{gh}, \qquad g, h \in G. \end{aligned}$$

这里， $\{u_g \mid g \in G\}$ 是由 G索引的形式基元素。 α 的余循环恒等式保证了结合律。

注 3.4. 本文中，我们会遇到以下类型的交叉积。

• $(R,\ C_m,\ \sigma,\ \alpha_\lambda)$ 表示循环群 $C_m = \langle b\rangle$ 通过 $\sigma: C_m \longrightarrow \mathrm{Aut}(R)$ 作用于代数R 所构成的交叉积，其余循环为 $\alpha_\lambda: C_m \times C_m \longrightarrow \mathbb{F}^\times$。其乘法满足

$$u_b r = \sigma_b(r)u_b, \qquad u_{b^i}u_{b^j} = \alpha_\lambda(b^i, b^j)u_{b^{i+j}}.$$

• $(K,\ H,\ \sigma|_H,\ \alpha|_H)$ 表示将作用和余循环限制到稳定子子群 $H \subseteq C_m$ 后得到的交叉积。因此

$$(K, H, \sigma|_H, \alpha|_H) = \bigoplus_{h\in H} Ku_h,$$

乘法定义为

$$u_h k = \sigma_h(k)u_h, \qquad u_h u_{h'} = \alpha(h, h')u_{hh'},$$

对于 $k \in K$ 和 $h,\ h' \in H$。

现在，根据轨道-稳定子定理，t 必须整除 m，且 $h = m/t$ 是一个正整数，因此中心幂等元 $e_{\mathcal{O}}$ 给出一个分量

$$A_{\mathcal{O}} = \mathbb{F}^\alpha G e_{\mathcal{O}} \cong (R, C_m, \sigma, \alpha_\lambda),$$

其中 $R = \mathbb{F}C_p e_{\mathcal{O}}$ 是一个交换半单代数。由于 $\mathcal{O}$ 包含 t 个弗罗贝尼乌斯轨道，每个轨道都贡献一个 K 的副本，因此我们有

$$R \cong \bigoplus_{i=1}^{t} K.$$

群 C_m 通过置换这 t 个副本而传递地作用于 R，每个副本的稳定子群为 H。稳定子 H 通过 $\mathbb{F}$- 代数自同构作用于选定的副本 K。由于 H 是循环群（作为 C_m 的子群），这一作用对应于伽罗瓦群 $\mathrm{Gal}(K/\mathbb{F}) \cong C_f$的一个子群。由于 σ_b^t 限制为 K 在 $\mathbb{F}_\ell$上的一个自同构，且 $\mathrm{Gal}(K/\mathbb{F}_\ell) \cong C_f$ 由弗罗贝尼乌斯自同构 $\varphi(\zeta) = \zeta^\ell$ 生成，因此存在唯一的 k (模 f)，使得

$$\sigma_b^t|_K = \varphi^k,$$

即，$r^t \equiv \ell^k$ （模 p），其中 φ 是弗罗贝尼乌斯自同构。于是，s 在伽罗瓦群$(K/\mathbb{F})$中的阶是满足以下条件的最小正整数：$(\sigma_b^t)^s = \varphi^{ks}$ 在 K上作用为恒等变换，即满足$\ell^{ks} \equiv 1$ （模 p）。

引理 3.5. 群 H 通过将自同构 σ_b^t 限制到 K 上而作用于 K。这给出了一个嵌入

$$H \hookrightarrow \mathrm{Gal}(K/\mathbb{F}) \cong C_f.$$

设 s是 σ_b^t在伽罗瓦群$(K/\mathbb{F})\cong C_f$中的阶。那么 s整除 h，s整除 f，且不动域 K^H的次数为 $[K^H : \mathbb{F}] = f/s$。

注 3.6. 条件 $s \mid h$ 和 $s \mid f$ 是由群论事实必然推出的结果。例如，如果 $f = 4$ 和 $h = 3$，那么 s 必须同时整除 3 和 4，这就意味着 $s = 1$ （平凡作用）。同样，如果 $f = 6$ 和 $h = 4$，那么 s 必须整除 $\gcd(4, 6) = 2$，因此 s 只能是 1 或 2。

4 分类

对于 t 为方便读者，我们总结了本节中使用的关键记号：

- $f = \mathrm{ord}_p(\ell)$：非平凡特征的每个弗罗贝尼乌斯轨道的大小。
- $K = \mathbb{F}_{\ell^f}$：与每个弗罗贝尼乌斯轨道对应的域。
- $t = |\mathcal{O}|$：弗罗贝尼乌斯轨道的一个 C_m-轨道的大小。
- $h = m/t$：$\mathcal{O}$ 中弗罗贝尼乌斯轨道的稳定子 H 的大小。
- s：σ_b^t 在 $\mathrm{Gal}(K/\mathbb{F}_\ell) \cong C_f$ 中的阶（因此 $s \mid \gcd(h, f)$）。
- $d = f/s = [K^H : \mathbb{F}_\ell]$：不动域的次数。
- $r = \sqrt{hs}$：矩阵大小参数（必须是整数）。
- $M_t(K)$：K 上的 $t \times t$ 矩阵代数。

我们回顾一些关于具有传递置换作用的交叉积的重要结构性结果。

定理 4.1 ([14])。设 $R = \bigoplus_{i=1}^{t} K$，其中 C_m 通过置换直和项传递地作用，并令 H 表示某个直和项的稳定子。那么

$$(R, C_m, \sigma, \alpha) \cong M_t\big((K, H, \sigma|_H, \alpha|_H)\big),$$

其中 $(K, H, \sigma|_H, \alpha|_H)$ 是 H 在 K 上的交叉积，具有该限制作用和余循环 .

在以下讨论中，我们设

$$B := (K, H, \sigma|_H, \alpha|_H),$$

这是一个以 $\mathbb{F}$ 为底的代数，并且

$$\dim_{\mathbb{F}} B = |H| \cdot \dim_{\mathbb{F}} K = h \cdot f.$$

命题 4.2。设 $B = (K, H, \sigma, \alpha)$ 是一个交叉积，其中 K 是一个域，且 H 通过域自同构作用。那么：

1. B 的中心是 $Z(B) = K^H$，即 H 在 K 上作用的不动域。*2.* B 是 K^H 上的中心单代数。*3.* 若 K 有限，则存在某个满足 $r^2 \cdot [K^H : \mathbb{F}] = h \cdot f$. 的正整数 r，使得 $B \cong M_r(K^H)$

证明。(1) 见 [14, 定理 4.4.1]。(2) 众所周知，交叉积是不动域上的中心单代数。(3) 由于有限域上的布劳尔群是平凡的（例如，参见 [19, 15]），每个有限域上的有限维中心单代数都同构于矩阵代数。关于维数的公式则可通过计算在 $\mathbb{F}$ 上的维数得到。

□

注 4.3。注意，等式 $r^2 = h \cdot s$ 对参数施加了一个非平凡的约束，可按如下方式推导。根据命题 4.2，$B \cong M_r(K^H)$ 是一个大小为 r、定义在 K^H 上的矩阵代数，因此它在 $\mathbb{F}_\ell$ 上的维数为

$$\dim_{\mathbb{F}_\ell} B = r^2 \cdot [K^H : \mathbb{F}_\ell] = r^2 \cdot d.$$

根据交叉积结构，我们还可以得到

$$\dim_{\mathbb{F}_\ell} B = |H| \cdot \dim_{\mathbb{F}_\ell} K = h \cdot f.$$

现在，由于 $d = f/s$（根据引理 3.5），令两个表达式相等可得

$$r^2 \cdot \mathbb{F}racfs = hf \quad \Longrightarrow \quad r^2 = h \cdot s.$$

因此，hs 必须是一个完全平方数，而 $r = \sqrt{h \cdot s}$ 是整数矩阵阶数。这并非额外假设，而是结构理论的必然结果：交叉积 B 是定义在 K^H 上的中心单代数，而有限域上的此类代数都是矩阵代数，因此 r 必须是正整数。因此，只有满足 $h \cdot s$ 为完全平方数的参数组合，才可能出现在有效的群作用中。

该条件与引理 3.5 中的 $s \mid \gcd(h,\ f)$ 一起，提供了强有力的约束，可排除许多不可能的参数组合，并为理论提供有用的一致性检查。

例 4.4。考虑 $m = 4$、$f = 6$，且稳定子作用的阶为 $s = 2$，那么根据 $t = 1$，我们有 $h = m/t = 4$，得到 $r = \sqrt{4 \cdot 2} = \sqrt{8}$，这不是一个整数。因此，这种配置不可能来自任何实际的群作用，参数 $(m,\ f,\ s) = (4,\ 6,\ 2)$ 彼此不相容。

由定理 4.1 和命题 4.2 可得

$$A_{\mathcal{O}} \cong M_t(B), \quad Z(A_{\mathcal{O}}) = Z(B) = K^H.$$

因此，

$$\dim_{\mathbb{F}} A_{\mathcal{O}} = t^2 \cdot \dim_{\mathbb{F}} B = t^2 \cdot h \cdot f = t^2 \cdot \mathbb{F}racmt \cdot f = t \cdot m \cdot f,$$

这与预期的维数一致

$$\dim_{\mathbb{F}} R \cdot m = (t \cdot f) \cdot m = t \cdot m \cdot f.$$

以下结果根据稳定子 H 及其在域 K 上的作用，对与中心幂等元 $e_{\mathcal{O}}$ 对应的分量 $A_{\mathcal{O}}$ 进行分类。

定理 4.5。设 $\mathcal{O}$ 是一组具有参数 f、t 的弗罗贝尼乌斯轨道的轨道，其稳定子为 H，阶为 $h = m/t$。设 s 为 σ_b^t 在伽罗瓦群 $\mathrm{Gal}(K/\mathbb{F}_\ell) \cong C_f$ 中的阶。定义

$$d = [K^H : \mathbb{F}_\ell] = f/s,$$
$$r = \sqrt{h \cdot s}.$$

那么：

1. 一般情形：$A_{\mathcal{O}} \cong M_{tr}(K^H)$，域 $K^H = \mathbb{F}_{\ell^d}$ 上的矩阵代数。

2. 特殊情形 $h = 1$：那么 $t = m$，H 是平凡的，$s = 1$，$d = f$，$r = 1$，且 $A_{\mathcal{O}} \cong M_m(K)$。当 C_m 在弗罗贝尼乌斯轨道上传递作用时，就会出现这种情况。

3. 特殊情形 $s = 1$: 那么 H 在 K上平凡作用，因此 $K^H = K$, $d = f$, $r = \sqrt{h}$，且 $A_{\mathcal{O}} \cong M_{t\sqrt{h}}(K)$。

4. 特殊情形 $t = 1$: 于是 $H = C_m$，因此整个群稳定一个弗罗贝尼乌斯轨道。在这种情况下， $A_{\mathcal{O}} \cong M_r(K^H)$，其中 $r = \sqrt{m \cdot s}$，其结构取决于 C_m 对 K 的作用是非平凡的（$s > 1$）还是平凡的（$s = 1$）。

在所有情形下， $A_{\mathcal{O}}$ 都是一个单代数，而 $\mathbb{F}^\alpha G$ 分解为简单分量的形式为

$$\mathbb{F}^\alpha G \cong \mathbb{F}^{\alpha_\lambda} C_m \oplus \bigoplus_{\mathcal{O}} A_{\mathcal{O}},$$

其中求和遍历所有非平凡弗罗贝尼乌斯轨道的 C_m-轨道。

注 4.6. 定理 4.5 中的分解涵盖了 C_m 对弗罗贝尼乌斯轨道的所有可能作用。要确定某个给定的群适用哪种情形，可以按照以下步骤进行:

- **步骤 1：计算** $f = \mathrm{ord}_p(\ell)$。这决定了每个弗罗贝尼乌斯轨道的大小以及域 $K = \mathbb{F}_{\ell^f}$。
- **步骤 2：确定弗罗贝尼乌斯轨道的数量**。该数量由 $N = (p-1)/f$ 给出。
- **步骤 3：分析** $C_m = \langle b \rangle$ **对弗罗贝尼乌斯轨道集合的作用**。元素 b 通过将特征标 χ 映射到 χ^r来作用，从而置换弗罗贝尼乌斯轨道。计算该此作用的轨道分解。设 $\mathcal{O}_1, \ldots, \mathcal{O}_u$ 为弗罗贝尼乌斯轨道在 C_m作用下的轨道，且其大小为 $t_1, \ldots, t_u$。注意 $\sum_{j=1}^{u} t_j = N$。
- **步骤 4：对于大小为** t_j**的每个轨道** $\mathcal{O}_j$ **，计算：**
  - $h_j = m/t_j$, the size of the stabilizer H_j of a Frobenius orbit in $\mathcal{O}_j$
  - s_j, the order of $\sigma_b^{t_j}|_K$ in $\mathrm{Gal}(K/\mathbb{F}_\ell) \cong C_f$
  - Verify the necessary conditions: $s_j \mid \gcd(h_j, f)$ (by Lemma 3.5)
  - Verify that $h_j s_j$ is a perfect square (by Remark 4.3)
  - Compute $d_j = f/s_j$ and $r_j = \sqrt{h_j s_j}$
- **第 5 步：确定适用的特殊情形：**

  – 如果 $t_j = m$，则 $h_j = 1$: 这是传递情形，得到 $A_{\mathcal{O}_j} \cong M_m(K)$– 如果 $t_j = 1$，则 $h_j = m$: 这是不动点情形，得到 $A_{\mathcal{O}_j} \cong M_{r_j}(K^{H_j})$，其中$r_j = \sqrt{m s_j}$– 如果 $1 < t_j < m$，则我们得到一个非平凡的中间情形，其中有 $1 < h_j < m$

请注意，这些参数必须满足所有一致性条件；不可能的组合（例如违反 $s_j \mid \gcd(h_j, f)$ 或完全平方条件的组合）不可能出现在任何有效的群作用中。

推论 4.7. 对于每个 C_m-轨道 $\mathcal{O}_j$，相应单分量的维数为

$$\dim_{\mathbb{F}_\ell} A_{\mathcal{O}_j} = (t_j \cdot r_j)^2 \cdot d_j = t_j^2 \cdot h_j s_j \cdot \mathbb{F}racf s_j = t_j^2 \cdot h_j \cdot f = t_j \cdot m \cdot f.$$

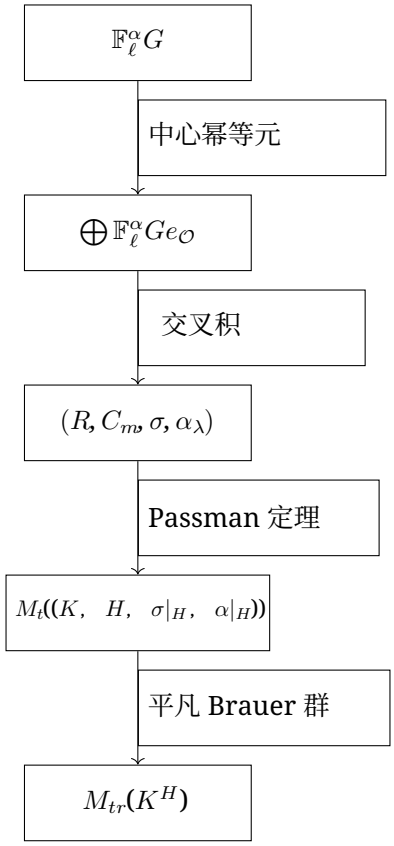


图 1：将 $\mathbb{F}_\ell^\alpha G$ 约化为简单分量

注意，对所有轨道求和，并加上由 $\mathbb{F}^{\alpha_\lambda} C_m$ 给出的交换分量（维数为 m），可得

$$\dim_{\mathbb{F}_\ell} \mathbb{F}^\alpha G = m + \sum_{j=1}^{u} t_j \cdot m \cdot f = m \cdot \left(1 + f \sum_{j=1}^{u} t_j\right) = m\,(1 + f \cdot \mathbb{F}racp - 1f) = m \cdot p = |G|,$$

这证实了该分解保持维数不变。图 1 展示了从扭群代数逐步约化为其简单分量的过程。

5 完整的 Wedderburn 分解

现在我们以明确的形式给出 $\mathbb{F}_\ell^\alpha G$ 的完整 Wedderburn 分解。我们先分析来自 C_p 的平凡特征的分量，然后提供总结所有情形的表格。对应于 C_p 的平凡特征的分量为

$$A_0 = \mathbb{F}_\ell^\alpha G e_{\mathrm{triv}} \cong \mathbb{F}_\ell^{\alpha_\lambda} C_m.$$

这是循环群 C_m 的扭群代数。其结构取决于 $\lambda \in \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^m$ 和域 $\mathbb{F}_\ell$。

命题 5.1。令 $\lambda \in \mathbb{F}_\ell^\times$ 表示 $\mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^m$ 中的一个上同调类。那么

$$\mathbb{F}_\ell^{\alpha_\lambda} C_m \cong \bigoplus_{d|m} \mathbb{F}_{\ell^d}^{\oplus a_d(\lambda)},$$

其中 $a_d(\lambda)$ 的确定方式如下

1. 若 $\lambda \in (\mathbb{F}_\ell^\times)^m$，则 α_λ 与平凡余循环上同调等价，且 $\mathbb{F}_\ell^{\alpha_\lambda} C_m \cong \mathbb{F}_\ell C_m \cong \bigoplus_{d|m} \mathbb{F}_{\ell^d}^{\oplus \varphi(d)}$，其中 φ 是欧拉函数。*2.* 否则，令 s 为 $\mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^m$ 中 λ 的阶。那么 $\mathbb{F}_\ell^{\alpha_\lambda} C_m \cong \mathbb{F}_{\ell^{m/s}} \oplus \bigoplus_{d|m,\ d\nmid m/s} \mathbb{F}_{\ell^d}^{\oplus b_d}$，其中重数 b_d 取适当值（精确公式见 *[11]*）。

为简化表格中的表示，我们将交换分量记为 $C(\lambda)$，其维数为 $\dim C(\lambda) = m$。对于每个由非平凡特征的弗罗贝尼乌斯轨道构成的 C_m-轨道 $\mathcal{O}$，我们需要计算

- $f = \mathrm{ord}_p(\ell)$
- $t = |\mathcal{O}|$：弗罗贝尼乌斯轨道的 C_m-轨道大小
- $h = m/t$：稳定子的大小
- $K = \mathbb{F}_{\ell^f}$
- s：σ_b^t 在伽罗瓦群 $\mathrm{Gal}(K/\mathbb{F}_\ell)$ 中的阶 $\cong C_f$（注意，根据引理 3.5，$s \mid \gcd(h, f)$）
- $d = f/s$：不动域的次数
- $r = \sqrt{h \cdot s}$：一个正整数（参见注 4.3）

定理 5.2 (完整 Wedderburn 分解)。设 $G = C_p \rtimes_r C_m$ 满足 $m \mid p-1$、$\ell \neq p$，且令 $f = \text{阶}_p(\ell)$。假设 C_m 对 C_p 的非平凡特征的弗罗贝尼乌斯轨道集合的作用将它们划分为轨道 $\mathcal{O}_1$、……、$\mathcal{O}_u$，其大小分别为 t_1、……、t_u。对于每个轨道 $\mathcal{O}_j$，令 $h_j = m/t_j$，令 $H_j \cong C_{h_j}$ 为稳定子，令 $K = \mathbb{F}_{\ell^f}$，并令 s_j 为 $\sigma_b^{t_j}$ 在伽罗瓦群 $(K/\mathbb{F}_\ell) \cong C_f$ 中的阶。定义

$$d_j = [K^{H_j} : \mathbb{F}_\ell] = f/s_j,$$
$$r_j = \sqrt{\mathbb{F}rach_j \cdot fd_j} = \sqrt{h_j \cdot s_j}.$$

则 $\mathbb{F}_\ell^\alpha G$ 的韦德伯恩分解为

$$\mathbb{F}_\ell^\alpha G \cong \mathbb{F}_\ell^{\alpha_\lambda} C_m \oplus \bigoplus_{j=1}^{u} M_{t_j \cdot r_j}(\mathbb{F}_{\ell^{d_j}}),$$

其中，$\mathbb{F}_\ell^{\alpha_\lambda} C_m$ 是命题 *5.1* 中描述的交换分量。此外，

$$\dim_{\mathbb{F}_\ell} \mathbb{F}_\ell^\alpha G = \dim_{\mathbb{F}_\ell} \mathbb{F}_\ell^{\alpha_\lambda} C_m + \sum_{j=1}^{u} (t_j \cdot r_j)^2 \cdot d_j = p \cdot m = |G|.$$

5.1 显式表

现在我们给出韦德伯恩分解的显式表。这些表按 C_m 对弗罗贝尼乌斯轨道的作用结构以及稳定子的伽罗瓦作用进行编排。

在表1、表2、表3和表 4中，参数必须满足约束$s \mid \gcd(h, f)$，且 hs 为完全平方数。注意，表2得出了 [8, 定理 12]中的结果。当 f 为奇数时， $2 \nmid f$，因此伽罗瓦群 Gal($K/\mathbb{F}$) 中唯一的 2 阶元素不能在 K 上非平凡地作用，从而迫使 $s = 1$成立。当 f 为偶数时， C_2 可以置换这两个弗罗贝尼乌斯轨道。

t	h	s	$d = f/s$	K^H	r	分量
1	m	1	f	$\mathbb{F}_{\ell^f}$	$\sqrt{m}$	$M_m(\mathbb{F}_{\ell^f})$
1	m	$s > 1$	f/s	$\mathbb{F}_{\ell^{f/s}}$	$\sqrt{ms}$	$M_m(\mathbb{F}_{\ell^{f/s}})$
m	1	1	f	$\mathbb{F}_{\ell^f}$	1	$M_m(\mathbb{F}_{\ell^f})$
t	m/t	1	f	$\mathbb{F}_{\ell^f}$	$\sqrt{m/t}$	$M_{t\sqrt{m/t}}(\mathbb{F}_{\ell^f})$
t	m/t	$s > 1$	f/s	$\mathbb{F}_{\ell^{f/s}}$	$\sqrt{(m/t)s}$	$M_{t\sqrt{(m/t)s}}(\mathbb{F}_{\ell^{f/s}})$

表1：弗罗贝尼乌斯轨道的 C_m-轨道的一般参数

注5.3。

- $r = \sqrt{hs}$ 为整数这一条件对参数施加了约束。例如，当 $m = 4$时， $h = 4$会得到 $r = \sqrt{8}$，而这不是整数。这种情形不可能出现，因为交叉积理论保证 r 是整数。因此，这类参数组合是不可能的，也提供了一致性检查。

- 类似地，条件 $s \mid f$ 排除了 s 不能整除 f的情形，例如当 $f = 4$时的 $s = 3$ 。

注 5.4。

- 表3的第一行要求 $3 \mid f$ ，并且 b 通过 $\chi \mapsto \chi^r$对特征的作用在伽罗瓦群 Gal($K/\mathbb{F}_\ell$) 中的阶为 3，即 $r^3 \equiv 1$ （模 p）（由于 $m = 3$，这自动成立），且 r 不是 ℓ 的幂，否则会得到更小的阶。当 $r \equiv \ell^k$ （模 p）时会出现这种情况，其中 k 满足 $3k \equiv 0$ （模 f）且 $k \not\equiv 0$ （模 $f/3$）。

- 表3的第二行出现在 C_3 将三个弗罗贝尼乌斯轨道传递地置换时，因此 $t = 3$、 $h = 1$，且对 K 的稳定子作用是平凡的（$s = 1$）。这要求三个弗罗贝尼乌斯轨道属于不同的 C_3-轨道，即 b 的作用将它们循环置换。

- 表 4 的第二行要求 $4 \mid f$ ，并且 b 通过 $\chi \mapsto \chi^r$ 对特征的作用在伽罗瓦群 $K/\mathbb{F}_\ell$ 中的阶为 4，即 $r^4 \equiv 1$ (模 p)、 $r^2 \not\equiv 1$ (模 p) 和 $r \equiv \ell^k$ (模 p)，其中 k 满足 $4k \equiv 0$ (模 f) 和 $k \not\equiv 0$ (模 $f/4$)。

- 表 4 的第三行要求 f 为偶数但不能被 4 整除，并且稳定子在K 上的作用的阶为 2，即 $r^2 \equiv 1 \pmod{p}$，但不满足 $r \not\equiv 1 \pmod{p}$；且 $r \equiv \ell^k \pmod{p}$，其中 k 满足$2k \equiv 0 \pmod{f}$，而 $k \not\equiv 0 \pmod{f/2}$。在这种情形下， C_4-轨道的大小为 $t = 2$，因为该作用将弗罗贝尼乌斯轨道两两配对。

f	作用	t	h	s	d	分量
odd	C_2 固定轨道	1	2	1	f	$M_2(\mathbb{F}_{\ell^f})$
even	C_2 成对置换	2	1	1	f	$M_2(\mathbb{F}_{\ell^f})$

表2：情形 $m = 2$ （二面体群）

条件	t	h	s	d	r	分量
$3 \mid f$, $s = 3$ （完全伽罗瓦作用）	1	3	3	$f/3$	3	M_3（$\mathbb{F}_{\ell^{f/3}}$）
f 任意，（平凡作用）	3	1	1	f	1	$M_3(\mathbb{F}_{\ell^f})$

表3：情形 $m = 3$

条件	t	h	s	d	r	分量
$4 \mid f$, $s = 1$ (平凡作用)	1	4	1	f	2	$M_4(\mathbb{F}_{\ell^f})$
$4 \mid f$, $s = 4$ (完全伽罗瓦作用)	1	4	4	$f/4$	4	$M_4(\mathbb{F}_{\ell^{f/4}})$
f 偶数，$4 \nmid f$, $s = 2$	2	2	2	$f/2$	2	$M_4(\mathbb{F}_{\ell^{f/2}})$
f 任意，$s = 1$ (传递)	4	1	1	f	1	$M_4(\mathbb{F}_{\ell^f})$

表 4：情形 $m = 4$

- 表 4 的第四行对应于 C_4 传递地置换这四个弗罗贝尼乌斯轨道的情形，因此$t = 4$、 $h = 1$，且稳定子作用是平凡的（$s = 1$）。这要求这四个弗罗贝尼乌斯轨道属于不同的 C_4-轨道；也就是说， b的作用以循环方式置换它们。

6 个示例

现在我们给出一些示例，以说明完整 Wedderburn 分解。前四个示例中， $\mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^m$ 平凡，因此 α 在上同调意义下是平凡的；示例 6.5 展示了一个具有非平凡余循环的情形。

示例 6.1. 令 $p = 7$, $m = 3$, $\ell = 2$, $r = 2$ （模 7 的阶为 3，因为 $2^3 = 8 \equiv 1$）。

首先，计算 $\mathbb{F}_2^\times = \{1\}$。由于这个群是平凡的， $\mathbb{F}_2^\times/(\mathbb{F}_2^\times)^3 = \{1\}$。因此，所有余循环在上同调意义下都是平凡的，并且 $\mathbb{F}_2^\alpha G \cong \mathbb{F}_2 G$。

现在分析群代数结构。

- 计算 $f = \mathrm{ord}_7(2)$： $2^3 \equiv 1$ (模 7)。因此 $f = 3$，且 $K = \mathbb{F}_{2^3} = \mathbb{F}_8$。
- 非平凡特征的弗罗贝尼乌斯轨道数量（$p - 1$）$/f = 6/3 = 2$。
- C_3的作用： σ_b 通过 $\zeta \mapsto \zeta^2$ 作用于 K ，由此生成伽罗瓦群 $\mathrm{Gal}(K/\mathbb{F}_2) \cong C_3$。因此 $s = 3$ 是稳定子的情况。
- 这两个弗罗贝尼乌斯轨道是

  −轨道 1：指数为 $\{1, 2, 4\}$ 的特征标（因为 $1 \cdot 2 = 2$、 $2 \cdot 2 = 4$、 $4 \cdot 2 = 8 \equiv 1$）−轨道 2：指数为 $\{3, 6, 5\}$ 的特征标（因为 $3 \cdot 2 = 6$、 $6 \cdot 2 = 12 \equiv 5$、 $5 \cdot 2 = 10 \equiv 3$）

由于 2 生成模 7 乘法群，弗罗贝尼乌斯轨道恰好是指数之间相差 2 的幂次倍数的集合，而乘以 $r = 2$ 会在这些轨道内置换元素。

- C_3 固定每个弗罗贝尼乌斯轨道。因此，对于每个轨道 $t = 1$, $h = 3$, $s = 3$, $d = f/s = 1$, $r = \sqrt{hs} = \sqrt{9} = \overline{3}$。
- 每个分量都是 $M_3(\mathbb{F}_2)$（因为 $d = 1$ 给出 $K^H = \mathbb{F}_2$）。

交换分量 $\mathbb{F}_2C_3 \cong \mathbb{F}_2 \oplus \mathbb{F}_4$，其维数为 $1 + 2 = 3$。因此，完整 Wedderburn 分解为

$$\mathbb{F}_2G \cong \mathbb{F}_2 \oplus \mathbb{F}_4 \oplus M_3(\mathbb{F}_2) \oplus M_3(\mathbb{F}_2).$$

维数验证 $1 + 2 + 9 + 9 = 21 = 7 \cdot 3 = pm$。

例6.2。设 $p = 11$, $m = 5$, $\ell = 2$，并选择 $r = 4$，它模 11 的阶为 5（因为$4^5 = 1024 \equiv 1$）。

首先，计算 $\mathbb{F}_2^\times = \{1\}$，因此 $\mathbb{F}_2^\times/(\mathbb{F}_2^\times)^5 = \{1\}$。所以所有余循环都是平凡的，并且 $\mathbb{F}_2^\alpha G \cong \mathbb{F}_2 G$.

- 计算 $f = \mathrm{ord}_{11}(2)$: $2^{10} \equiv 1 \pmod{11}$，因此 $f = 10$，且 $K = \mathbb{F}_{2^{10}}$。
- 非平凡特征的弗罗贝尼乌斯轨道数：$(p-1)/f = 10/10 = 1$。
- 唯一的弗罗贝尼乌斯轨道包含全部 10 个非平凡特征。

- 带有 $r = 4$ 的 C_5 作用： σ_b 将 ζ 映射到 ζ^4。我们需要求 σ_b 在 $\mathrm{Gal}(K/\mathbb{F}_2) \cong C_{10}$ 中的阶。弗罗贝尼乌斯自同构 φ 生成 $\mathrm{Gal}(K/\mathbb{F}_2)$，且 $\varphi(\zeta) = \zeta^2$。求解 $2^k \equiv 4 \pmod{11}$: $2^2 = 4$，因此 $k = 2$。于是 $\sigma_b = \varphi^2$，其阶为 $10/\gcd(10,\ 2) = 10/2 = 5$。
- 因此 $s = 5$, $d = f/s = 10/5 = 2$，所以 $K^H = \mathbb{F}_{2^2} = \mathbb{F}_4$。
- $t = 1$, $h = 5$, $r = \sqrt{h \cdot s} = \sqrt{5 \cdot 5} = 5$。
- 分量： $M_5(\mathbb{F}_4)$。

交换分量 $\mathbb{F}_2C_5 \cong \mathbb{F}_2 \oplus \mathbb{F}_{16}$，维数为 $1 + 4 = 5$。因此

$$\mathbb{F}_2G \cong \mathbb{F}_2 \oplus \mathbb{F}_{16} \oplus M_5(\mathbb{F}_4).$$

维数检验 $1 + 4 + 25 \cdot 2 = 1 + 4 + 50 = 55 = 11 \cdot 5 = p \cdot m$。

例6.3。设 $p = 11$, $m = 5$, $\ell = 3$，且 $r = 4$ （模 11 的阶为 5）。

首先，计算 $\mathbb{F}_3^\times = \{1, 2\}$，这是一个阶为 2 的循环群。由于 $\gcd(5,\ 2) = 1$，映射 $x \mapsto x^5$ 是 $\mathbb{F}_3^\times$ 的一个自同构。因此 $(\mathbb{F}_3^\times)^5 = \mathbb{F}_3^\times$，并且

$$\mathbb{F}_3^\times/(\mathbb{F}_3^\times)^5 = \{1\}.$$

因此，所有余循环都是上同调平凡的，并且 $\mathbb{F}_3^\alpha G \cong \mathbb{F}_3 G$。

- 计算 $f = \mathrm{ord}_{11}(3)$: $3^5 \equiv 1 \pmod{11}$（因为 $3^5 = 243 = 22 \cdot 11 + 1$），所以 $f = 5$，且 $K = \mathbb{F}_{3^5}$。

- 非平凡特征的弗罗贝尼乌斯轨道数：$(p-1)/f = 10/5 = 2$。
- 这两个弗罗贝尼乌斯轨道是：

  $-$轨道 A：指数为 $\{1,3,9,5,4\}$ 的特征（因为 $1\cdot 3 = 3$, $3\cdot 3 = 9$, $9\cdot 3 = 27 \equiv 5$, $5\cdot 3 = 15 \equiv 4$, $4\cdot 3 = 12 \equiv 1$）$-$轨道 B：指数为 $\{2,6,7,10,8\}$ 的特征（因为 $2\cdot 3 = 6$, $6\cdot 3 = 18 \equiv 7$,$7\cdot 3 = 21 \equiv 10$, $10\cdot 3 = 30 \equiv 8$, $8\cdot 3 = 24 \equiv 2$）

- 当 C_5 具有 $r = 4$ 时的作用：乘以 4 会固定每个轨道。
- 因此，对于每个轨道： $t = 1$, $h = 5$。
- σ_b 通过 $\zeta \mapsto \zeta^4$作用于 K 。由于 $\mathrm{Gal}(K/\mathbb{F}_3) \cong C_5$ 由 $\varphi(\zeta) = \zeta^3$生成，并且 $4 \equiv 3^2$（模 11）按指数相乘， $\sigma_b = \varphi^2$，其阶也为 5。因此 $s = 5$。
- $d = f/s = 5/5 = 1$，所以 $K^H = \mathbb{F}_3$。
- $r = \sqrt{h\cdot s} = \sqrt{5\cdot 5} = 5$。
- 每个分量： $M_5(\mathbb{F}_3)$。

交换分量 $\mathbb{F}_3 C_5 \cong \mathbb{F}_3 \oplus \mathbb{F}_{81}$，维数为 $1+4=5$。因此

$$\mathbb{F}_3 G \cong \mathbb{F}_3 \oplus \mathbb{F}_{81} \oplus M_5(\mathbb{F}_3) \oplus M_5(\mathbb{F}_3).$$

维数检验 $1+4+25+25 = 55 = 11\cdot 5 = p\cdot m$。

例 6.4。 令 $p = 13, m = 3, \ell = 2, r = 3$ （模 13 的阶为 3，因为 $3^3 = 27 \equiv 1$）。首先，计算 $\mathbb{F}_2^\times = \{1\}$，因此 $\mathbb{F}_2^\times/(\mathbb{F}_2^\times)^3 = \{1\}$。所以所有余循环都是平凡的，且 $\mathbb{F}_2^\alpha G \cong \mathbb{F}_2 G$。

- 计算 $f = \mathrm{ord}_{13}(2)$： $2^{12} \equiv 1$ （模 13），因此 $f = 12$，且 $K = \mathbb{F}_{2^{12}}$。
- 非平凡特征的弗罗贝尼乌斯轨道数：$(p-1)/f = 12/12 = 1$。
- 这一个弗罗贝尼乌斯轨道包含全部 12 个非平凡特征。
- 当 $r = 3$ 时， C_3 的作用： σ_b 将 ζ 映射到 ζ^3。我们需要确定 σ_b 在伽罗瓦群 $(K/\mathbb{F}_2) \cong C_{12}$ 中的阶。
- 弗罗贝尼乌斯自同构 φ 生成伽罗瓦群 $\mathrm{Gal}(K/\mathbb{F}_2)$，其中 $\varphi(\zeta) = \zeta^2$。求解 $2^k \equiv 3 \pmod{13}$： $2^4 = 16 \equiv 3$，因此 $k = 4$。于是 $\sigma_b = \varphi^4$，其阶为 $12/\gcd(12, 4) = 12/4 = 3$。
- 因此 $s = 3$, $d = f/s = 12/3 = 4$，所以 $K^H = \mathbb{F}_{2^4} = \mathbb{F}_{16}$。
- $t = 1$, $h = 3$, $r = \sqrt{h\cdot s} = \sqrt{3\cdot 3} = 3$。
- 分量： $M_3(\mathbb{F}_{16})$。

交换分量 $\mathbb{F}_2 C_3 \cong \mathbb{F}_2 \oplus \mathbb{F}_4$，其维数为 $1+2=3$。因此

$$\mathbb{F}_2 G \cong \mathbb{F}_2 \oplus \mathbb{F}_4 \oplus M_3(\mathbb{F}_{16}).$$

维数检查 $1+2+9\cdot 4 = 1+2+36 = 39 = 13\cdot 3 = p\cdot m$。

例 6.5（非平凡余循环）。令 $p = 7$、$m = 3$、$\ell = 13$ 和 $r = 2$（其模 7 的阶为 3，因为 $2^3 = 8 \equiv 1$（模 7））。注意，$\ell = 13$ 与 $p = 7$ 互素，因此半单性成立。

首先，计算 $\mathbb{F}_{13}^{\times} \cong C_{12}$。映射 $x \mapsto x$ 在 C_{12} 上的核大小为 $\gcd(3, 12) = 3$，因此 $(\mathbb{F}_{13}^{\times})^3$ 是 C_{12} 中唯一的指数为 3 的子群，且同构于 C_4。于是

$$\mathbb{F}_{13}^{\times}/(\mathbb{F}_{13}^{\times})^3 \cong C_3,$$

一个阶为 3 的非平凡群。令 λ 为 $\mathbb{F}_{13}^{\times}/(\mathbb{F}_{13}^{\times})^3$ 中一个非平凡上同调类的代表元。那么 $\mathbb{F}_{13}^{\alpha_\lambda} C_3$ 是 C_3 的扭群代数。由于根据命题 5.1，$\lambda \notin (\mathbb{F}_{13}^{\times})^3$，，所以 $\mathbb{F}_{13}^{\alpha_\lambda} C_3 \cong \mathbb{F}_{13^3} = \mathbb{F}_{2197}$（一个关于 $\mathbb{F}_{13}$ 的 3 次扩张域）。

现在分析代数的其余部分

- 计算 $f = \mathrm{ord}_7(13)$：$13 \equiv 6$（模 7），且 $6^2 = 36 \equiv 1$（模 7），因此 $f = 2$。于是 $K = \mathbb{F}_{13^2} = \mathbb{F}_{169}$，且伽罗瓦群 $\mathrm{Gal}(K/\mathbb{F}_{13}) \cong C_2$，由弗罗贝尼乌斯自同构 $\varphi(\zeta) = \zeta^{13} = \zeta^{-1}$ 生成（因为 $13 \equiv -1$（模 7））。
- 非平凡特征的弗罗贝尼乌斯轨道数：$(p-1)/f = 6/2 = 3$。因此共有三个弗罗贝尼乌斯轨道，每个轨道的大小为 $f = 2$，对应于域 $K = \mathbb{F}_{169}$。
- 对 $C_3 = \langle b \rangle$ 的作用（取 $r = 2$）：在特征上，σ_b 将 χ 映到 χ^2，即对于本原七次单位根 ζ，有 $\sigma_b(\zeta) = \zeta^2$。
- 我们需要确定 C_3 如何作用于这三个弗罗贝尼乌斯轨道。有两种可能：
  - 情形 1（不动点）：C_3 分别固定每个弗罗贝尼乌斯轨道。于是，对于每个轨道，$t = 1$（在 C_3 作用下的轨道大小）和 $h = m/t = 3$（稳定子大小）。对于一个固定轨道，稳定子 $H = C_3$ 通过 $\sigma_b|_K$ 作用于 K。但 $\mathrm{Gal}(K/\mathbb{F}_{13}) \cong C_2$ 的阶为 2，因此 K 在 $\mathbb{F}_{13}$ 上的任意自同构的阶只能为 1 或 2。自同构 $\sigma_b|_K$ 将 $\zeta \mapsto \zeta^2$ 映到 $K/\mathbb{F}_{13}$。要属于 $\mathrm{Gal}(K/\mathbb{F}_{13})$，它必须满足 $2 \equiv 13^k$（模 7），其中某个 k 满足条件。由于 $13 \equiv -1$（模 7），$13^k \equiv (-1)^k$，其值要么为 1（若 k 为偶数），要么为 6（若 k 为奇数）。两者都不等于 2，因此 $\sigma_b|_K$ 不属于 $\mathrm{Gal}(K/\mathbb{F}_{13})$。然而，$\sigma_b$ 在 K 上的限制必须是 K 在 $\mathbb{F}_{13}$ 上的域自同构，这就产生了矛盾。因此这种情形不可能发生。更系统地说：对于一个固定轨道，我们需要 s，即 $\sigma_b|_K$ 在 $\mathrm{Gal}(K/\mathbb{F}_{13})$ 中的阶，同时整除 $h = 3$ 和 $f = 2$。因此 $s \mid \gcd(3, 2) = 1$，这迫使 $s = 1$ 成立。于是 $r = \sqrt{hs} = \sqrt{3}$ 不是整数，与 r 必须为整数这一要求矛盾（注 4.3）。因此情形 1 不可能发生。– 情形 2（传递作用）：C_3 传递地置换这三个弗罗贝尼乌斯轨道。于是 $t = 3$（这三个轨道构成单个 C_3 轨道），$h = m/t = 1$（平凡稳定子）。由于 H 平凡，它在 K 上的作用也是平凡的，因此 $s = 1$。于是 $d = f/s = 2$，所以 $K^H = K = \mathbb{F}_{169}$。由于 $h = 1$ 和 $s = 1$，我们有 $r = \sqrt{hs} = 1$，而该分量为 $M_{tr}(K^H) = M_3(\mathbb{F}_{169})$。
- 因此，这三个弗罗贝尼乌斯轨道构成一个大小为 $t = 3$ 的单一 C_3-轨道，其稳定子作用是平凡的。

因此，完整 Wedderburn 分解为

$$\mathbb{F}_{13}^{\alpha_\lambda} G \cong \mathbb{F}_{2197} \oplus M_3(\mathbb{F}_{169}).$$

我们可以检验维数 $\dim \mathbb{F}_{2197} = 3$ 和 $\dim\ M_3(\mathbb{F}_{169}) = 3^2 \cdot 2 = 9 \cdot 2 = 18$。注意，总和为 $3 + 18 = 21 = 7 \cdot 3 = p \cdot m = |G|$，这证实了该分解。

7 结论

我们为有限域上忠实分裂元循环群的扭曲群代数建立了一套完整理论。主要结果如下

- 完整计算 $H^2(G,\ \mathbb{F}^\times) \cong \mathbb{F}^\times/(\mathbb{F}^\times)^m$ （定理 2.3），表明所有扭曲都发生在 C_m 因子上，并且可以假设余循环在 C_p上的限制是平凡的。
- 在弗罗贝尼乌斯自同构作用下，将 $\mathbb{F}C_p$ 分解为弗罗贝尼乌斯轨道（命题 2.6）。
- 通过 C_m 对这些轨道的作用，确定本原中心幂等元（引理 3.2）。
- 利用交叉积进行结构约化（定理 4.1），并精确描述中心，同时纳入稳定子的伽罗瓦作用（命题 4.2、引理 3.5），且给出明确约束： $s \mid \gcd(h,\ f)$，以及 hs 为完全平方数（注释 3.6 和 4.3）。
- 完整分类了所有情形中的简单分量，并给出明确参数 t, h, s, d 和 r （定理 4.5）。
- 韦德伯恩分解的显式表（表 1–4），剔除了所有不可能的参数组合，并附有说明性脚注。
- 完整 Wedderburn 分解 $\mathbb{F}_\ell^\alpha G \cong \mathbb{F}_\ell^{\alpha_\lambda} C_m \oplus \bigoplus_{j=1}^{u} M_{t_j r_j}(\mathbb{F}_{\ell^{d_j}})$，（定理 5.2），其中所有参数均由 p、 m、 ℓ 和 r 明确确定，且 $\dim\ = pm = |G|$。

此外，我们还提供了说明性示例，包括一个具有非平凡余循环的扭群代数情形（例 6.5），突显了扭交换分量及其参数约束。

参考文献

[1] Angelot Behajaina、Martino Borello、Javier de la Cruz 和 Wolfgang Willems。扭斜 g-码。*Designs, Codes and Cryptography*，92:1803–1821，2024。[2] Jos´e Joaqu´ın Bernal、Angel del R´ıo 和 Juan Jacobo Sim´on。群码的内在描述。*Des. Codes Cryptogr.*，51(3):289–300，2009。[3] Kenneth S. Brown。群的上同调，第87卷，载于*Graduate Texts in Mathematics*。Springer-Verlag，纽约，1994。1982年原版的修订重印本。[4] Javier de la Cruz 和 Ricardo Villanueva-Polanco。基于扭曲二面体群代数的公钥密码学。*Adv. Math. Commun.*，18(3):857–877，2024。

[5] Javier de la Cruz 和 Wolfgang Willems。扭群码。IEEE 信息论汇刊，67(8):5178–5184，2021。[6] A. Duarte、A. Pereira 和 C. Polcino Milies。交叉积码。J. Algebra Appl.，23(8):论文编号2550045，12，2024。[7] A. Duarte 和 C. Polcino Milies。阿贝尔群的扭群代数：综述。载于《代数结构与应用》，Contemp. Math. 第826卷，第325–339页。美国数学会，[普罗维登斯], 罗得岛州，[2025] ©2025。[8] Andr´e Duarte。有限域上二面体群的扭群代数。Finite Fields Appl.，112:论文编号102792，2026。[9] Yun Fan 和 Yue Leng。Consta-二面体码及其渐近性质。IEEE 信息论汇刊，71(9):6785–6800，2025。[10] Nathan Jacobson。《抽象代数讲义》第III卷：域论与伽罗瓦理论。D. Van Nostrand Co., Inc.，普林斯顿、新泽西州—多伦多、安大略省—伦敦—纽约，1964。[11] Gregory Karpilovsky。群表示。第2卷，North-Holland Mathematics Studies 第177卷。North-Holland Publishing Co.，阿姆斯特丹，1993。[12] Leo Margolis 和 Ofir Schnabel。域上的扭群环同构问题。Israel J. Math.，238(1):209–242，2020。[13] Consuelo Mart´ınez 和 Fabi´an Molina。群码中的伴随式译码算法。Finite Fields Appl.，89:论文编号102206，17，2023。[14] Donald S. Passman。无限交叉积，Pure and Applied Mathematics 第135卷。Academic Press, Inc.，波士顿，MA，1989。[15] Richard S. Pierce。结合代数，Studies in the History of Modern Science 第9卷。Springer-Verlag，纽约—柏林，1982。Graduate Texts in Mathematics，第88卷。.[16] I. Schur。《关于有限群通过分式线性变换的表示》。J. Reine Angew. Math.，127:20–50，1904。[17] I. Schur。《关于有限群通过分式线性变换的表示的研究》。J. Reine Angew. Math.，132:85–137，1907。.[18] I. Schur。《关于对称群和交错群通过分式线性变换的表示》。J. Reine Angew. Math.，139:155–250，1911。[19] Jean-Pierre Serre。有限群的线性表示，Graduate Texts in Mathematics 第42卷。Springer-Verlag，纽约—海德堡，法文版，1977。[20] K. V. Vedenev 和 V. M. Deundyak。二面体群代数中码与幂等元之间的关系。Mat. Zametki，107(2):178–194，2020。