arXiv:2303.04372v3 [math.RA] 4 Oct 2024

(σ,τ)-群环导子及其应用

Praveen Manju 和 Rajendra Kumar Sharma

印度理工学院德里分校数学系，
豪兹卡斯，新德里-110016，印度[1]

摘要

Leo Creedon 和 Kieran Hughes 在 [18] 中根据群 G的生成元和关系子研究了群 G 在交换含幺环 R上的群环 RG 的导子。本文将这一研究推广到 (σ,τ)-导子。我们给出了一个映射 $f: X \to RG$ 可唯一扩张为 RG的 (σ,τ)-导子 D 的充要条件，其中 R是含幺交换环， G是具有表示 $\langle X \mid Y\rangle$ 的群（X 为生成元集， Y为关系元集），且 (σ,τ) 是 RG的一对 R-代数自同态，它们是 G的群自同态的 R-线性扩张。此外，我们根据秩以及相应 R-模的基，对任意群 G 在任意交换含幺环 R上的群代数 RG 的所有内 (σ,τ)-导子进行分类；该模由 RG的所有内 (σ,τ)-导子组成。我们得到若干推论，特别是当 G是 (σ,τ)-FC群或有限群 G ，以及当 R 是域时的推论。我们还证明，若 R 是含幺环， G是一个阶在 R中可逆的群，则 RG的每个 (σ,τ)-导子都是内导子。我们将上述结果应用于研究正特征域上的交换群代数的 σ-导子，并对任意特征域 $\mathbb{F}$ 上的二面体群代数 $\mathbb{F}D_{2n}$($D_{2n}=\langle a,b \mid a^n=b^2=1, b^{-1}ab=a^{-1}\rangle$,$n\geq 3$) 的所有内导子和外导子$\sigma$进行分类。最后，我们通过给出一种名为 IDD 码的新码的形式化构造及示例，说明这些扭曲导子在编码理论中的应用。

关键词：(σ,τ)-导子；内 (σ,τ)-导子；外 (σ,τ)-导子；群环；群代数；(σ,τ)-共轭类；(σ,τ)-中心；中心化子；反中心化子；二面体；编码理论；IDD 码

数学主题分类（2020）：16S34, 16W25, 13N15, 94B05

1 引言

导子的概念源自解析理论，历史悠久，在研究代数系统的结构与性质方面发挥着重要作用。导子在

[1]电子邮件地址：praveenmanjuiitd@gmail.com(Praveen Manju), rksharmaiitd@gmail.com(Rajendra Kumar Sharma)。

数学和物理学中发挥着至关重要的作用。导子理论已在环及众多代数中得到发展，有助于研究和理解它们的结构。例如，BCI-代数 [43], MV-代数 [33, 44], 巴拿赫代数 [47], 冯·诺伊曼代数 [12], 具有诸多应用的倾斜代数[34], 在信息论等领域十分重要的格：信息恢复、信息访问管理和密码分析[13]。可微流形、算子代数、 $\mathbb{C}^*$-代数，以及李群的表示论，均正借助导子进行研究 [35]。关于导子的历史概述及其更多应用，读者可参阅 [10, 25, 42]。

本文中，我们考察纯代数结构，即群环及其 (σ,τ)-导子，它们有诸多应用（参见 [1] 及其中的参考文献）。关于群环的历史，请读者参阅 [40, 第 3],章；关于导子的历史，请参阅综述文章 [25, 42]。Jacobson [31]提出了 (s_1, s_2)-导子的概念。后来，这类导子通常称为 (σ,τ)-导子或 (θ,ϕ)-导子。人们对它们在素环和半素环中的情形进行了大量研究，并主要将其用于求解函数方程[12]。扭曲导子有诸多应用。导子，尤其是群环的 (σ,τ)-导子，在编码理论中有各种应用 [18, 19]。导子的显式描述有助于构造码（参见 [18]）。它们还用于导数的乘法变形和离散化，这些方法在量子现象模型以及复杂系统与过程的分析中有诸多应用。物理学和工程学领域也对其进行了广泛研究。利用扭曲导子，可以将李代数推广为 Hom-李代数，并以类似于李代数的方式发展 Hom-李代数的中心扩张理论。正如李代数最初被视为导子代数一样，Hom-李代数被定义为扭曲导子代数。利用扭曲导子，可以得到 Witt代数的推广（变形和类似结构）；Witt代数是作用于单变量 Laurent 多项式代数 $\mathbb{C}[t,t^{-1}]$ 上的导子所构成的复李代数。变形的 Witt代数和维拉索罗型代数在分析学、数值数学、代数几何、算术几何、数论和物理学中均有应用。详情请参阅[27, 30, 36, 50] 。扭曲导子还被用于将除环上的伽罗瓦理论加以推广，以及研究数论中的 q-差分算子。关于 (σ,τ)-导子的更多应用，请参阅 [1] 及其中的参考文献。

群环的导子以及（σ,τ）-导子（纯粹以代数方式定义）尚未受到太多关注。群环导子的研究始于论文[51], ，作者在其中研究了域 $\mathbb{F}$上的有限生成无挠幂零群 G 的群环导子。例如，文中证明此类群环总是含有外导子。她运用 $\mathbb{F}G$的导子这一概念，证明了此类群环 $\mathbb{F}G$ 的克鲁尔维数有限；若 G 满足某些额外条件，该维数等于 G 的 $\mathbb{F}$-秩。在 [52, 定理 1], 中， [52], 的主定理证明了有限群的整数群环上的每个导子都是内导子。在 [23, 定理 1.1],中，[23], 的主定理表明，若 G 是一个挠群，其中心Z（G）在 G 中具有有限指数，且 R 是一个半素环，使得 char（R）为 0，或不整除 G中任何元素的阶，那么群环 RG 的每个 R-导子都是内导子。在[15] 和 [16], 中，作者分别将 [52] 和 [23] 的上述结果推广到域和整环上有限群的群环的（σ,τ）-导子，其中σ、 τ 满足某些条件。在 [15], 中，作者证明了以下主定理：

定理 1.1 （[15, 定理 1.1]）。 设 G 是一个有限群，且 R 是一个含单位元的整环，并满足 $|G|$ 在 R中可逆。设 σ、τ 是 R-代数自同态，作用于 RG 且逐个固定 $Z(RG)$ 元素。

(i) 若 R 是域，则 RG 的每个 (σ,τ)-导子都是内导子。

(ii) 若 R 是一个非域整环，且 σ,τ 是 G的群同态的 R-线性扩张，则 RG 的每个 (σ,τ)-导子都是内导子。

她还将以下结论作为上述定理的推论给出：若 G 是有限群，且 $R=\mathbb{Z}$和 σ,τ满足上述定理 (ii) 部分的条件，则 $\mathbb{Z}G$ 的每个 (σ,τ)-导子都是内导子。在 [16, 定理 1.1], 中，本文作者证明了：若 R 是含单位元的半素环，且满足以下条件之一： R 没有挠元；或者 R 具有 p-挠元，但 p 不整除 $|G|$; 其中 G 是一个挠群，满足 $[G:Z(G)]<\infty$，并且若 σ,τ 是 RG 的 R-代数自同态，且逐点固定 $Z(RG)$，则存在一个环 T，使得 $R\subseteq T$, $Z(R)\subseteq Z(T)$; 对于 σ,τ到 TG, $H^1(TG,{}_\sigma TG_\tau)=\{0\}$的自然扩张，其 1 次 Hochschild 上同调——也就是说，存在半素环 R的一个环扩张 T，使得对于 σ,τ到 TG的自然扩张， TG的所有 (σ,τ)-导子都是内导子。A. A. Arutyunov 在其多篇论文（[1, 3, 4, 5, 6, 8, 9]）中运用拓扑和特征研究普通导子与扭导子。详情请参阅第 3.4 和 4.2 小节末尾，我们在那里概述了这些论文中的研究工作。在 [2], 中，作者研究了群 G 在含幺环 R 上的群环，其中 G 中各元素的阶的所有素因子在 R中均可逆。他们证明，若 R 有限且 G 是挠 FC-群，则 RG 的所有导子都是内导子。他们还针对其他群类 G 和环类 R得到了类似结果。在[18], 中，作者根据群的生成元和关系子研究了交换含幺环 R 上的群环的导子。在 [18, 定理 2.5], 中，也就是他们文章的主定理中，作者给出了一个充要条件，用以判定从群 G 的生成集到群环 RG 的映射能否扩张为 RG的导子。利用这一刻画，作者在[18, 定理 3.4] 中，通过给出底域（特征为 p的域）上所有导子构成的向量空间的维数和一组基，对特征为 p的域上的交换群代数的普通导子进行了分类。在 [18, 定理 3.11 和定理 3.13], 中，作者还明确描述了特征为 2 的域上的二面体群代数的普通导子和普通内导子。本文研究群环上更一般的 (σ,τ)-导子相关问题或疑问。本文将讨论任意特征下群代数上的 (σ,τ)-导子和内 (σ,τ)-导子。本文还探讨了另一个问题，即扭导子问题。群环的导子问题旨在探究群环中的所有导子是否都是内导子，或者外导子的空间是否平凡。关于导子问题的历史和重要性，请参阅 [1, 4, 7, 8] 。本文研究 (σ,τ)-导子的类似问题。

我们将手稿分为七节。第 2 节介绍了一些基本定义和事实。在第 3 节中，我们根据群σ、τ的生成元和关系子，研究交换含幺环 RG 上群 G的群环 R 的 (G, τ)-导子。本节又细分为四个小节。在第 3.1 小节中，我们陈述并

证明一些有用的结果，这些结果将在本节主定理 3.4 和定理 3.6 的证明中用到。在第 3.2 小节中，我们借助一个关键的引理 3.3，证明主定理 3.4 中关于 σ-导子的结论。在第 3.3 小节中，我们将第 3.2 小节的结果推广到 (σ,τ)-导子。我们借助一个重要的引理 3.5 证明主定理 3.6。定理 3.4 和定理 3.6 的证明基本思路来自 [18]。然而，在主定理的证明中使用自由群的泛性质，使我们第 3 节主定理的证明不同于 [18] 中的证明。我们将看到，自由群的泛性质在本节主定理（定理 3.4 和定理 3.6）的证明中起着关键作用。在第 3.4 小节中，我们将所得结果应用于交换群代数的 σ-导子研究。

在第 4 节中，我们研究群代数的内（σ,τ）-导子。为此，我们采用双扭共轭类的概念，即（σ,τ）-共轭类；当 $\sigma = id = \tau$ 时，这一概念扩展了经典群论中通常共轭类的概念。群论中的扭共轭类概念于二十世纪提出。在第 4.1 小节中，我们基于双扭共轭类，考察了一些与经典群论中类似的结果和术语。在第 4.2 小节中，我们得到了本节的主要结果。在本节的主要定理，即定理 4.13 中，我们通过求出由所有内（σ,τ）-导子构成的 R-模 Inn$_{(\sigma,\tau)}(\mathbb{F}G)$ 的秩及其一组基，对任意群 G 上、系数取自任意交换含幺环 R 的群环 RG 的所有内（σ,τ）-导子进行了分类。据我们所知，此前文献中尚无结果对任意群 G 上、系数取自任意交换含幺环 R 的群代数 RG 的所有内（σ,τ）-导子进行分类。我们还推论出定理 4.13 的若干推论。推论 4.14 针对 RG 的内（σ,τ）-导子，其中 G 是（σ,τ）-FC群。推论 4.15 针对 RG 的内（σ,τ）-导子，其中 G 是有限群。推论 4.16 针对 RG 的内（σ,τ）-导子，其中 R 是域，且 G 是有限群。在定理 4.17 中，我们证明：若 R 是含幺环，且 G 是阶在 R 中可逆的有限群，则 RG 的每个（σ,τ）-导子都是内（σ,τ）-导子。推论 4.18 是推论 4.15 和定理 4.17 的推论之一。

在第5节中，我们研究第3节和第4节所得结果的应用，以分类任意特征的任意域 $\mathbb{F}$ 上二面体群代数 $\mathbb{F}D_{2n}$ ($n \geq 3$) 的所有内 σ-导子和外 σ-导子。描述由群代数的导子构成的导子代数，是一个众所周知的问题。本节描述任意域上的二面体群代数的 σ-导子代数。为此，我们将本节分为四个小节。在第5.1小节中，我们考察特征为 0 或奇有理素数 p 的域 $\mathbb{F}$ 上 D_{2n} 的群代数 $\mathbb{F}D_{2n}$。我们通过给出 σ-导子代数 $\mathcal{D}_\sigma(\mathbb{F}D_{2n})$ 的维数和一个 $\mathbb{F}$-基，明确分类 $\mathbb{F}D_{2n}$ 的所有 σ-导子。在第5.2小节中，我们对特征为 2 的域 $\mathbb{F}$ 上 D_{2n} 的群代数 $\mathbb{F}D_{2n}$ 做同样的研究。在第5.1小节中，我们确定 D_{2n} 的所有 σ-共轭类。在第5.4小节中，我们分类任意域 $\mathbb{F}$ 上 $\mathbb{F}D_{2n}$ 的所有内 σ-导子和外 σ-导子，从而解决任意域上的二面体群代数的 σ-扭导子问题。因此，本节说明了第3节和第4节的结果对于群环扭导子理论的重要性。

在第6节中，我们讨论所得结果在编码理论中的应用。我们提出编码理论中的一种新码，即导子像导出码（IDD码），并给出其定义和构造，再通过一些示例加以说明。最后，在第

7，我们总结了研究结果。

2 基本定义

下面陈述一些常见知识。设 R 是一个交换含幺环， $\mathcal{A}$ 是一个结合 R-代数。设 (σ,τ) 是 $\mathcal{A}$ 上一对 R-代数自同态。

定义 2.1. 满足 $d(\alpha\beta) = d(\alpha)\beta + \alpha d(\beta)$ 的 R-线性映射 $d: \mathcal{A} \to \mathcal{A}$，若对所有 $\alpha,\beta \in \mathcal{A}$ 均成立，则称为 $\mathcal{A}$ 的导子。若存在某个 $\beta \in \mathcal{A}$ 使得对所有 $\alpha \in \mathcal{A}$ 均有 $d(\alpha) = \beta\alpha - \alpha\beta$，则称其为内导子，此时记作 d_β。所有 $\mathcal{A}$ 的导子所构成的 R-模，除以所有内导子构成的 R- 子模所得的商中的元素，称为外导子。

定义 2.2. (σ,τ)-导子 $D: \mathcal{A} \to \mathcal{A}$ 是一个 R-线性映射，满足 (σ,τ)-扭曲广义恒等式： $D(\alpha\beta) = D(\alpha)\tau(\beta) + \sigma(\alpha)D(\beta)$，对所有 $\alpha,\beta \in \mathcal{A}$ 均成立。若存在某个 $\beta \in \mathcal{A}$ 使得对所有 $\alpha \in \mathcal{A}$ 均有 $D(\alpha) = \beta\tau(\alpha) - \sigma(\alpha)\beta$，则称其为内导子，此时记作 D_β。所有 $\mathcal{A}$ 的 (σ,τ)-导子所构成的 R-模，除以所有内 (σ,τ)-导子构成的 R-子模所得的商中的元素，称为外 (σ,τ)-导子。

定义 2.3. 若 $\tau = \sigma$，则广义单位元等式变为 $D(\alpha\beta) = D(\alpha)\sigma(\beta) + \sigma(\alpha)D(\beta)$；为方便起见，我们将这种 (σ,σ)-导子称为 σ-导子。若存在某个 $\beta \in \mathcal{A}$，使得对所有 $\alpha \in \mathcal{A}$ 都有 $D(\alpha) = \beta\sigma(\alpha) - \sigma(\alpha)\beta$，则称 σ-导子 $D: \mathcal{A} \to \mathcal{A}$ 为内 σ-导子。 $\mathcal{A}$ 的所有 σ-导子构成的 R-模，模去所有内 σ-导子构成的 R-子模后，其商中的元素称为外σ-导子。

记号 2.4. 我们将 $\mathcal{A}$ 上所有 (σ,τ)-导子的集合记为 $\mathcal{D}_{(\sigma,\tau)}(\mathcal{A})$，将 $\mathcal{A}$ 上所有 σ-导子的集合记为 $\mathcal{D}_\sigma(\mathcal{A})$，并将 $\mathcal{A}$ 上所有普通导子的集合记为 $\mathcal{D}(\mathcal{A})$。我们将 $\mathcal{A}$ 上相应的内 (σ,τ)-导子、内 σ-导子和普通内导子的集合分别记为 $\mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$、$\mathrm{Inn}_\sigma(\mathcal{A})$ 和 $\mathrm{Inn}(\mathcal{A})$。我们将 $\mathcal{A}$ 上相应的外 (σ,τ)-导子、外 σ-导子和普通外导子的集合分别记为 $\mathrm{Out}^{(\sigma,\tau)}(\mathcal{A})$、$\mathrm{Out}_\sigma(\mathcal{A})$ 和 $\mathrm{Out}(\mathcal{A})$。

注 2.5. 若 $\sigma = \tau = id_{\mathcal{A}}$（ $\mathcal{A}$上的恒等映射），则通常的莱布尼茨恒等式成立，并且（σ， τ）-导子、内（σ， τ）-导子和外（σ， τ）-导子分别变为$\mathcal{A}$上的普通导子、普通内导子和普通外导子。定义逐分量加法和模作用后， $\mathcal{D}_{(\sigma,\tau)}$（$\mathcal{A}$）成为一个 R-模，同时也是 $\mathcal{A}$-模，而 $\mathrm{Inn}^{(\sigma,\tau)}$（$\mathcal{A}$）成为其子模。若 1 是 $\mathcal{A}$ 中的单位元，且 D 是 $\mathcal{A}$的一个（σ， τ）-导子，则 $D(1) = 0$。

根据上述定义 2.2 和注记 2.5，外 (σ,τ)-导子恰好是商模 $\mathrm{Out}^{(\sigma,\tau)}(\mathcal{A}) = {}^{\mathcal{D}_{(\sigma,\tau)}(\mathcal{A})}/_{\mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})}$ 中的元素。另请注意，集合 $\mathcal{D}_{(\sigma,\tau)}(\mathcal{A}) \setminus \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$ 是所有非~~内 (σ,τ)-~~导子的集合。下面的引理建立了外 (σ,τ)-导子这一概念与 $\mathcal{A}$ 的非内 (σ,τ)-导子之间的联系。

引理 2.6. 设 $T = \{D_i \in \mathcal{D}_{(\sigma,\tau)}(\mathcal{A}) \mid i \in I\}$ (I 某个指标集) 是 $\mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$ 在 $\mathcal{D}_{(\sigma,\tau)}(\mathcal{A})$ 中的一个左陪集横截系，其中 0 是陪集 $\mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$ 的陪集代表元。则 $\mathcal{A}$ 的非内 (σ,τ)-导子与集合 $\bigcup_{D_i\in T\setminus\{0\}}(D_i + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A}))$ 中的元素一一对应。更准确地说，$\mathcal{D}_{(\sigma,\tau)}(\mathcal{A}) \setminus \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A}) = \bigcup_{D_i\in T\setminus\{0\}}(D_i + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A}))$。

证明。设 $D \in \mathcal{D}_{(\sigma,\tau)}(\mathcal{A}) \setminus \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$。于是 $D \in \mathcal{D}_{(\sigma,\tau)}(\mathcal{A})$，但 $D \notin \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$。这意味着 $D + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A}) \neq \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$，因此对于某个 $D_i \in T \setminus \{0\}$，有 $D + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A}) = D_i + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$。因此，$D - D_i \in \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$，所以存在某个 $D_0 \in \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$，使得 $D - D_i = D_0$。最后，我们得到 $D = D_i + D_0$，因此 $D \in D_i + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$。所以，$D \in \bigcup_{D_i\in T\setminus\{0\}}(D_i + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A}))$。因此，$\mathcal{D}_{(\sigma,\tau)}(\mathcal{A}) \setminus \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A}) \subseteq \bigcup_{D_i\in T\setminus\{0\}}(D_i + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A}))$。

反过来，设 $D \in \bigcup_{D_i\in T\setminus\{0\}}(D_i + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A}))$。于是，对于某个 $D_i \in T\setminus\{0\}$，有 $D \in D_i + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$。因此，$D + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A}) = D_i + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$。但由于 $D_i + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A}) \neq \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$，所以 $D + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A}) \neq \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$，从而 $D \notin \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$，也就是说，$D \in \mathcal{D}_{(\sigma,\tau)}(\mathcal{A}) \setminus \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$。因此，$\bigcup_{D_i\in T\setminus\{0\}}(D_i + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})) \subseteq \mathcal{D}_{(\sigma,\tau)}(\mathcal{A}) \setminus \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$。 □

注 2.7. 根据引理 2.6，D 是 $\mathcal{A}$ 的非内导子，当且仅当 $D + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$ 是 $\mathrm{Out}^{(\sigma,\tau)}(\mathcal{A}) = {}^{\mathcal{D}_{(\sigma,\tau)}(\mathcal{A})}/_{Inn_{(\sigma,\tau)}(\mathcal{A})}$ 中的非零元素。换句话说，D 是 ~~$\mathcal{A}$ 的非内~~导子，当且仅当 $D + \mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})$ 是 $\mathcal{A}$ 的非平凡外导子。因此，研究 $\mathcal{A}$ 的非平凡外导子等价于研究 $\mathcal{A}$ 的非内导子（详见 [45, 第 11] 章）。

许多作者将环 R（或代数 $\mathcal{A}$）的外导子定义为 R（或 $\mathcal{A}$）的非内导子。关于这一点的一些参考文献有 [11, 17, 20, 22, 26, 39, 46, 49, 53]。在[9] 和 [41], 中，作者起初将集合 $\mathcal{D}(\mathcal{A}) \setminus \mathrm{Inn}(\mathcal{A})$ 称为外导子的集合，但随后指出，将商模 $\mathrm{Out}(\mathcal{A}) = {}^{\mathcal{D}(\mathcal{A})}/_{\mathrm{Inn}(\mathcal{A})}$ 称为外导子的集合更为自然，因为该模可以解释为 $\mathcal{A}$ 的、系数取自 $\mathcal{A}$ 的 1st Hochschild 上同调模。类似地，商模 $\mathrm{Out}^{(\sigma,\tau)}(\mathcal{A}) = {}^{\mathcal{D}_{(\sigma,\tau)}(\mathcal{A})}/_{\mathrm{Inn}^{(\sigma,\tau)}(\mathcal{A})}$ 是我们的外 (σ,τ)-导子集合，因为该模可以解释为 $\mathcal{A}$ 的、系数取自 $\mathcal{A}$ 的 1st (σ,τ)-Hochschild 上同调模（见[30]）。

定义 2.8. 若 $\mathcal{A}$ 仅有零 (σ,τ)-导子，即 $\mathcal{D}_{(\sigma,\tau)}(\mathcal{A}) = \{0\}$，则称 $\mathcal{A}$ 是 (σ,τ)-微分平凡的。

定义 2.9. 若 R 是一个环，且 G 是一个群，则定义 G 在 R 上的群环为集合

$$RG = \{\sum_{g\in G} a_g g \mid a_g \in R, \forall g \in G \ \ and \ \ |supp(\alpha)| < \infty\},$$

其中，对于 $\alpha = \sum_{g\in G} a_g g$，$\mathrm{supp}(\alpha)$ 表示 α 的支撑，它由 G 中出现在 α 表达式中的元素组成。集合 RG 在逐分量加法以及如下定义的乘法下构成一个环：对于 $\alpha = \sum_{g\in G} a_g g$、$\beta = \sum_{g\in G} b_g g \in RG$,

$$(\sum_{g\in G} a_g g) + (\sum_{g\in G} b_g g) = \sum_{g\in G}(a_g + b_g)g \ \ and \ \ \alpha\beta = \sum_{g,h\in G} a_g b_h gh.$$

若环 R 是具有单位元 1 的交换环，且群 G 是具有单位元 e 的阿贝尔群，则 RG 成为以 R 为底、单位元为 $1 = 1e$ 的交换含幺代数。我们约定空和为 0，空积为 1。

3 群环的（σ,τ）-导子

本节将给出映射 $f: X \to RG$ 能够扩张为群环 RG 上的 (σ,τ)-导子的充要条件，其中 X 是群 G 的生成元集， R 是交换含幺环，而 (σ,τ) 是 RG 上一对含幺（将单位元映到自身的） R-代数自同态，它们是群 G 的群自同态的 R-线性扩张。不过，我们先给出 $\tau = \sigma$ 情形下的结果。然后，我们利用这些结果对正特征域上的交换群代数的所有 σ-导子进行分类。

3.1 一些有用结果

我们将在主要定理的证明中使用自由群的泛性质3.4 和3.6。

定理 3.1。（自由群的泛性质）：设 X 是一个字母表， $F(X)$ 是以字母表 X 为基的自由群。设 G 是一个群， $f: X \to G$ 是一个集合映射。那么˜存在唯一的群同态 $f: F(X) \to G$ ，使得下图交换:

$$\begin{array}{ccc} X & \xrightarrow{i} & F(X) \\ & \searrow^{f} & \downarrow \tilde{f} \\ & & G \end{array}$$

˜其中 $i: X \to F(X)$ 是包含映射，也就是说，对于所有 $x \in X$，都有 $f(x) = f(x)$。

引理 3.2. 设 $\mathcal{A}$ 是含幺环 R 上的结合代数，且 σ 和 τ 是 $\mathcal{A}$ 的两个代数自同态，它们将 $\mathcal{A}$ 的单位元 1 映为其自身。设 D 是 $\mathcal{A}$ 的（σ,τ）-导子。那么

(i) $D\left(\prod_{i=1}^{k}\alpha_i\right) = \sum_{i=1}^{k}\left(\prod_{j=1}^{i-1}\sigma(\alpha_j)\right)D(\alpha_i)\left(\prod_{j=i+1}^{k}\tau(\alpha_j)\right)$ *for all* $\alpha_i \in \mathcal{A}$.

(ii) $D(\alpha^k) = \sum_{i=0}^{k-1}(\sigma(\alpha))^i D(\alpha)(\tau(\alpha))^{k-i-1}$ 对所有 $\alpha \in \mathcal{A}$ 和 $k \in \mathbb{N}$均成立。

(iii) $\sum_{i=0}^{r-1}(\sigma(\alpha))^i D(\alpha)(\tau(\alpha))^{r-1-i} = 0$ 对 $\mathcal{A}$ 中所有阶为 r的单位元 α 均成立。

(iv) $D(\alpha^k) = \left(\sum_{i=0}^{k-1}(\sigma(\alpha))^i(\tau(\alpha))^{k-i-1}\right)D(\alpha)$ 对所有满足 $\sigma(\alpha)$ 和 $\tau(\alpha)$ 与 $D(\alpha)$ 及 $k \in \mathbb{N}$可交换的 $\alpha \in \mathcal{A}$ 均成立。特别地，若 $\sigma = \tau$ 且 $\sigma(\alpha)$ 与 $D(\alpha)$ 可交换，则 $D(\alpha^k) = k(\sigma(\alpha))^{k-1}D(\alpha)$。

(v) $D(\alpha^k) = k(\sigma(\alpha))^{k-1}D(\alpha)$ 对于任意在 $\mathcal{A}$ 中为单位元且满足 $\sigma(\alpha)$ 与 $D(\alpha)$ 可交换的 α ，以及任意 $k \in \mathbb{Z}$，均成立。

证明。（i）我们对 k 使用归纳法证明该等式。对于 $k = 1$，左边为 $D(\alpha_1)$，右边为 $\sum_{i=1}^{1} 1D(\alpha_1)1 = D(\alpha_1)$，二者相等。现假设该结论对 $k-1$ 成立。则

$$D(\prod_{i=1}^{k}\alpha_i) = D(\prod_{i=1}^{k-1}\alpha_i)\tau(\alpha_k) + \sigma(\prod_{i=1}^{k-1}\alpha_i)D(\alpha_k)$$

$$= \left(\sum_{i=1}^{k-1}\left(\prod_{j=1}^{i-1}\sigma(\alpha_j)\right)D(\alpha_i)\left(\prod_{j=i+1}^{k-1}\tau(\alpha_j)\right)\right)\tau(\alpha_k) + \sigma(\prod_{i=1}^{k-1}\alpha_i)D(\alpha_k)$$
$$= \sum_{i=1}^{k}\left(\prod_{j=1}^{i-1}\sigma(\alpha_j)\right)D(\alpha_i)\left(\prod_{j=i+1}^{k}\tau(\alpha_j)\right).$$

因此，由归纳法，该结论对所有 $k \in \mathbb{N}$ 都成立。
(ii) 在 (i) 中对所有 $i \in \{1, ..., k\}$ 令 $\alpha_i = \alpha$，可得

$$D(\alpha^k) = \sum_{i=1}^{k}\left(\left(\prod_{j=1}^{i-1}\sigma(\alpha)\right)D(\alpha)\left(\prod_{j=i+1}^{k}\tau(\alpha)\right)\right) = \sum_{i=0}^{k-1}(\sigma(\alpha))^i D(\alpha)(\tau(\alpha))^{k-i-1}.$$

(iii) 设 $\alpha \in \mathcal{A}$ 是一个阶为 r 的单位元，使得 $\alpha^r = 1$。那么由 (ii) 可得，

$$0 = D(1) = D(\alpha^r) = \sum_{i=0}^{r-1}(\sigma(\alpha))^i D(\alpha)(\tau(\alpha))^{r-1-i}.$$

(iv) 设 $\alpha \in \mathcal{A}$ 满足 $\sigma(\alpha)$ 和 $\tau(\alpha)$ 与 $D(\alpha)$ 交换。那么由 (ii) 可得，

$$D(\alpha^k) = \left(\sum_{i=0}^{k-1}(\sigma(\alpha))^i(\tau(\alpha))^{k-i-1}\right)D(\alpha)$$

对于 $k \in \mathbb{N}$。若 $\tau = \sigma$，则

$$D(\alpha^k) = \left(\sum_{i=0}^{k-1}(\sigma(\alpha))^{k-1}\right)D(\alpha) = k(\sigma(\alpha))^{k-1}D(\alpha).$$

(v) 设 α 是 $\mathcal{A}$ 中的一个单位元，满足 $\sigma(\alpha)$ 和 $D(\alpha)$ 彼此交换。由 (iv)，该结论对所有 $k \in \mathbb{N}$ 均成立。对于 $k = 0$，$D(\alpha^0) = D(1) = 0$，且右侧是空和，显然为 0。因此，该等式对 $k = 0$ 也成立。

我们有

$$\sigma(\alpha^{-1})D(\alpha) = \sigma(\alpha^{-1})D(\alpha)\sigma(\alpha\alpha^{-1}) = \sigma(\alpha^{-1})\sigma(\alpha)D(\alpha)\sigma(\alpha^{-1}) = D(\alpha)\sigma(\alpha^{-1}).$$

因此，α^{-1} 也是 $\mathcal{A}$ 中的一个单位元，使得 $\sigma(\alpha^{-1})$和 $D(\alpha)$彼此交换。因此，

$$0 = D(1) = D(\alpha^{-1}\alpha) = D(\alpha^{-1})\sigma(\alpha) + \sigma(\alpha^{-1})D(\alpha)$$

从而 $D(\alpha^{-1}) = -\sigma(\alpha^{-2})D(\alpha)$。此外，

$\sigma(\alpha^{-1})D(\alpha^{-1}) = \sigma(\alpha^{-1})(-\sigma(\alpha^{-2})D(\alpha)) = (-\sigma(\alpha^{-2})D(\alpha))\sigma(\alpha^{-1}) = D(\alpha^{-1})\sigma(\alpha^{-1})$。

现在，由 (iv) 可知，对于任意 $k \in \mathbb{N}$,

$$\begin{aligned} D(\alpha^{-k}) &= D((\alpha^{-1})^k) \\ &= k(\sigma(\alpha^{-1}))^{k-1}D(\alpha^{-1}) \\ &= k(\sigma(\alpha))^{-k+1}(-(\sigma(\alpha))^{-2}D(\alpha)) \\ &= -k(\sigma(\alpha))^{-k-1}D(\alpha). \end{aligned}$$

因此，结论 (v) 对所有 $k \in \mathbb{Z}$ 都成立。 □

3.2 σ-导子的主定理

引理 3.3. 设 $G = \langle X \mid Y \rangle$ 是一个群，其生成元集为 X，关系元集为 Y。设 R 是一个交换含幺环，σ 是 RG 的一个 R-代数端同态，并且是 G 的一个群自同态的 R-线性扩张。设 $F(X)$ 是由 X 生成的自由群。那么，任意映射 $f: X \to RG$ 都可以唯一地扩张为映射 $\tilde{f}: F(X) \to RG$，使得

$$\tilde{f}(vw) = \tilde{f}(v)\tilde{\sigma}(w) + \tilde{\sigma}(v)\tilde{f}(w), \forall\, v, w \in F(X), \tag{3.1}$$

其中，$\tilde{\sigma}: F(X) \to G$ 是唯一的群同态，满足对于所有$x \in X$，$\tilde{\sigma}(x) = \sigma(x)$。

证明。由定理 3.1，σ 可以唯一地扩张为群同态 $\tilde{\sigma}: F(X) \to G$ 使得 $\tilde{\sigma}(x) = \sigma(x)$ 对所有 $x \in X$成立。令 $X^{-1} = \{x^{-1} \mid x \in X\}$。那么，对于任意 $x \in X$，

$$1 = \tilde{\sigma}(1) = \tilde{\sigma}(x)\tilde{\sigma}(x^{-1}) = \sigma(x)\tilde{\sigma}(x^{-1})$$

于是，$\tilde{\sigma}(x^{-1}) = \sigma(x^{-1})$。因此，对于所有 $g \in G$，$\tilde{\sigma}(g) = \sigma(g)$。

定义 $\tilde{f}: F(X) \to RG$ 为

$$\tilde{f}(x) = \begin{cases} f(x) & \text{if } x \in X \\ -\sigma(x)f(x^{-1})\sigma(x) & \text{if } x \in X^{-1} \\ 0 & \text{if } x = 1 \end{cases} \tag{3.2}$$

并且若 $w = \prod_{i=1}^{m} x_i$，对于 $x_i \in X \cup X^{-1}\,(1 \le i \le m)$，则

$$\tilde{f}(w) = \sum_{i=1}^{m} \left(\left(\prod_{j=1}^{i-1} \sigma(x_j) \right) \tilde{f}(x_i) \left(\prod_{j=i+1}^{m} \sigma(x_j) \right) \right). \tag{3.3}$$

令 $0 \le m \le n$，$v = \prod_{i=1}^{m} x_i$ 且 $w = \prod_{i=m+1}^{n} x_i$。由（3.2）和（3.3），

$$\begin{aligned} \tilde{f}(vw) &= \tilde{f}((\prod_{i=1}^{m} x_i)(\prod_{i=m+1}^{n} x_i)) = \tilde{f}(\prod_{i=1}^{n} x_i) = \sum_{i=1}^{n} \left(\left(\prod_{j=1}^{i-1} \sigma(x_j) \right) \tilde{f}(x_i) \left(\prod_{j=i+1}^{n} \sigma(x_j) \right) \right) \\ &= \left(\sum_{i=1}^{m} \left(\prod_{j=1}^{i-1} \sigma(x_j) \right) \tilde{f}(x_i) \left(\prod_{j=i+1}^{m} \sigma(x_j) \right) \right) \left(\prod_{j=m+1}^{n} \sigma(x_j) \right) \\ &\quad + (\prod_{i=1}^{m} \sigma(x_j))(\sum_{i=m+1}^{n} (\prod_{j=m+1}^{i-1} \sigma(x_j))\tilde{f}(x_i)(\prod_{j=i+1}^{n} \sigma(x_j))) \\ &= \tilde{f}(v)\tilde{\sigma}(w) + \tilde{\sigma}(v)\tilde{f}(w). \end{aligned}$$

因此，$\tilde{f}$ 满足（3.1）。

对于 X 上的任意单词 w，令 $\overline{w}$ 表示 X 上的约化词。为证明映射 f 是良定义的，必须证明对于 X 上的所有单词 w，都有 $f(w) = f(\overline{w})$。

利用 (3.1) 和 (3.2)，注意对于任意 $x \in X$，

$$\tilde{f}(xx^{-1}) = \tilde{f}(x)\tilde{\sigma}(x^{-1}) + \tilde{\sigma}(x)\tilde{f}(x^{-1}) = f(x)\sigma(x^{-1}) - \sigma(x)\sigma(x^{-1})f(x)\sigma(x^{-1}) = 0.$$

类似地，对于任意 $x \in X^{-1}$, $\tilde{f}(xx^{-1}) = 0$。因此，对于 X 上的任意两个字 v 和 w，以及任意 $x \in X \cup X^{-1}$,

$$\begin{aligned}\tilde{f}(vxx^{-1}w) &= \tilde{f}(v)\tilde{\sigma}(xx^{-1}w) + \tilde{\sigma}(v)\tilde{f}(xx^{-1}w)\\ &= \tilde{f}(v)\tilde{\sigma}(w) + \tilde{\sigma}(v)(\tilde{f}(xx^{-1})\tilde{\sigma}(w) + \tilde{\sigma}(xx^{-1})\tilde{f}(w))\\ &= \tilde{f}(v)\tilde{\sigma}(w) + \tilde{\sigma}(v)\tilde{f}(xx^{-1})\tilde{\sigma}(w) + \tilde{\sigma}(v)\tilde{f}(w)\\ &= \tilde{f}(v)\tilde{\sigma}(w) + \tilde{\sigma}(v)\tilde{f}(w)\\ &= \tilde{f}(vw).\end{aligned}$$

因此，对于所有关于 X 的单词 w， $f(w) = f(\overline{w})$。

现在，剩下要证明的是 f 的唯一性。若不然，假设 $\tilde{g}\colon F(X) \to RG$ 是 f 的另一个扩张，且不同于满足下列条件的 f

$$\tilde{g}(vw) = \tilde{g}(v)\tilde{\sigma}(w) + \tilde{\sigma}(v)\tilde{g}(w)$$

对于所有 v， $w \in F(X)$。

注意到

$$\tilde{g}(1) = \tilde{g}(1)\tilde{\sigma}(1) + \tilde{\sigma}(1)\tilde{g}(1) = \tilde{g}(1) + \tilde{g}(1)$$

因此 $\tilde{g}(1) = 0$。所以， $\tilde{g}(1) = 0 = f(1)$。

再次，由于 $\tilde{f}$ 和 $\tilde{g}$ 是 $f : X \to RG$ 的扩张，因此，

$$\tilde{g}(x) = f(x) = \tilde{f}(x)$$

对所有 $x \in X$ 均成立。

此外，对于任意 $x \in X$,

$$0 = \tilde{g}(1) = \tilde{g}(xx^{-1}) = \tilde{g}(x)\tilde{\sigma}(x^{-1}) + \tilde{\sigma}(x)\tilde{g}(x^{-1})$$

从而

$$\tilde{g}(x^{-1}) = -\sigma(x^{-1})f(x)\sigma(x^{-1}) = \tilde{f}(x^{-1}).$$

因此，对所有 $x \in X \cup X^{-1}$， $\tilde{g}(x) = \tilde{f}(x)$。

由于 $\tilde{g} \neq f$，因此存在某个 $w_0 \in F(X)$，使得对于所有长度严格小于 w_0 的单词 $w \in F(X)$， $\tilde{g}(w_0) \neq f(w_0)$ 且 $\tilde{g}(w) = f(w)$。现在，由于 $w_0 \in F(X)$，所以对于某个 $x_i \in X \cup X^{-1} (1 \leq i \leq m_0)$，有 $w_0 = \prod_{i=1}^{m_0} x_i$，其中 m_0 是单词 w_0 的长度。由于 $\prod_{i=1}^{m_0-1} x_j$，存在 $x_{m_0} \in F(X)$，使得它们的长度严格小于 $m_0$of w_0 的长度，因此根据我们对 w_0 的选择,

$$\tilde{g}(\prod_{i=1}^{m_0-1} x_j) = \tilde{f}(\prod_{i=1}^{m_0-1} x_j) \qquad \text{and} \qquad \tilde{g}(x_{m_0}) = \tilde{f}(x_{m_0}).$$

这给出

$$\tilde{g}(w_0) = \tilde{g}(\prod_{i=1}^{m_0} x_i) = \tilde{g}((\prod_{i=1}^{m_0-1} x_i)x_{m_0})$$

$$
\begin{aligned}
&= \tilde{g}(\prod_{i=1}^{m_0-1} x_j)\tilde{\sigma}(x_{m_0}) + \tilde{\sigma}(\prod_{i=1}^{m_0-1} x_j)\tilde{g}(x_{m_0}) \\
&= \tilde{f}(\prod_{i=1}^{m_0-1} x_j)\tilde{\sigma}(x_{m_0}) + \tilde{\sigma}(\prod_{i=1}^{m_0-1} x_j)\tilde{f}(x_{m_0}) \\
&= \tilde{f}(\prod_{i=1}^{m_0} x_i) = \tilde{f}((\prod_{i=1}^{m_0-1} x_i)x_{m_0}) \\
&= \tilde{f}(w_0)
\end{aligned}
$$

但这与以下事实矛盾：$\tilde{g}(w_0) \neq f(w_0)$。因此，$\tilde{f}$ 是 f 的唯一延拓：$X \to RG$ 从 $F(X)$到 RG，且满足（3.1）。 □

定理 3.4。在引理 3.3的假设下，映射 $f: X \to RG$ 可以扩展为一个 σ-导子 D 在 RG 当且仅当 $f(y) = 0$ 对所有 $y \in Y$成立。

证明。首先，假设给定的映射 $f: X \to RG$ 可以扩展为 σ-导子 D在 RG上。因此，对所有 $x \in X$，$D(x) = f(x)$。此外，对于任意 $x \in X$，

$$0 = D(1) = D(xx^{-1}) = D(x)\sigma(x^{-1}) + \sigma(x)D(x^{-1})$$

从而

$$D(x^{-1}) = -\sigma(x^{-1})D(x)\sigma(x^{-1}) = -\sigma(x^{-1})f(x)\sigma(x^{-1}) = \tilde{f}(x^{-1}).$$

因此，对所有 $x \in X \cup X^{-1}$，$D(x) = \tilde{f}(x)$。

现在，令 $y \in Y$。于是 $y = \prod_{i=1}^{k} y_i$ 对于某个 $y_i \in X \cup X^{-1}\,(1 \leq i \leq k)$。由 (3.3) 及引理 3.2(i),

$$
\begin{aligned}
\tilde{f}(y) = \tilde{f}(\prod_{i=1}^{k} y_i) &= \sum_{i=1}^{k} \left(\left(\prod_{j=1}^{i-1} \sigma(y_j) \right) \tilde{f}(y_i) \left(\prod_{j=i+1}^{k} \sigma(y_j) \right) \right) \\
&= \sum_{i=1}^{k} \left(\left(\prod_{j=1}^{i-1} \sigma(y_j) \right) D(y_i) \left(\prod_{j=i+1}^{k} \sigma(y_j) \right) \right) \\
&= D(\prod_{i=1}^{k} y_i) = D(y) = D(1) = 0.
\end{aligned}
$$

因此，对所有 $y \in Y$，$\tilde{f}(y) = 0$。

反过来，假设 $\tilde{f}(y) = 0$ 对所有 $y \in Y$均成立。注意到，对所有 $y \in Y$，$\tilde{\sigma}(y) = \sigma(y) = 1$。因此，对于任意 $y \in Y$，

$$0 = \tilde{f}(1) = \tilde{f}(yy^{-1}) = \tilde{f}(y)\tilde{\sigma}(y^{-1}) + \tilde{\sigma}(y)\tilde{f}(y^{-1}) = \tilde{f}(y^{-1}).$$

因此，对所有 $y \in Y$，$\tilde{f}(y^{-1}) = 0$ 均成立。

令 $Y^{F(X)}$ 为 Y 在 $F(X)$ 中的正规闭包。那么

$$Y^{F(X)} = \langle w^{-1}yw \mid w \in F(X), y \in Y \rangle$$

它也是唯一的满群同态 $\phi: F(X) \to G$ 的核，该同态在 X上为单位映射，也就是说，$G \cong {}^{F}{}_{(X)Y^{F(X)}}$。令 $\varepsilon \in \{1, -1\}$。于是，利用（3.1）以及$f(y^{\varepsilon}) = 0$对所有 $y \in Y$成立这一事实，可得对于任意 $w \in F(X)$,

$$\begin{aligned}\tilde{f}(w^{-1}y^{\varepsilon}w) &= \tilde{f}(w^{-1})\tilde{\sigma}(y^{\varepsilon}w) + \tilde{\sigma}(w^{-1})\tilde{f}(y^{\varepsilon}w)\\ &= \tilde{f}(w^{-1})\tilde{\sigma}(w) + \tilde{\sigma}(w^{-1})(\tilde{f}(y^{\varepsilon})\tilde{\sigma}(w) + \tilde{\sigma}(y^{\varepsilon})\tilde{f}(w))\\ &= \tilde{f}(w^{-1})\tilde{\sigma}(w) + \tilde{\sigma}(w^{-1})\tilde{f}(w)\\ &= \tilde{f}(w^{-1}w) = \tilde{f}(1) = 0.\end{aligned}$$

现在，令 $v \in Y^{F(X)}$。那么 $v = \prod_{i=1}^{m} w_i^{-1}y_i^{\varepsilon}w_i$对于某个 $m \in \mathbb{N}$, $w_i \in F(X)$, $y_i \in Y(1 \le i \le m)$。如上所示，该结论对 $m = 1$成立。假设该结论对 $m = k - 1$成立，即 $\tilde{f}(\prod_{i=1}^{k-1} w_i^{-1}y_i^{\varepsilon}w_i) = 0$。那么利用（3.3）和归纳假设可得，对于 $m = k$,

$$\begin{aligned}\tilde{f}(v) = \tilde{f}(\prod_{i=1}^{k} w_i^{-1}y_i^{\varepsilon}w_i) &= \tilde{f}((\prod_{i=1}^{k-1} w_i^{-1}y_i^{\varepsilon}w_i)(w_k^{-1}y_k^{\varepsilon}w_k))\\ &= \tilde{f}(\prod_{i=1}^{k-1} w_i^{-1}y_i^{\varepsilon}w_i)\tilde{\sigma}(w_k^{-1}y_k^{\varepsilon}w_k) + \tilde{\sigma}(\prod_{i=1}^{k-1} w_i^{-1}y_i^{\varepsilon}w_i)\tilde{f}(w_k^{-1}y_k^{\varepsilon}w_k)\\ &= 0\tilde{\sigma}(w_k^{-1}y_k^{\varepsilon}w_k) + \tilde{\sigma}(\prod_{i=1}^{k-1} w_i^{-1}y_i^{\varepsilon}w_i)0 = 0.\end{aligned}$$

因此，对于所有 $v \in Y^{F(X)}$, $\tilde{f}(v) = 0$。此外，对于所有 $v \in Y^{F(X)}$, $\tilde{\sigma}(v) = 1$。因此，对于任意$w \in F(X)$ 和 $v \in Y^{F(X)}$,

$$\tilde{f}(wv) = \tilde{f}(w)\tilde{\sigma}(v) + \tilde{\sigma}(w)\tilde{f}(v) = \tilde{f}(w)1 + \tilde{\sigma}(w)0 = \tilde{f}(w).$$

令 $g \in G$ 和 $g = \prod_{i=1}^{m} x_i$，其中 $m \in \mathbb{N}, x_i \in X \cup X^{-1}(1 \le i \le m)$。因此，$g$是 X上的一个字，使得 $g \in F(X)$。事实上，g是 $F(X)$ 中满足 $\phi(g) = g$ 的约化词。若 $w \in F(X)$ 满足 $\phi(w) = g$，则 w 要么等价于约化词 g，要么 w的表达式（作为来自 $X \cup X^{-1}$ 的元素之积）包含来自 $Y^{F(X)}$ 的元素。无论哪种情况，$\tilde{\sigma}(w) = \sigma(g)$。

现在，定义 $D: G \to RG$ 如下:

$$D(g) = \tilde{f}(w)$$

其中，对于 $g \in G$, $w \in F$（X）满足 ϕ（w）$= g$。这样的 w 存在，因为 ϕ: F（X）$\to G$ 是满群同态；或者，如上段所述，我们可以取 $w = g$。˜映射 D 是良定义的，因为如前所示，f: F（X）$\to RG$ 是良定义映射，且对于所有 $v \in Y^{F(X)}$，都有 $\tilde{f}$（wv）$= \tilde{f}$（w）。

现在，令 $g, h \in G$。那么存在某个 $u, w \in F(X)$，使得

$$\phi(u) = g \qquad \text{and} \qquad \phi(w) = h.$$

Then

$$\tilde{\sigma}(u) = \sigma(g), \quad \tilde{\sigma}(w) = \sigma(h) \quad \text{and} \quad \phi(uw) = \phi(u)\phi(w) = gh.$$

因此，根据 D的定义，

$$D(g) = \tilde{f}(u), \quad D(h) = \tilde{f}(w) \quad \text{and} \quad D(gh) = \tilde{f}(uw).$$

最后，利用（3.1），可得

$$D(gh) = \tilde{f}(uw) = \tilde{f}(u)\tilde{\sigma}(w) + \tilde{\sigma}(u)\tilde{f}(w) = D(g)\sigma(h) + \sigma(g)D(h).$$

因此，对于任意 $g, h \in G$， $D(gh) = D(g)\sigma(h) + \sigma(g)D(h)$。

现在，将其线性延拓到整个 RG。我们仍用 D 表示这个延拓映射。因此，若 $\lambda \in R$，且对于某些 λ_g, $\mu_h \in R$ $(g, h \in G)$，$\alpha = \sum_{g\in G} \lambda_g g$, $\beta = \sum_{h\in G} \mu_h h \in RG$，则$D(\alpha + \beta) = D(\alpha) + D(\beta)$，并且 $D(\lambda\alpha) = \lambda D(\alpha)$，因为 D 是一个 R-线性映射。此外，

$$\begin{aligned}
D(\alpha\beta) &= D((\sum_{g\in G} \lambda_g g)(\sum_{g\in G} \mu_h h)) \\
&= D(\sum_{g,h\in G} \lambda_g \mu_h (gh)) = \sum_{g,h\in G} \lambda_g \mu_h D(gh) \\
&= \sum_{g,h\in G} \lambda_g \mu_h (D(g)\sigma(h) + \sigma(g)D(h)) \\
&= \sum_{g,h\in G} \lambda_g \mu_h D(g)\sigma(h) + \sum_{g,h\in G} \lambda_g \mu_h \sigma(g)D(h) \\
&= D(\sum_{g\in G} \lambda_g g)\sigma(\sum_{h\in G} \mu_h h) + \sigma(\sum_{g\in G} \lambda_g g)D(\sum_{h\in G} \mu_h h) \\
&= D(\alpha)\sigma(\beta) + \sigma(\alpha)D(\beta).
\end{aligned}$$

因此，D 是 RG 上的一个 σ-导子，它将 $f\colon X \to RG$ 延拓到整个 RG。

现在，只需证明 $\tilde{D}$ 与 D 是一致的。为此，设 $\tilde{D}$ 是 σ-导子，它是 RG 的扩张，且扩张了 $f\colon X \to RG$。那么，存在某个 $g_0 \in G$ 使得，对于所有满足 g 的长度严格小于 g_0的 $g \in G$，都有 $D(g_0) \neq D(g_0)$ 且 $D(g) = D(g)$。

注意，$\tilde{D}(1) = 0 = D(1)$。此外，对于所有 $x \in X$，$D(x) = f(x) = D(x)$。现在，对于任意$x \in X$，

$$0 = \tilde{D}(1) = \tilde{D}(xx^{-1}) = \tilde{D}(x)\sigma(x^{-1}) + \sigma(x)\tilde{D}(x^{-1}) = f(x)\sigma(x^{-1}) + \sigma(x)\tilde{D}(x^{-1})$$

使得 $\tilde{D}(x^{-1}) = -\sigma(x^{-1})f(x)\sigma(x^{-1}) = \tilde{f}(x^{-1}) = D(x^{-1})$。

对于某些 $x_0, y_0 \in G$，我们可以将 $g_0 \in G$ 写成 $g_0 = x_0 y_0$，使得 x_0 和 y_0 的长度都严格小于 g_0的长度。由此，考虑到我们的假设，$D(x_0) = D(x_0)$ 且 $D(y_0) = D(y_0)$。因此，

$$\begin{aligned}
\tilde{D}(g_0) &= \tilde{D}(x_0 y_0) \\
&= \tilde{D}(x_0)\sigma(y_0) + \sigma(x_0)\tilde{D}(y_0) \\
&= D(x_0)\sigma(y_0) + \sigma(x_0)D(y_0) \\
&= D(x_0 y_0)
\end{aligned}$$

$$= D(g_0).$$

但是，这与 $D(g_0) \neq D(g_0)$ 的事实矛盾。因此， $D: RG \to RG$ 是将给定映射 $f: X \to RG$ 扩张的唯一 σ-导子。

由此得证。 □

3.3 (σ, τ)-导子的主定理

在本小节中，我们证明引理 3.3 和定理 3.4，并将其推广到 (σ, τ)-导子的情形。证明思路基本相同，但为求完整起见，我们仍给出证明。

引理 3.5. 设 $G = \langle X \mid Y \rangle$ 是一个群，其生成元集为 X，关系元集为 Y。设 R 是一个交换含幺环，且 σ 和 τ 是 R-代数 RG的端同态，它们分别是 G的群自同态的 R-线性扩张。设 $F(X)$ 是由 X生成的自由 ˜群。那么，任意映射 $f: X \to RG$ 都可以唯一扩张为映射 $f: F(X) \to RG$，使得

$$\tilde{f}(vw) = \tilde{f}(v)\tilde{\tau}(w) + \tilde{\sigma}(v)\tilde{f}(w), \ \forall\, v, w \in F(X), \tag{3.4}$$

其中 $\tilde{\sigma}, \tilde{\tau}: F(X) \to G$ 是满足以下条件的唯一群同态：对所有 $x \in X$， $\tilde{\sigma}(x) = \sigma(x)$ 且$\tilde{\tau}(x) = \tau(x)$。

证明。根据定理 3.1， σ 和 τ 可以唯一地延拓为群同态 $\tilde{\sigma}: F(X) \to G$和 $\tilde{\tau}: F(X) \to G$，使得对所有 $x \in X$，均有 $\tilde{\sigma}(x) = \sigma(x)$ 且 $\tilde{\tau}(x) = \tau(x)$。

如引理 3.3 的证明所示， $\tilde{\sigma}(g) = \sigma(g)$ 对所有 $g \in G$ 均成立。类似地，可以证明 $\tilde{\tau}(g) = \tau(g)$ 对所有 $g \in G$ 均成立。

定义 $f: F(X) \to RG$ 为

$$\tilde{f}(x) = \begin{cases} f(x) & \text{if } x \in X \\ -\sigma(x) f(x^{-1}) \tau(x) & \text{if } x \in X^{-1} \\ 0 & \text{if } x = 1 \end{cases} \tag{3.5}$$

并且若 $w = \prod_{i=1}^{m} x_i$，对于 $x_i \in X \cup X^{-1}$ $(1 \leq i \leq m)$，则

$$\tilde{f}(w) = \sum_{i=1}^{m} \left(\left(\prod_{j=1}^{i-1} \sigma(x_j) \right) \tilde{f}(x_i) \left(\prod_{j=i+1}^{m} \tau(x_j) \right) \right). \tag{3.6}$$

设 $0 \leq m \leq n$， $v = \prod_{i=1}^{m} x_i$ 且 $w = \prod_{i=m+1}^{n} x_i$。由（3.5）和（3.6），

$$\begin{aligned} \tilde{f}(vw) &= \tilde{f}((\prod_{i=1}^{m} x_i)(\prod_{i=m+1}^{n} x_i)) = \tilde{f}(\prod_{i=1}^{n} x_i) = \sum_{i=1}^{n} \left(\left(\prod_{j=1}^{i-1} \sigma(x_j) \right) \tilde{f}(x_i) \left(\prod_{j=i+1}^{n} \tau(x_j) \right) \right) \\ &= \left(\sum_{i=1}^{m} \left(\prod_{j=1}^{i-1} \sigma(x_j) \right) \tilde{f}(x_i) \left(\prod_{j=i+1}^{m} \tau(x_j) \right) \right) \left(\prod_{j=m+1}^{n} \tau(x_j) \right) \\ &\quad + (\prod_{i=1}^{m} \sigma(x_j))(\sum_{i=m+1}^{n} (\prod_{j=m+1}^{i-1} \sigma(x_j)) \tilde{f}(x_i) (\prod_{j=i+1}^{n} \tau(x_j))) \\ &= \tilde{f}(v)\tilde{\tau}(w) + \tilde{\sigma}(v)\tilde{f}(w). \end{aligned}$$

˜因此， f 满足（3.4）。

˜对于 w 上的任意单词 X，令 $\overline{w}$ 表示 X 上的约化词。为证明映射 f 是˜ ˜良定义的，必须证明对于 X 上的所有单词 w，都有 $f(w) = f(\overline{w})$。

利用（3.4）和（3.5），注意到对于任意 $x \in X$，

$$\tilde{f}(xx^{-1}) = \tilde{f}(x)\tilde{\tau}(x^{-1}) + \tilde{\sigma}(x)\tilde{f}(x^{-1}) = f(x)\tau(x^{-1}) - \sigma(x)\sigma(x^{-1})f(x)\tau(x^{-1}) = 0.$$

类似地，对于任意 $x \in X^{-1}$， $\tilde{f}(xx^{-1}) = 0$。因此，对于 X 上的任意两个单词 v 和 w，以及任意 $x \in X \cup X^{-1}$，

$$\begin{aligned}
\tilde{f}(vxx^{-1}w) &= \tilde{f}(v)\tilde{\tau}(xx^{-1}w) + \tilde{\sigma}(v)\tilde{f}(xx^{-1}w) \\
&= \tilde{f}(v)\tilde{\tau}(w) + \tilde{\sigma}(v)(\tilde{f}(xx^{-1})\tilde{\tau}(w) + \tilde{\sigma}(xx^{-1})\tilde{f}(w)) \\
&= \tilde{f}(v)\tilde{\tau}(w) + \tilde{\sigma}(v)\tilde{f}(xx^{-1})\tilde{\tau}(w) + \tilde{\sigma}(v)\tilde{f}(w) \\
&= \tilde{f}(v)\tilde{\tau}(w) + \tilde{\sigma}(v)\tilde{f}(w) \\
&= \tilde{f}(vw).
\end{aligned}$$

˜ ˜因此，对于 X 上的所有单词 w， $f(w) = f(\overline{w})$。

˜现在，正如引理 3.3 的证明中那样，我们证明 f 的唯一性。假设存在˜使得 $\tilde{g}$： $F(X)$ $\to RG$ 是 f 的另一个扩张，且不同于 f，并满足

$$\tilde{g}(vw) = \tilde{g}(v)\tilde{\tau}(w) + \tilde{\sigma}(v)\tilde{g}(w)$$

对所有 $v, w \in F(X)$。

注意

$$\tilde{g}(1) = \tilde{g}(1)\tilde{\tau}(1) + \tilde{\sigma}(1)\tilde{g}(1) = \tilde{g}(1) + \tilde{g}(1)$$

˜，因此 $\tilde{g}(1) = 0$。所以， $\tilde{g}(1) = 0 = f(1)$。

再者，由于 $\tilde{f}$ 和 $\tilde{g}$ 是 $f : X \to RG$ 的扩张，因此，

$$\tilde{g}(x) = f(x) = \tilde{f}(x)$$

对所有 $x \in X$。

此外，对于任意 $x \in X$，

$$0 = \tilde{g}(1) = \tilde{g}(xx^{-1}) = \tilde{g}(x)\tilde{\tau}(x^{-1}) + \tilde{\sigma}(x)\tilde{g}(x^{-1})$$

因此

$$\tilde{g}(x^{-1}) = -\sigma(x^{-1})f(x)\tau(x^{-1}) = \tilde{f}(x^{-1}).$$

因此，对于所有 $x \in X \cup X^{-1}$， $\tilde{g}(x) = \tilde{f}(x)$。

˜按照引理 3.3 证明中的步骤，由于 $\tilde{g} \neq f$，因此存在某个˜ ˜$w_0 \in F(X)$，使得对于所有长度严格小于 w_0 的字 $w \in F(X)$，都有 $\tilde{g}(w_0) \neq f(w_0)$ 且 $\tilde{g}(w) = f(w)$。由于 $w_0 \in F(X)$，因此对于某个 $x_i \in X \cup X^{-1} (1 \leq i \leq m_0)$，有 $w_0 = \prod_{i=1}^{m_0} x_i$，其中 m_0 是字 w_0 的长度。由于 $\prod_{i=1}^{m_0-1} x_j$，存在 $x_{m_0} \in F(X)$，其长度严格小于 w_0 的长度 m_0，因此根据我们对 w_0 的选择，

$$\tilde{g}(\prod_{i=1}^{m_0-1} x_j) = \tilde{f}(\prod_{i=1}^{m_0-1} x_j) \qquad \text{and} \qquad \tilde{g}(x_{m_0}) = \tilde{f}(x_{m_0}).$$

这给出

$$\begin{aligned}\tilde{g}(w_0) &= \tilde{g}(\prod_{i=1}^{m_0} x_i) = \tilde{g}((\prod_{i=1}^{m_0-1} x_i)x_{m_0}) \\ &= \tilde{g}(\prod_{i=1}^{m_0-1} x_j)\tilde{\tau}(x_{m_0}) + \tilde{\sigma}(\prod_{i=1}^{m_0-1} x_j)\tilde{g}(x_{m_0}) \\ &= \tilde{f}(\prod_{i=1}^{m_0-1} x_j)\tilde{\tau}(x_{m_0}) + \tilde{\sigma}(\prod_{i=1}^{m_0-1} x_j)\tilde{f}(x_{m_0}) \\ &= \tilde{f}(\prod_{i=1}^{m_0} x_i) = \tilde{f}((\prod_{i=1}^{m_0-1} x_i)x_{m_0}) \\ &= \tilde{f}(w_0).\end{aligned}$$

但这与以下事实矛盾：$\tilde{g}(w_0) \neq f(w_0)$。因此，$\tilde{f}$ 是 f 的唯一延拓：$X \to RG$ 从 $F(X)$ 到 RG，且满足 (3.4)。 □

定理 3.6。在引理 3.5的假设下，映射 $f: X \to RG$ 可延拓为一个 (σ,τ)-导子 D，其定义在 RG 上，当且仅当 $f(y) = 0$ 对所有 $y \in Y$ 都成立。

证明。首先，假设给定的映射 $f: X \to RG$ 可以延拓为 RG 上的 (σ,τ)-导子 D。于是，对所有 $x \in X$，$D(x) = f(x)$。此外，对于任意 $x \in X$，

$$0 = D(1) = D(xx^{-1}) = D(x)\tau(x^{-1}) + \sigma(x)D(x^{-1})$$

使得

$$D(x^{-1}) = -\sigma(x^{-1})D(x)\tau(x^{-1}) = -\sigma(x^{-1})f(x)\tau(x^{-1}) = \tilde{f}(x^{-1}).$$

因此，对所有 $x \in X \cup X^{-1}$，$D(x) = \tilde{f}(x)$。

现在，令 $y \in Y$。那么 $y = \prod_{i=1}^{k} y_i$ 对于某个 $y_i \in X \cup X^{-1}\,(1 \le i \le k)$。由 (3.6) 和引理 3.2(i),

$$\begin{aligned}\tilde{f}(y) = \tilde{f}(\prod_{i=1}^{k} y_i) &= \sum_{i=1}^{k}\left(\left(\prod_{j=1}^{i-1}\sigma(y_j)\right)\tilde{f}(y_i)\left(\prod_{j=i+1}^{k}\tau(y_j)\right)\right) \\ &= \sum_{i=1}^{k}\left(\left(\prod_{j=1}^{i-1}\sigma(y_j)\right)D(y_i)\left(\prod_{j=i+1}^{k}\tau(y_j)\right)\right) \\ &= D(\prod_{i=1}^{k} y_i) = D(y) = D(1) = 0.\end{aligned}$$

因此，对所有 $y \in Y$，都有 $\tilde{f}(y) = 0$。

反过来，假设 $\tilde{f}(y) = 0$ 对所有 $y \in Y$ 均成立。注意，$\tilde{\sigma}(y) = \sigma(y) = 1$ 且 $\tilde{\tau}(y) = \tau(y) = 1$ 对所有 $y \in Y$ 均成立。因此，对于任意 $y \in Y$，

$$0 = \tilde{f}(1) = \tilde{f}(yy^{-1}) = \tilde{f}(y)\tilde{\tau}(y^{-1}) + \tilde{\sigma}(y)\tilde{f}(y^{-1}) = \tilde{f}(y^{-1}).$$

因此，$\tilde{f}(y^{-1}) = 0$ 对所有 $y \in Y$ 均成立。

与定理 3.4 的证明中一样，令 $Y^F(X)$ 为 Y 在 $F(X)$ 中的正规闭包。于是 $_{Y^F}(X)$ $= \langle w^{-1}yw \mid w \in F(X)\ y \in Y \rangle$，且它是唯一的满群同态 $\phi\colon F(X) \to G$ 的核，该同态在 X 上为恒等映射，也就是说，$G \cong {}^F(X)_{Y^F}(X)$。令 $\varepsilon \in \{1, -1\}$。于是 $\tilde{}$，利用~~(3.4)~~ 以及对所有 $y \in Y$ 都有 $f(y^\varepsilon) = 0$ 这一事实，我们得到对于任意 $w \in F(X)$,

$$\begin{aligned}\tilde{f}(w^{-1}y^\varepsilon w) &= \tilde{f}(w^{-1})\tilde{\tau}(y^\varepsilon w) + \tilde{\sigma}(w^{-1})\tilde{f}(y^\varepsilon w)\\ &= \tilde{f}(w^{-1})\tilde{\tau}(w) + \tilde{\sigma}(w^{-1})(\tilde{f}(y^\varepsilon)\tilde{\tau}(w) + \tilde{\sigma}(y^\varepsilon)\tilde{f}(w))\\ &= \tilde{f}(w^{-1})\tilde{\tau}(w) + \tilde{\sigma}(w^{-1})\tilde{f}(w)\\ &= \tilde{f}(w^{-1}w) = \tilde{f}(1) = 0.\end{aligned}$$

现在，令 $v \in Y^F(X)$。于是 $v = \prod_{i=1}^m w_i^{-1}y_i^\varepsilon w_i$ 对于某个 $m \in \mathbb{N}$, $w_i \in F(X)$, $y_i \in Y (1 \le i \le m)$。如上所示，该结论对 $m = 1$成立。假设该结论对 $m = k - 1$成立，也就是说，$\tilde{f}(\prod_{i=1}^{k-1} w_i^{-1}y_i^\varepsilon w_i) = 0$。于是利用 (3.6) 和归纳假设，我们得到对于 $m = k$,

$$\begin{aligned}\tilde{f}(v) = \tilde{f}(\prod_{i=1}^{k} w_i^{-1}y_i^\varepsilon w_i) &= \tilde{f}((\prod_{i=1}^{k-1} w_i^{-1}y_i^\varepsilon w_i)(w_k^{-1}y_k^\varepsilon w_k))\\ &= \tilde{f}(\prod_{i=1}^{k-1} w_i^{-1}y_i^\varepsilon w_i)\tilde{\tau}(w_k^{-1}y_k^\varepsilon w_k) + \tilde{\sigma}(\prod_{i=1}^{k-1} w_i^{-1}y_i^\varepsilon w_i)\tilde{f}(w_k^{-1}y_k^\varepsilon w_k)\\ &= 0\tilde{\tau}(w_k^{-1}y_k^\varepsilon w_k) + \tilde{\sigma}(\prod_{i=1}^{k-1} w_i^{-1}y_i^\varepsilon w_i)0 = 0.\end{aligned}$$

因此，对于所有 $v \in Y^F(X)$, $\tilde{f}(v) = 0$。此外，对于所有 $v \in Y^F(X)$, $\tilde{\sigma}(v) = \tilde{\tau}(v) = 1$。因此，对于任意 $w \in F(X)$ 和 $v \in Y^F(X)$,

$$\tilde{f}(wv) = \tilde{f}(w)\tilde{\tau}(v) + \tilde{\sigma}(w)\tilde{f}(v) = \tilde{f}(w)1 + \tilde{\sigma}(w)0 = \tilde{f}(w).$$

设 $g \in G$ 和 $g = \prod_{i=1}^m x_i$，其中某个 $m \in \mathbb{N}$, $x_i \in X \cup X^{-1}$ $(1 \le i \le m)$。因此，g 是 X 上的一个字，使得 $g \in F(X)$。实际上，g 是 $F(X)$ 中满足 $\phi(g) = g$ 的约化词。若 $w \in F(X)$ 满足 $\phi(w) = g$，则 w 等价于约化词 g，或者 w 的表达式（作为来自 $X \cup X^{-1}$ 的元素之积）包含来自 $Y^F(X)$ 的元素。无论哪种情况，$\tilde{\sigma}(w) = \sigma(g)$，且 $\tilde{\tau}(w) = \tau(g)$。

现在，定义 $D\colon G \to RG$ 为

$$D(g) = \tilde{f}(w)$$

其中，对于 $g \in G$, $w \in F(X)$ 满足 $\phi(w) = g$。这样的 w 存在，因为 $\phi\colon F(X) \to G$ 是一个满群同态；或者如上段所述，我们可以取 $w = g$。$\tilde{}$映射 D 是良定义的，因为如前所示，$f\colon F(X) \to RG$ 是一个良定义映射，且对于所有 $v \in Y^F(X)$，都有 $\tilde{f}(wv) = \tilde{f}(w)$。

现在，令 $g, h \in G$。那么存在某个 $u, w \in F(X)$，使得

$$\phi(u) = g \qquad \text{and} \qquad \phi(w) = h.$$

Then

$$\tilde{\sigma}(u) = \sigma(g), \quad \tilde{\tau}(w) = \tau(h) \quad \text{and} \quad \phi(uw) = \phi(u)\phi(w) = gh.$$

因此，根据 D的定义，

$$D(g) = \tilde{f}(u), \quad D(h) = \tilde{f}(w) \quad \text{and} \quad D(gh) = \tilde{f}(uw).$$

最后利用（3.4），得到

$$D(gh) = \tilde{f}(uw) = \tilde{f}(u)\tilde{\tau}(w) + \tilde{\sigma}(u)\tilde{f}(w) = D(g)\tau(h) + \sigma(g)D(h).$$

因此，对于所有的 $g, h \in G$， $D(gh) = D(g)\tau(h) + \sigma(g)D(h)$。

现在，将其线性延拓至整个 RG。我们仍用 D 表示延拓后的映射。因此，若 $\lambda \in R$，且对于某些 λ_g, $\mu_h \in R\,(g, h \in G)$ 有 $\alpha = \sum_{g\in G} \lambda_g g$, $\beta = \sum_{h\in G} \mu_h h \in RG$，则$D(\alpha + \beta) = D(\alpha) + D(\beta)$，并且 $D(\lambda\alpha) = \lambda D(\alpha)$，因为 D 是一个 R-线性映射。此外，

$$\begin{aligned}
D(\alpha\beta) &= D((\sum_{g\in G} \lambda_g g)(\sum_{g\in G} \mu_h h)) \\
&= D(\sum_{g,h\in G} \lambda_g \mu_h (gh)) = \sum_{g,h\in G} \lambda_g \mu_h D(gh) \\
&= \sum_{g,h\in G} \lambda_g \mu_h (D(g)\tau(h) + \sigma(g)D(h)) \\
&= \sum_{g,h\in G} \lambda_g \mu_h D(g)\tau(h) + \sum_{g,h\in G} \lambda_g \mu_h \sigma(g)D(h) \\
&= D(\sum_{g\in G} \lambda_g g)\tau(\sum_{h\in G} \mu_h h) + \sigma(\sum_{g\in G} \lambda_g g)D(\sum_{h\in G} \mu_h h) \\
&= D(\alpha)\tau(\beta) + \sigma(\alpha)D(\beta).
\end{aligned}$$

因此， D 是 RG 的一个 (σ, τ)-导子，它将 $f\colon X \to RG$ 延拓至整个 RG。

现在，只需证明 $\tilde{D}$ 的唯一性。假设存在另一个 (σ, τ)-导子，它将 $\tilde{f}\colon X \to RG$ 延拓。于是存在某个 $g_0 \in G$，使得 $D(g_0) \neq D(g_0)$，且对于所有长度严格小于 g_0 的 $g \in G$，都有 $D(g) = D(g)$。

注意到 $1 \in X$，有 $\tilde{D}(1) = 0$。此外，$f(x) = D(x)$。现在，对于任意$x \in X$，

$$0 = \tilde{D}(1) = \tilde{D}(xx^{-1}) = \tilde{D}(x)\tau(x^{-1}) + \sigma(x)\tilde{D}(x^{-1}) = f(x)\tau(x^{-1}) + \sigma(x)\tilde{D}(x^{-1})$$

从而 $\tilde{D}(x^{-1}) = -\sigma(x^{-1})f(x)\tau(x^{-1}) = \tilde{f}(x^{-1}) = D(x^{-1})$。

我们可以将 $g_0 \in G$ 写成 $g_0 = x_0 y_0$，其中存在某些 x_0、$y_0 \in G$，使得 x_0 和 y_0 的长度都严格小于 g_0的长度。然后根据我们的假设， $D(x_0) = D(x_0)$，且 $D(y_0) = D(y_0)$。因此，

$$\begin{aligned}
\tilde{D}(g_0) &= \tilde{D}(x_0 y_0) \\
&= \tilde{D}(x_0)\tau(y_0) + \sigma(x_0)\tilde{D}(y_0)
\end{aligned}$$

$$
\begin{aligned}
&= D(x_0)\tau(y_0) + \sigma(x_0)D(y_0) \\
&= D(x_0y_0) \\
&= D(g_0).
\end{aligned}
$$

˜但这与 $D(g_0) \neq D(g_0)$这一事实矛盾。因此， $D: RG \to RG$ 是将给定映射 $f: X \to RG$延拓的唯一（σ， τ）-导子。

因此得证。 □

注 3.7。 环 R 是交换环这一假设对于定理 3。6是必要的。例如，设 R 是一个非交换环，且 a， $b \in R$ 满足 $ab \neq ba$。设 $X = \{x, y\}$ 和 $G = F(X)$ 是由 X生成的自由群。定义 $f: X \to RG$ 如下:

$$f(x) = a \quad and \quad f(y) = b.$$

定义 σ 和 τ 为 G 的两个群自同态，如下:

$$\sigma(x) = x,\ \sigma(y) = y \quad and \quad \tau(x) = y,\ \tau(y) = x.$$

若可能，假设 f可扩张为 RG的一个 (σ, τ)-导子 D。那么

$$
\begin{aligned}
D(xby) = D(bxy) &= bD(xy) \\
&= b(D(x)\tau(y) + \sigma(x)D(y)) \\
&= b(f(x)\tau(y) + \sigma(x)f(y)) \\
&= b(ax + xb) = bax + bxb \\
&= (ba + b^2)x
\end{aligned}
$$

and

$$
\begin{aligned}
D(x)\tau(by) + \sigma(x)D(by) &= D(x)b\tau(y) + \sigma(x)bD(y) \\
&= f(x)b\tau(y) + \sigma(x)bf(y) \\
&= abx + xb^2 \\
&= (ab + b^2)x.
\end{aligned}
$$

由于 $ab \neq ba$，因此， $D(xby) \neq D(x)\tau(by) + \sigma(x)D(by)$。这就产生了矛盾。

3.4 应用： σ-导子与交换群代数

在本小节中，我们应用小节 3.2 的结果来分类交换群代数上的 σ-导子。本小节中，我们假设 R 是一个交换含幺环， G 是一个群，并且 σ 是一个 R-代数端同态， RG 它是 R-线性扩张，来自 G的群自同态。

定理 3.8. 设 H 是 G 的一个子群，使得 $\sigma(H) = \{\sigma(h) \mid h \in H\}$ 是 G 的一个挠中心子群，并且 $\sigma(H)$ 中每个元素的阶在 R 中可逆。那么，σ 的每个 RG 导子都是一个 RH 导子，即对于所有 $D \in \mathcal{D}_\sigma(RG)$， $D(RH) = \{0\}$ 。

证明. 设 $D \in \mathcal{D}_\sigma(RG)$ 和 $h \in H$。 $\sigma(h)$ 的阶有限，设为 r，且在R 中可逆。由于 $\sigma(h)$ 与 $D(h)$ 交换，因此由引理 3.2(v),

$$0 = D(1) = D(h^r) = r(\sigma(h))^{r-1}D(h).$$

由于 $r = |\sigma(h)|$ 在 R 中可逆，因而在 RG 中也可逆，所以由上文可得 $D(h) = 0$。因此，对所有 $h \in H$，都有 $D(h) = 0$。

现在，设 $\alpha \in RH$。那么，对某个 $\lambda_h \in R$ （$h \in H$）有 $\alpha = \sum_{h\in H} \lambda_h h$。由于 D 是 R-线性的，因此

$$D(\alpha) = D(\sum_{h\in H} \lambda_h h) = \sum_{h\in H} \lambda_h D(h) = \sum_{h\in H} \lambda_h 0 = 0.$$

因此， $D(RH) = \{0\}$。 □

推论 3.9. 若 G 是有限阿贝尔群，且 $\mathbb{F}$ 是特征为 0 的域，则 $\mathbb{F}G$ 没有非零的 σ-导子。

证明。 由定理 $H = G$ 中取 3。8 即得。 □

注意，推论 3.9 并非一个判据。也就是说，若 $\mathbb{F}$ 是任意域， G 是任意群，且σ 是 RG 的任意端同态，它是 R-线性的群G自同态的扩张，那么并不一定有 G 是有限阿贝尔群，或 $\mathbb{F}$ 是特征为 0 的域。下面给出一些例子来说明这一点。

例 3.10 和3.11 说明了以下情形：当 $\mathbb{F}G$ 没有非零 σ-导子，且 G 是有限阿贝尔群，但域 $\mathbb{F}$ 的特征不为 0 时。

群的子群 H 称为关于有理素数 p 的 p-正则子群，如果 H 中的每个元素的阶都不是 p 的倍数。

例 3.10。设 p 和 q 是两个不同的有理素数。设 $G = C_{q^t} = \langle x \mid x^{q^t} = 1\rangle$是阶为 q^t 的循环群（其中 $t \in \mathbb{N}$）， $\mathbb{F}$ 是特征为 p的域。那么， G 是一个 p-正则有限阿贝尔群。此外，设 σ 是 $\mathbb{F}G$的一个 $\mathbb{F}$-代数端同态，它是 G的一个群自同态的 $\mathbb{F}$-线性扩张。

由定理 3.8可知，每个 σ-导子 $\mathbb{F}G$都是一个 $\mathbb{F}G$-导子，即 $D(\mathbb{F}G) = \{0\}$对所有 $D \in \mathcal{D}_\sigma(RG)$ 都成立。换言之， $\mathbb{F}G$ 没有非零 σ-导子。

注意，在这里， $\mathbb{F}G$ 没有非零的 σ-导子，且 G 是一个有限阿贝尔群，但域 $\mathbb{F}$ 的特征不为 0；$\mathbb{F}$ 是一个特征为 p （奇有理素数）的域。

下面的例子是例 3.10 的一个更一般化的版本。

例3.11. 设 p、 q_1、 ...、 q_s （$s \in \mathbb{N}$）是互不相同的奇有理素数，且 t_1、 ...、 t_s 是正整数。对于每个 $i \in \{1, ..., s\}$，令 $C_{q^{t_i}} = \langle x_i \mid x_i^{t_i} = 1\rangle$ 表示一个阶为 q^{t_i}的循环群。设 $G = C_{q^{t_1}} \times ... \times C_{q^{t_s}}$是一个阶为$q^{t_1}...q^{t_s}$的有限阿贝尔群。那么 G成为一个 p-正则群。此外，设 $\mathbb{F}$是一个特征为 p 的域，且 σ 是 $\mathbb{F}G$ 的一个 $\mathbb{F}$-线性扩张的群自同态的 $\mathbb{F}$-代数端同态。

由定理 3.8可知，每个 σ-导子都是 $\mathbb{F}G$-导子，也就是说， $\mathbb{F}G$-导子满足 $D(\mathbb{F}G) = \{0\}$对所有 $D \in \mathcal{D}_\sigma(RG$均成立。换言之， $\mathbb{F}G$ 没有非零的 σ-导子。

再次注意， $\mathbb{F}G$ 没有非零的 σ导子，且 G 是有限阿贝尔群，但域 $\mathbb{F}$ 的特征不为 0； $\mathbb{F}$ 是特征为 p （奇有理素数）的域。

例 3.12 和 3.13在下文中展示了以下两种情形：

1. $\mathbb{F}G$ 没有非零的 σ-导子，且 $\mathbb{F}$ 是特征为 0 的域，但群 G不是有限阿贝尔群。

2. $\mathbb{F}G$没有非零的 σ-导子，但域 $\mathbb{F}$ 的特征不为 0，且群 G 不是有限阿贝尔群。

例 3.12. 考虑阶为$2n$ $(n \geq 3)$的二面体群 $D_{2n} = \langle a, b \mid a^n = 1 = b^2, (ab)^2 = 1\rangle$，其中 n 为奇数。设 $\mathbb{F}$ 是特征为 0 的域，或是奇有理素数 p。

映射 $\sigma_{-1}: D_{2n} \to D_{2n}$ 由 $\sigma_{-1}(a) = 1$ 和 $\sigma_{-1}(b) = 1$ 给出，是群 D_{2n}的平凡群自同态。将其扩张为 σ_{-1} $\mathbb{F}$-线性的 $\mathbb{F}D_{2n}$的 $\mathbb{F}$-代数端同态。

由于 $\sigma_{-1}(b) = \sigma_{-1}(ab) = 1 \in D_{2n} \cap Z(\mathbb{F}D_{2n})$，因此根据定义 5.1 后的注记，

$C(\sigma_{-1}(b)) = C(\sigma_{-1}(ab)) = \{0\}$，其中对于任意的 $\beta \in \mathbb{F}D_{2n}$，$C(\beta) = \{\alpha \in \mathbb{F}D_{2n} \mid \alpha\beta = -\beta\alpha\}$表示 β 在 $\mathbb{F}D_{2n}$ 中的反中心化子（见定义 5.1）。

首先，我们确定 $\mathcal{D}_{\sigma_{-1}}(\mathbb{F}D_{2n})$。为此，设 $f: X = \{a, b\} \to \mathbb{F}D_{2n}$是一个可延拓为 σ_{-1}-导子的映射。根据定理 $\mathbb{F}D_{2n}$，由定理 3.4，这当且仅当

$$\tilde{f}(a^n) = 0, \quad \tilde{f}(b^2) = 0 \quad \text{and} \quad \tilde{f}((ab)^2) = 0,$$

其中 $f: F(X) \to \mathbb{F}D_{2n}$ 是 f 的唯一延拓，在（3.2）和（3.3）中定义并满足（3.1），且 $F(X)$ 是由 X生成的自由群。

如引理 5.2 的证明后段所述，$\tilde{f}(b^2) = 0$ 当且仅当$f(b) \in \bar{C}(\sigma_{-1}(b))$，并且 $\tilde{f}((ab)^2) = 0$当且仅当 $\tilde{f}(ab) \in \bar{C}(\sigma_{-1}(ab))$。但由于 $\bar{C}(\sigma_{-1}(b)) = C(\sigma_{-1}(ab)) = \{0\}$，因此，$f(b) = f(ab) = 0$。

进而，由(3.2)，$f(a) = 0$。因此，$\tilde{f}(ab)\sigma_{-1}(b) - \sigma_{-1}(a)f(b)\sigma_{-1}(b)$。但是，由于 $f(b) = 0 = \tilde{f}(a)$

由于 $f(a) = 0 = f(b)$，因此，$\mathbb{F}D_{2n}$没有非零的 σ_{-1}-导子，也就是说，$\mathcal{D}_{\sigma_{-1}}(\mathbb{F}D_{2n}) = \{0\}$。因此，$\mathbb{F}D_{2n}$ 没有非零的 σ_{-1}-导子。

但请注意，此处的群 D_{2n} 不是阿贝尔群。此外，域 $\mathbb{F}$ 的特征可以是 0，也可以是奇有理素数 p。

例 3.13. 现在，考虑二面体群 D_{2n}，其中 n 为偶数，且域 $\mathbb{F}$的特征为 0 或奇有理素数 p。

如第 5 节所述，映射 $\sigma_2: D_{2n} \to D_{2n}$ 由 $\sigma_2 = a^s$ $(s = 0, \frac{n}{2})$ 和$\sigma_2(b) = a^t$ $(t = 0, \frac{n}{2})$ 定义，是群 D_{2n} 的群自同态。将 σ_2 $\mathbb{F}$-线性地扩张为一个 $\mathbb{F}$-代数端同态 $\mathbb{F}D_{2n}$。

再者，由于 $\sigma_2(b) = \sigma_2(ab) \in D_{2n} \cap Z(\mathbb{F}D_{2n})$，根据定义 5.1 后的注释，$C(\sigma_2(b)) = C(\sigma_2(ab)) = \{0\}$。因此，如上面的例 3.12 所示，可以用类似的方法证明 $\mathcal{D}_{\sigma_2}(\mathbb{F}D_{2n}) = \{0\}$。因此，$\mathbb{F}D_{2n}$ 没有非零的 σ_2-导子。

再者，注意这里的群 D_{2n} 是非阿贝尔群，而域 $\mathbb{F}$ 的特征可以是 0 或奇有理素数 p。

以下推论是定理 3.8 的直接推论，并推广了例 3.10 和3.11。

推论 3.14. 设 G 是一个有限阿贝尔群， H 是群 G 的一个 p-正则子群，其中p 是一个有理素数。设 $\mathbb{F}$ 是一个特征为 p 的域。那么， $\mathbb{F}G$ 的每个 σ-导子都是一个 $\mathbb{F}H$-导子。

根据有限阿贝尔群基本定理，每个有限阿贝尔群 G 都同构于一个 p-正则群与一个 p-群的直积，其中 p 是有理素数；也就是说， $G \cong H \times K$，其中 H 是 p-正则群，而 K 是 p-群。群 K 的表示为 $K = \langle X \mid Y \rangle$，其中 $X = \{x_1, ..., x_r\}$ 是 K 的一组生成元， $r \in \mathbb{N}$ 取某个值，且 $Y = \{x_i^{p^{r_i}}, x_i^{-1}x_j^{-1}x_ix_j,$ 取某个值，其中 $r_i \in \mathbb{N}$、 $i \in \{1, ..., r\}\}$。现在，我们有如下定理，它对上述形式的 $\mathbb{F}G$ 上的所有 σ-导子进行了分类，其中 $\mathbb{F}$ 是特征为 p 的域，而 G 是一个有限阿贝尔群。

定理 3.15。 $\mathcal{D}_\sigma(\mathbb{F}G)$ 的维数为 $r|G|$ ， 一组基为

$$\mathcal{B} = \{gD_i \mid g \in G, 1 \le i \le r\},$$

其中，对每个 $i \in \{1, ..., r\}$、 D_i： $\mathbb{F}G \to \mathbb{F}G$ 是由 $D_i(x_j) = \delta_{ij}$ 定义的 σ-导子，其中 $\mathbb{F}G$ 是克罗内克 delta。

证明。 根据推论 3。14，每个 σ-导子 $\mathbb{F}G$ 都是一个 $\mathbb{F}H$-导子。

对每个 $i \in \{1, ..., r\}$，定义 f_i： $X \to \mathbb{F}G$ 为

$$f_i(x_j) = \delta_{ij}, \quad \text{that is,} \quad f_i(x_j) = \begin{cases} 1 & \text{if } j = i \\ 0 & \text{if } j \neq i \end{cases}.$$

˜于是，根据引理 3。3，每个 f_i 都可以唯一地扩展为映射 f_i ： $F(X) \to \mathbb{F}G$ ，且满足（3.1）。令 i， k， $l \in \{1, ..., r\}$。于是根据（3.3），

$$\tilde{f}_i(x_k^{p^{r_k}}) = \sum_{t=1}^{p^{r_k}} \left(\left(\prod_{j=1}^{t-1} \sigma(x_k) \right) \tilde{f}_i(x_k) \left(\prod_{j=t+1}^{p^{r_k}} \sigma(x_k) \right) \right) = p^{r_k}((\sigma(x_k))^{p^{r_k}-1} f_i(x_k) = 0,$$

and

$$\begin{aligned}
\tilde{f}_i(x_k^{-1}x_l^{-1}x_kx_l) &= \tilde{f}_i(x_k^{-1})\tilde{\sigma}(x_l^{-1}x_kx_l) + \tilde{\sigma}(x_k^{-1})\tilde{f}_i(x_l^{-1}x_kx_l) \\
&= \tilde{f}_i(x_k^{-1})\sigma(x_l^{-1}x_kx_l) + \sigma(x_k^{-1})(\tilde{f}_i(x_l^{-1})\tilde{\sigma}(x_kx_l) + \tilde{\sigma}(x_l^{-1})\tilde{f}_i(x_kx_l)) \\
&= -\sigma(x_k^{-1})f_i(x_k)\sigma(x_k^{-1})\sigma(x_l^{-1}x_kx_l) + \sigma(x_k^{-1})\tilde{f}_i(x_l^{-1})\sigma(x_kx_l) \\
&\quad + \sigma(x_k^{-1})\sigma(x_l^{-1})\tilde{f}_i(x_kx_l) \\
&= -\sigma(x_k^{-1})f_i(x_k) - \sigma(x_l^{-1})f_i(x_l)\sigma(x_l^{-1})\sigma(x_l) + \sigma(x_k^{-1})\sigma(x_l^{-1})(\tilde{f}_i(x_k)\tilde{\sigma}(x_l) \\
&\quad + \tilde{\sigma}(x_k)\tilde{f}_i(x_l)) \\
&= -\sigma(x_k^{-1})f_i(x_k) - \sigma(x_l^{-1})f_i(x_l) + \sigma(x_k^{-1})f_i(x_k) + \sigma(x_l^{-1})f_i(x_l) = 0.
\end{aligned}$$

˜因此我们证明了 $f_i(y) = 0$ 对所有 $y \in Y$和 $i \in \{1, ..., r\}$. 因此，根据定理 3.4，对于每个 $i \in \{1, ..., r\}$，映射 f_i: $X \to \mathbb{F}G$ 都可以唯一地扩张为一个 σ-导子 D_i，其作用于 $\mathbb{F}G$。

令 $\mathcal{B} = \{gD_i \mid g \in G, 1 \leq i \leq r\}$。我们证明， $\mathcal{B}$ 是 $\mathbb{F}$-向量空间$\mathcal{D}_\sigma(\mathbb{F}G)$的一组基。

由于对每个 $i \in \{1, ..., r\}$， D_i都是 f_i 的扩张，因此，对所有 $1 \leq i$、 $j \leq r$， $D_i(x_j) = f_i(x_j) = \delta_{ij}$。

现在，设 $D \in \mathcal{D}_\sigma(\mathbb{F}G)$ 且 i、 $j \in \{1, ..., r\}$。设对某个 $\lambda_{jg} \in \mathbb{F}(g \in G)$， $D(x_j) = \sum_{g\in G} \lambda_{jg} g$。那么

$$D(x_j) = \sum_{g\in G} \lambda_{jg} g1 = \sum_{g\in G} \lambda_{jg} gD_j(x_j) = \left(\sum_{g\in G} \lambda_{jg}(gD_j)\right)(x_j).$$

进一步，

$$0 = D_i(1) = D_i(x_j x_j^{-1}) = D_i(x_j)\sigma(x_j^{-1}) + \sigma(x_j)D_i(x_j^{-1})$$

从而

$$D_i(x_j^{-1}) = -\sigma(x_j^{-1})D_i(x_j)\sigma(x_j^{-1}) = -\sigma(x_j^{-2})D_i(x_j) = -\sigma(x_j^{-2})\delta_{ij}.$$

类似地， $D(x_j^{-1}) = -\sigma(x_j^{-2})D(x_j)$，从而

$$D(x_j^{-1}) = \sum_{g\in G} \lambda_{jg} g(-\sigma(x_j^{-2})) = \sum_{g\in G} \lambda_{jg} gD_j(x_j^{-1}) = (\sum_{g\in G} \lambda_{jg}(gD_j))(x_j^{-1}).$$

现在，由于 X 是群 K 的生成集，因此，对任意 $g_0 \in G$，因为 D 是一个 $\mathbb{F}H$-导子，所以对某些 $s \in \mathbb{N}$、 $i_l \in \{1, ..., r\}$、 $x_{i_l} \in X$，有 $D(g_0) = D(x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} ... x_{i_s}^{\varepsilon_s})$，且 $\varepsilon_l \in \{-1, 1\}$ ($1 \leq l \leq s$)。因此现在立即可得

$$D = \sum_{i=1}^{r} \sum_{g\in G} \lambda_{ig}(gD_i).$$

因此，集合 $\mathcal{B}$ 在 $\mathbb{F}$ 上张成 $\mathcal{D}_\sigma(\mathbb{F}G)$。

现在，假设

$$\sum_{i=1}^{r} \sum_{g\in G} c_{ig}(gD_i) = 0$$

对于某个 $c_{ig} \in \mathbb{F}$ ($1 \leq i \leq r$ 和 $g \in G$)。那么

$$\sum_{i=1}^{r} \sum_{g\in G} c_{ig}(gD_i)(x_j) = 0$$

对所有 $1 \leq j \leq r$。接着利用 $D_i(x_j) = \delta_{ij} (1 \leq i, j \leq r)$ 这一事实，我们得到 t

$$\sum_{g\in G} c_{jg} g = 0$$

对所有 $1 \leq j \leq r$， $c_{jg} = 0$ 对所有 $g \in G$。 □

最后，我们将本节的结果与此前关于交换代数扭导子的若干已知结果进行比较。在此之前，人们曾多次尝试描述 R-代数 $\mathcal{A}$ （R 一个环）的普通导子或扭导子的 R-模。例如，在 [18, 第 3.1], 小节中，作者研究了交换群代数的普通导子。本文第 3.4 小节将 [18, 第 3.1] 小节的结果推广到了σ-导子，并给出了更详尽、完整的论证。在 [14], 中，作者研究了交换含幺环上的交换代数的（σ,τ）-导子。在 [14, 定理 3.1], 中，作者研究了交换环上的交换代数的（σ,τ）-导子的泛映射性质。作者还通过将（σ,τ）-导子所作用的二次数域代数整数环 $O_K=\mathbb{Z}[\sqrt{d}]$ （d 一个无平方因子整数）视为一个（交换） $\mathbb{Z}$-代数，研究了该环的导子。更确切地说，在 [14, 定理 4.2], 中，作者证明，若 σ,τ是 O_K的两个不同环自同态，那么任何满足 $D(1)=0$的 $\mathbb{Z}$-线性映射 $D\colon O_K\to O_K$都是 O_K的（σ,τ）-导子；作者还给出了使 O_K的（σ,τ）-导子为内导子的一个充分条件。这些环 O_K提供了若干非唯一分解整环的例子。在 [52], 中，作者描述了任意阿贝尔群 G的 $\mathbb{Z}G$ 的导子。在 [16, 定理 4.6], 中，作者给出了 RG 中的一个元素（它是交换含幺环 R 上阿贝尔群 G 的交换群代数，且满足某些条件）；在存在某个 $b\in RG$使得 $(\tau-\sigma)(b)$ 在 RG中可逆的条件下，该元素使 RG 的（σ,τ）-导子成为内导子，其中 σ,τ 是 RG的 R-代数自同态。在 [48], 中，作者证明了交换代数的 σ-导子上的某个括号保持内导子不变（见命题 2.3.1），并以此得到了结构性结果，为单变量劳朗多项式上的 σ-导子提供了新的见解；$\mathbb{C}[t,t^{-1}]$ 它是一个唯一分解整环。在 [27], 中，作者基于扭导子提出了 Witt 代数和 Virasoro代数的变形方法。作者证明，若 $\mathcal{A}$ （一个 $\mathbb{C}$上的代数）是唯一分解整环（UFD），那么 $\mathcal{A}$ 的所有（$\sigma,id_{\mathcal{A}}$）-导子所成的 $\mathcal{A}$-模$\mathcal{D}_{(\sigma,id_{\mathcal{A}})}(\mathcal{A})$是秩一自由 $\mathcal{A}$-模。这里， σ 和 τ 是 $\mathcal{A}$的两个不同代数自同态，生成元是由 $\Delta=\frac{\tau-\sigma}{g}$给出的一个（$\sigma,\tau$）-导子，其中$g=$是$((\tau-\sigma)(\mathcal{A}))$的最大公因数（见定理 4）。作者还利用扭导子定义了广义Witt代数。在 [48], 中，作者进一步指出，一个（$\sigma,id_{\mathcal{A}}$）-导子 $a\Delta$是内导子，当且仅当 g 整除 a。更确切地说，所有内（$\sigma,id_{\mathcal{A}}$）-导子构成的 $\mathcal{A}$-子模为秩一，其生成元为 $g\mathcal{A}\Delta$（见命题 2.4.1）。随后，作者针对代数 $\mathcal{A}=\mathbb{C}[t,t^{-1}]$得到了更深入、精确的结果；该代数也是唯一分解整环。请注意，在本文中，我们将群环 RG 的（σ,τ）-导子集视为一个 R-模，而非RG-模；其中 R 是交换含幺环， G 是群。

有几篇论文，尤其是 A. A. Arutyunov 的论文（如引言第 1 节所述），对群代数的导子进行了描述。在[1], 中，作者研究了离散可数群 G 的群代数 $\mathbb{C}G$ 上的 (σ,τ)-导子和 (σ,id)-导子，其中 σ、 τ 是 $\mathbb{C}G$ 上的 $\mathbb{C}$-代数自同态，且它们是群自同态的 $\mathbb{C}$-线性扩张。在 [1, 定理 4], 中，作者证明了一个分解定理，该定理给出了有限生成的 (σ,τ)-FC 群 $\mathbb{C}G$ 上所有 (σ,τ)-导子的 $\mathbb{C}$-向量空间的分解；其中，(σ,τ)-FC 群是指每个 (σ,τ)-共轭类都具有有限大小的群。

在 [3], 中，作者使用拓扑

逻辑与特征方法研究了有限群和 FC 群的普通导子。他们针对交换含幺环 A 上有限群或 FC 群的群环 AG 中的导子，得到了分解定理（FC 群是指每个共轭类都具有有限大小的群） G （参见 [3, 定理 3.2、4.1]）。更确切地说，作者证明，对于有限生成 FC 群 G，其所有导子的 A-模同构于其所有 AG 的内导子构成的 A-子模与 $\bigoplus_{[u]\in G^G}\mathrm{Hom}_{Ab}(Z(u)\ A)$ 的直和，其中 $\mathrm{Hom}_{Ab}(Z(u)\ A)$ 是从固定元素 $u \in G$ 的中心化子 $Z(u)$ 到环 A 的所有加法同态构成的集合，而 G^G 是 G 中所有可能的不同共轭类 $[u]$ $(u \in G)$ 构成的集合（参见 [3, 定理 3.2]）。此外，若 G 是有限群，则其所有外导子的 A-模同构于$\bigoplus_{[u]\in G^G}\mathrm{Hom}_{Ab}(Z(u)\ A)$（参见 [3, 定理 4.1]）。

在 [4] 中也根据群的伴随作用群胚的特征给出了导子的描述，并提出了一种描述有限可呈离散群 G 的复群代数 $\mathbb{C}G$ 的所有外导子空间的方法。在 [5],中，作者研究了有限生成群G的复群代数 $\mathbb{C}G$ 的导子。作者构造了内导子和拟内导子的理想，并建立了导子与伴随作用群胚上的特征之间的联系（见命题 2.11 和推论 3.2）。作者运用组合群论的方法描述了 $\mathbb{C}G$的外导子和拟外导子空间，尤其考察了群 G 的端数以及共轭图各连通分支的端数（例如，见定理 3.6、推论 3.7、定理 4.2、推论 4.3、推论 4.5、推论 4.7、命题 5.1）。在 [6], 中，作者根据群的伴随作用 2-群胚的特征空间，描述了有限呈示离散群的群代数中所有内导子和外导子的空间。在[7], 中，作者建立了复群代数的导子与研究拓扑空间端数的理论之间的联系。在 [7, 定理 5 和 6], 中，作者描述了复群代数的外导子和拟外导子空间。

在 [8], 中，作者根据与该群相关联的群胚上的特征，研究了一般无限非交换离散群 G 的群代数 $\mathbb{C}G$ 中的导子空间。在 [8, 定理 2], 中，作者构造了$\mathbb{C}G$的一个非内导子子代数，该子代数可以嵌入所有外导子构成的代数中。在 [8, 定理 3], 中，作者得到了特征定义导子的必要条件。在 [8,命题 8], 中，作者描述了有限秩自由阿贝尔群的复群代数中所有导子所构成的空间。在 [8, 定理 4 和定理 5], 中，作者明确描述了二阶幂零群的复群代数中所有导子和外导子所构成的空间。在 [9], 中，作者根据该群的伴随作用群胚的凯莱复形，描述了有限呈示离散群 $\mathbb{C}G$ 的群代数中所有外导子所构成的空间（见定理 3、定理 4、推论1、推论 2）。他们证明，外导子空间同$\mathbb{C}$上的凯莱复形的一维紧支撑群同构。在 [41], 中，作者研究了有限生成离散群 $\mathbb{C}G$ 的复群代数的导子。在 [41, 节 3], 中，作者利用该群伴随作用群胚上的特征描述了 $\mathbb{C}G$的导子（见定理 2 和定理 3）。在 [41, 节 4], 中，作者通过建立外导子空间与凯莱复形的一维上同调之间的同构，描述了该空间

该群胚（见推论1）。在 [9, 节 5]和 [41, 节 5], 作者描述了加法群 $\mathbb{Z}$、有限生成自由阿贝尔群和有限生成自由群的复群代数的普通导子空间。

4 群环的内（σ， τ）-导子

设 G 为一个群， R 为一个交换含幺环。除非另有说明，本节始终假设 σ 和 τ 是群代数 RG 的任意两个含幺 R- 代数自同态，它们是群 G 的群自同态的 R- 线性扩张。本节通过给出所有 RG的内（σ， τ）-导子的秩和一个基，对 RG 的所有内（σ， τ）-导子进行分类。此外，我们证明，当 G 的阶在 R中可逆时， RG 的每个（σ， τ）-导子都是一个内（σ， τ）-导子；在这一结果中，σ 和 τ 是 RG 的任意两个含幺 R-代数自同态，并不一定是 G的群自同态。因此，当 G 是一个阶在 R中可逆的有限群时，我们明确地对 RG的所有（σ， τ）-导子进行分类。为证明我们的结果，我们需要双扭共轭类的概念，该概念在第 4.1 小节中引入。

4.1 双扭曲共轭类

定义4.1. 对于 x、 $y \in G$、 x，如果 x 在 G 中与 y (σ、 τ)-共轭，则称

$$y = \sigma(g)x(\tau(g))^{-1}$$

对某个 $g \in G$ 成立。所有与 x (σ、 τ)-共轭的元素构成的集合记为

$$x^G_{(\sigma,\tau)} = \{\sigma(g)x(\tau(g))^{-1} \mid g \in G\}$$

并称其为 x 在 G 中的 (σ、 τ)-共轭类。

特别地，如果 $\tau = \sigma$，则我们简称 (σ、 τ)-共轭为 σ-共轭。注意，(σ、 τ)-共轭是一个等价关系。下面我们陈述一些类似于经典群论中结果的结论。

引理4.2. G 的任意两个 (σ、 τ)-共轭类要么相等，要么不相交，即如果 x、 $y \in G$，则或者 $x^G_{(\sigma,\tau)} = y^G_{(\sigma,\tau)}$，或者 $x^G_{(\sigma,\tau)} \cap y^G_{(\sigma,\tau)} = \emptyset$。

注意，若 1 是 G 中的单位元，则对于任意 $x \in G$, $x = \sigma(1)x(\tau(1))^{-1}$，使得 $x \in x^G_{(\sigma,\tau)}$。因此， G 是其所有 (σ, τ)-共轭类的并。

推论 4.3. G 是其所有 (σ, τ)-共轭类的并，且不同的 (σ, τ)-共轭类两两不相交。

定义 4.4. 若 $G = \bigcup_{i=1}^{r}(x_i)^G_{(\sigma,\tau)}$，使得 ($\sigma, \tau$)-共轭类 $(x_i)^G_{(\sigma,\tau)}$ 的 ($1 \le i \le r$) 互不相同，则称 $x_1, ..., x_r$ 为 G 的 (σ, τ)- 共轭类 $(x_1)^G_{(\sigma,\tau)}, ..., (x_r)^G_{(\sigma,\tau)}$ 的代表元。

我们进一步研究（σ, τ）-共轭这一概念。

引理 4.5. 设 $x, y \in G$ 满足： x 与 y 是 σ-共轭的。那么，对任意 $n \in \mathbb{Z}$， x^n 与 y^n 是 σ-共轭的。此外， x 和 y 的阶相同。

定义 4.6. 设 $x \in G$，则 x 在 G 中的 (σ, τ)-中心化子定义为集合

$$C_{(\sigma,\tau)}(x) = \{g \in G \mid x\tau(g) = \sigma(g)x\}.$$

注意， $C_{(\sigma,\tau)}(x)$ 是一个幺半群。特别地，若 G 是有限的，则 $C_{(\sigma,\tau)}(x)$ 是 G 的一个子群。一般而言， x 不一定是 $C_{(\sigma,\tau)}(x)$ 的元素。

引理 4.7. 设 G 是一个有限群，且 $x \in G$。则

$$|x^G_{(\sigma,\tau)}| = \left|\frac{G}{C_{(\sigma,\tau)}(x)}\right| = \frac{|G|}{|C_{(\sigma,\tau)}(x)|}.$$

特别地， $|x^G_{(\sigma,\tau)}|$ 整除 $|G|$。

定义 4.8. 集合

$$Z_{(\sigma,\tau)}(G) = \{z \in G \mid z\tau(g) = \sigma(g)z, \forall\, g \in G\}$$

称为 G 的 (σ, τ)-中心。

注意， $Z_{(\sigma,\tau)}(G) = \{z \in G \mid C_{(\sigma,\tau)}(z) = G\}$。若 $\tau = \sigma$，则将 G 的 (σ, τ)-中心简记为 $Z_\sigma(G)$，它是一个幺半群。若 $\tau = \sigma = id_G$ （ G 上的恒等映射），则 G 的 (σ, τ)-中心就是通常中心，记为 $Z(G)$。特别地，若 G 是有限的，则 $Z_\sigma(G)$ 是 G 的一个子群。根据引理 4.7， $|x^G_{(\sigma,\tau)}| = 1$ 当且仅当 $x \in Z_{(\sigma,\tau)}(G)$。注意，我们已经证明了以下定理。

定理 4.9。设 G 是一个有限群， x_1， ...， x_r 是 G 的 (σ, τ)-共轭类代表元。那么

$$|G| = |Z_{(\sigma,\tau)}(G)| + \sum_{x_i \notin Z_{(\sigma,\tau)}(G)} |(x_i)^G_{(\sigma,\tau)}|,$$

其中 $|(x_i)^G_{(\sigma,\tau)}| = \frac{|G|}{|C_{(\sigma,\tau)}(x_i)|}$ $(1 \le i \le r)$。

注意，(σ, τ)-共轭的概念类似于经典群论中通常的共轭概念。还可以作出更多这样的类比。

4.2 主要结果

定义 4.10. 集合

$$Z_{(\sigma,\tau)}(RG) = \{z \in RG \mid z\tau(\alpha) = \sigma(\alpha)z, \forall\, \alpha \in RG\}$$

称为 RG 的 (σ, τ)-中心。

容易验证， $Z_{(\sigma,\tau)}(RG)$是 R-模 RG的 R-子模。若$\tau = \sigma$，则将 RG 的(σ, τ)-中心记为 $Z_\sigma(RG)$，且 $Z_\sigma(RG)$是RG的子代数。若 $\tau = \sigma = id_{RG}$ （ RG上的恒等映射），则 RG 的 (σ, τ)-中心变为 RG的通常中心，记为 $Z(RG)$。现在，我们需要求$Z_{(\sigma,\tau)}(RG)$这个 R-模的秩和一组基。

定义4.11。令 $\{C_i\}_{i\in I}$为 G 中所有有限大小的(σ,τ)-共轭类构成的集合。对于每个指标 $i\in I$, 定义其和

$$\hat{C}_i = \sum_{g\in C_i} g.$$

ˆ这些和 C_i 是 RG 中的元素，称为 (σ,τ)-类和。

引理 4.12. 设 $\{C_i\}_{i\in I}$ 为 G 的所有有限大小的 (σ,τ)-共轭类的集合。那么，(σ,τ)-类和 $\{C_i\}_{i\in I}$ 构成 $Z_{(\sigma,\tau)}(RG)$ 的一个 R-基。特别地，若群 G 是有限群，且恰有 r 个不同的 (σ,τ)-共轭类，则 $Z_{(\sigma,\tau)}(RG)$ 的秩为 r。

证明。 证明与 22 中命题 12 [24] 或定理 3 的证明。6。2（见 [40]）类似。

□

定理 4.13. 设 R 为含幺交换环， G 为群，且 $\{C_i\}_{i\in I}$（I 为某个指标集）是 G 的所有有限大小的 (σ,τ)-共轭类及其对应代表元集 $\{x_i\}_{i\in I}$ 的集合。设 $J\subseteq I$，使得对所有 $j\in J$ 均有 $|C_j|=1$，且对所有 $i\in I\setminus J$ 均有$|C_i|\geq 2$。此外，设 $\{C_{i'}\}_{i'\in I'}$ 为 G 的所有无限大小的 (σ,τ)-共轭类的集合。那么集合

$$\mathcal{B}_0 = \left\{ D_g \;\middle|\; g\in \left(\bigcup_{i\in I\setminus J}(C_i\setminus\{x_i\})\right)\cup\left(\bigcup_{i'\in I'} C_{i'}\right)\right\}$$

构成 $\mathrm{Inn}^{(\sigma,\tau)}(RG)$ 的 R-基。

ˆ证明。 由引理 4.12，集合 $\mathcal{B}_1=\{C_i \mid i\in I\}$ 是 R-基，属于 $Z_{(\sigma,\tau)}(RG)$。我们将此定理的证明分为两步。

步骤 1：构造 $\mathrm{Inn}^{(\sigma,\tau)}(RG)$ 的 R-基。

假设基 $\mathcal{B}_1$ 可扩充为一个 R-基，记为

$$\mathcal{B}_2 = \{\hat{C}_i\}_{i\in I}\cup\{\gamma_{i''}\}_{i''\in I''}$$

RG 的基，其中指标集为 I''。（注意，为了继续证明，我们必须作此假设，因为对于任意交换含幺环 R，一般而言， R-模 M 的 R-子模 N 的基并不一定能扩充为 M 的基。然而，如果 R 是一个域，那么 N 的基总能扩充为 M 的基。）

令 $\mathcal{B}=\{D_{\gamma_{i''}} \mid i''\in I''\}$。我们证明 $\mathcal{B}$ 是 $\mathrm{Inn}^{(\sigma,\tau)}(RG)$ 的 R-基。

设 $\lambda\in R$ 和 δ、δ_1、$\delta_2\in RG$。则对所有 $\alpha\in RG$,

$$D_{\lambda\delta}(\alpha) = (\lambda\delta)\tau(\alpha)-\sigma(\alpha)(\lambda\delta) = \lambda(\delta\tau(\alpha)-\sigma(\alpha)\delta) = \lambda D_\delta(\alpha) = (\lambda D_\delta)(\alpha)$$

and

$$\begin{aligned}(D_{\delta_1}+D_{\delta_2})(\alpha) &= D_{\delta_1}(\alpha)+D_{\delta_2}(\alpha)\\ &= (\delta_1\tau(\alpha)-\sigma(\alpha)\delta_1)+(\delta_2\tau(\alpha)-\sigma(\alpha)\delta_2)\end{aligned}$$

$$= (\delta_1 + \delta_2)\tau(\alpha) - \sigma(\alpha)(\delta_1 + \delta_2)$$
$$= D_{\delta_1+\delta_2}(\alpha)$$

因此， $D_{\lambda\delta} = \lambda D_\delta$ 和 $D_{\delta_1+\delta_2} = D_{\delta_1} + D_{\delta_2}$。

现在，令 $D \in \mathrm{Inn}_{(\sigma,\tau)}(RG)$。那么，对于某个

$$\delta = \sum_{k=1}^{s} \lambda_{i_k} \hat{C}_{i_k} + \sum_{l=1}^{t} \mu_{i''_l} \gamma_{i''_l}$$

在 RG 中，对于某个 $\{i_k\}_{k=1}^{s} \subseteq I$ （对于某个 $s \in \mathbb{N}$）以及 $\{i''_l\}_{l=1}^{t} \subseteq I''$ （对于某个 $t \in \mathbb{N}$）。因此

$$D_\delta = \sum_{k=1}^{s} \lambda_{i_k} D_{\hat{C}_{i_k}} + \sum_{l=1}^{t} \mu_{i''_l} D_{\gamma_{i''_l}}.$$

注意，对所有 $k \in \{1, ..., s\}$， $D_{\hat{C}_{i_k}} = 0$。因此 $D_\delta = \sum_{l=1}^{t} \mu_{i''_l} D_{\gamma_{i''_l}}$。所以， $\mathcal{B}$ 在 R 上张成 $\mathrm{Inn}_{(\sigma,\tau)}(RG)$。

现在，令 $\lambda_{i'} \in R$ 对于某个 $\{i''_l\}_{l=1}^{t} \subseteq I''$ （对于某个 $t \in \mathbb{N}$），使得 $\sum_{l=1}^{t} \lambda_{i''_l} D_{\gamma_{i''_l}} = 0$。

$\Rightarrow D_{\sum_{l=1}^{t} \lambda_{i''_l}\gamma_{i''_l}}(\alpha) = 0, \forall\, \alpha \in RG. \Rightarrow \left(\sum_{l=1}^{t} \lambda_{i''_l}\gamma_{i''_l}\right)\tau(\alpha) - \sigma(\alpha)\left(\sum_{l=1}^{t} \lambda_{i''_l}\gamma_{i''_l}\right) = 0,$
$\forall\, \alpha \in RG. \Rightarrow \sum_{l=1}^{t} \lambda_{i''_l}\gamma_{i''_l} \in Z_{(\sigma,\tau)}(RG). \Rightarrow \sum_{l=1}^{t} \lambda_{i''_l}\gamma_{i''_l} = \sum_{k=1}^{s} \mu_{i_k} \hat{C}_{i_k}$ 对于某个 $\mu_{i_k} \in R$，对于某个 $\{i_k\}_{k=1}^{s} \subseteq I$ （对于某个 $s \in \mathbb{N}$）。$\Rightarrow \mu_{i_k} = 0, \forall\, k \in \{1, ..., s\}$ 以及 $\lambda_{i''_l} = 0, \forall\, l \in \{1, ..., t\}$。

因此， $\mathcal{B}$ 的每个有限子集在 R上都是线性无关的。因此，集合 $\mathcal{B}$是 R-线性无关的。因此， $\mathcal{B}$ 构成 $\mathrm{Inn}_{(\sigma,\tau)}(RG)$ 的一个 R-基。

步骤 2：构造 $\{\gamma_{i''}\}_{i'' \in I''}$。

Put

$$\mathcal{B}_3 = \left\{ g \;\middle|\; g \in \bigcup_{i \in I \setminus J} (C_i \setminus \{x_i\}) \right\} \bigcup \left\{ g \;\middle|\; g \in \bigcup_{i' \in I'} C_{i'} \right\}.$$

由于 G 是 RG 的一个 R-线性无关子集，且 $\mathcal{B}_3$ 是 G的子集，因此， $\mathcal{B}_3$也是 RG的一个 R-线性无关子集。

由于 $\mathcal{B}_1$ 和 $\mathcal{B}_3$ 的 R-张成空间交集平凡，且集合 $\mathcal{B}_1$、 $\mathcal{B}_3$ 都是 R-线性无关的，因此，集合 $\mathcal{B}'_2 = \mathcal{B}_1 \cup \mathcal{B}_3$ 是 RG的一个 R-线性无关子集。

现在，我们证明 $\mathcal{B}'_2$ 在 R上张成 RG 。

设 $g \in G$ 任意但固定。则有以下几种可能情形。

情形 1： $g \in Z_{(\sigma,\tau)}(G)$ 。

由定义 4.8之后的观察可知， $|g^G_{(\sigma,\tau)}| = 1$。因此， $g^G_{(\sigma,\tau)} = C_{j_0}$，也就是说，$\hat{C}_{j_0} = \{g\}$ 对于某个 $j_0 \in J$。于是 $C_{j_0} = g$。因此， $g \in \mathcal{B}_1 \subseteq \mathcal{B}'_2$。所以， g 属于R-张成的子空间 $\mathcal{B}'_2$。

情形 2： $g \in G \setminus Z_{(\sigma,\tau)}(G)$。

那么，根据定义4.8之后的观察 $|g^G_{(\sigma,\tau)}| \geq 2$。因此，

$$g \in \left(\bigcup_{i \in I \setminus J} C_i \right) \bigcup \left(\bigcup_{i' \in I'} C_{i'} \right).$$

于是我们得到以下情形。

子情形 2.1：$g \in \bigcup_{i' \in I'} C_{i'}$。

于是 $g \in \mathcal{B}_3 \subseteq \mathcal{B}'_2$。因此，$g$ 属于 $\mathcal{B}'_2$ 的 R-张成空间。

子情形 2.2：$g \in \bigcup_{i \in I \setminus J} C_i$。

于是，对某个 $i \in I \setminus J$，有 $g \in C_i$。

现在，由于 $C_i = (x_i)^G_{(\sigma,\tau)}$，所以 $C_i = (C_i \setminus \{x_i\}) \cup \{x_i\}$。因此，$g \in C_i$ 意味着 $g \in C_i \setminus \{x_i\}$ 或 $g \in \{x_i\}$。

若 $g \in C_i \setminus \{x_i\}$，则 $g \in \mathcal{B}_3 \subset \mathcal{B}'_2$。因此，$g$ 属于 $\mathcal{B}'_2$ 的 R-张成空间。

若 $g = x_i$，则注意到 $C_i = \sum_{h \in C_i} x_h$。因此 g 属于 $\mathcal{B}'_2$ 的 R-张成空间。

这样，我们终于穷尽了所有情形。在所有可能的情形下，我们都证明了 g属于 $\mathcal{B}'_2$ 的 R-张成空间。

由于 $g \in G$ 是任意的，因此 G 中的每个元素都属于 $\mathcal{B}'_2$ 的 R-张成空间。也就是说，G 包含于 $\mathcal{B}'_2$ 的 R-张成空间中。因此，G 的 R-张成空间包含于 $\mathcal{B}'_2$ 的 R-张成空间中。

由于 G 是 RG 的一个 R-基，因此它的 R-张成空间等于整个 RG。所以，我们证明了 RG 包含于 $\mathcal{B}'_2$ 的 R-张成空间中。

由于 $\mathcal{B}'_2$ 是 RG 的子集，因此其 R-张成空间自动包含于 RG .

因此，$\mathcal{B}'_2$ 的 R-张成空间等于 RG，也就是说，$\mathcal{B}'_2$ 在 R 上张成 RG。

因此，$\mathcal{B}'_2$ 成为 RG 的一个 R-线性无关子集，它在 R 上张成 RG。因此，$\mathcal{B}'_2$ 是 RG 的一个 R-基。

因此，$\mathcal{B}'_2 = \mathcal{B}_1 \cup \mathcal{B}_3$ 是 RG 的一个 R-基，它扩充了 $Z_{(\sigma,\tau)}(RG)$ 的 R-基 $\mathcal{B}_1$。所以，我们可以将集合 $\{\gamma_{i''}\}_{i'' \in I''}$（如步骤 1 中所述）取为 $\mathcal{B}_3$（即 $I'' = (I \setminus J) \cup I'$）。

因此，根据步骤 1，集合 $\mathcal{B}_0 = \{D_g \mid g \in \mathcal{B}_3\}$ 是 $\mathrm{Inn}_{(\sigma,\tau)}(\mathbb{F}G)$ 的一个 R-基。注意，$\mathcal{B}_0$ 与定理陈述中给出的集合相同。

因此得证。 □

回顾 σ,τ)-FC 群的定义，见 [1]（参见第 6 节）。若 G 是一个群，且 σ,τ是其群自同态，则称 G 为 (σ,τ)-FC 群，如果 σ,τ-共轭类均 G具有有限大小。

下面给出的推论是定理 4.13 的直接推论。

推论 4.14. 设 R 是一个含幺交换环，G 是一个 (σ,τ)-FC 群，且 $\{C_i\}_{i \in I}$（I 某个指标集）是 G 的所有 (σ,τ)-共轭类的集合，其相应的代表元集为 $\{x_i\}_{i \in I}$。设 $J \subseteq I$，使得对所有 $j \in J$，$|C_j| = 1$ 成立，且对所有 $i \in I \setminus J$，$|C_i| \geq 2$ 成立。那么集合

$$\mathcal{B}_0 = \left\{ D_g \;\middle|\; g \in \bigcup_{i \in I \setminus J} (C_i \setminus \{x_i\}) \right\}$$

构成 $\mathrm{Inn}_{(\sigma,\tau)}(RG)$ 的 R-基。

下面给出有限群的另一个推论，它是 (σ,τ)-FC 群的一个特例。

推论 4.15. 设 R 是含幺交换环， G 是阶为 n 的有限群，且 $C_1,...,C_r$ 分别是 G 的所有可能的不同 (σ,τ)-共轭类，代表元分别为 $x_1,...,x_r$。则 R-模 $\mathrm{Inn}_{(\sigma,\tau)}(RG)$ 的秩为 $n-r$。此外，若 s 是正整数，使得对所有 $i\in\{1,...,s\}$ 均有 $|C_i|=1$，且对所有 $i\in\{s+1,...,r\}$ 均有 $|C_i|\geq 2$，则集合

$$\mathcal{B}_0=\left\{D_g \;\middle|\; g\in\bigcup_{i=s+1}^{r}(C_i\setminus\{x_i\})\right\}$$

是 $\mathrm{Inn}_{(\sigma,\tau)}(RG)$ 的一个 R-基。

下面的推论特别针对 $R=\mathbb{F}$ 为域的情形。

推论 4.16. 设 $\mathbb{F}$ 是域， G 是阶为 n 的有限群，且 $C_1,...,C_r$ 分别是 G 的所有可能的不同 (σ,τ)-共轭类，代表元分别为 $x_1,...,x_r$。则 $\mathrm{Inn}_{(\sigma,\tau)}(\mathbb{F}G)$ 关于 $\mathbb{F}$ 的维数为 $n-r$。若 s 是正整数，使得对所有 $i\in\{1,...,s\}$ 均有$|C_i|=1$，且对所有 $i\in\{s+1,...,r\}$ 均有 $|C_i|\geq 2$，则集合

$$\mathcal{B}_0=\left\{D_g \mid g\in\bigcup_{i=s+1}^{r}(C_i\setminus\{x_i\})\right\}$$

是 $\mathrm{Inn}_{(\sigma,\tau)}(\mathbb{F}G)$ 的 $\mathbb{F}$-基。

证明。 证明可直接由定理 4.13 或推论 4.15得出，不过我们也可以在最后采用一种略有不同的方法来证明。

ˆ根据引理 4.12，$\dim(Z_{(\sigma,\tau)}(\mathbb{F}G))=r$，且 $\mathcal{B}_1=\{C_i\mid 1\leq i\leq r\}$是 $\mathbb{F}$-基ˆˆ $Z_{(\sigma,\tau)}(\mathbb{F}G)$。基 $\mathcal{B}_1$ 可以扩充为一个 $\mathbb{F}$-基，记作 $\mathcal{B}_2=\{C_1,...,C_r,\gamma_{r+1},...,\gamma_n\}$，属于$\mathbb{F}G$。

令 $\mathcal{B}=\{D_{\gamma_i}\mid r+1\leq i\leq n\}$。如定理 4.13的证明所示，可以证明 $\mathcal{B}$ 是 $\mathrm{Inn}_{(\sigma,\tau)}(\mathbb{F}G$上关于 $\mathbb{F}$ 的一个基。

由于 $|\mathcal{B}|=n-r$，因此 $\dim(\mathrm{Inn}_{(\sigma,\tau)}(\mathbb{F}G))=n-r$。注意，这一事实也可由以下事实推出：映射 $\theta:\mathbb{F}G\to\mathrm{Inn}_{(\sigma,\tau)}(\mathbb{F}G)$ $(\alpha\mapsto D_\alpha)$ 是一个 $\mathbb{F}$-线性映射，其零空间为 $Z_{(\sigma,\tau)}(\mathbb{F}G)$。

现在，我们证明 $\mathcal{B}_0$ 是 $\mathrm{Inn}_{(\sigma,\tau)}(\mathbb{F}G)$ 的 $\mathbb{F}$-基。

设 $|C_i|=n_i$、$\forall\, i\in\{s+1,...,r\}$。由于 $G=\bigcup_{i=1}^{r}C_i$ 和 (σ,τ)-共轭类两两不相交，因此

$$n=|G|=|\bigcup_{i=1}^{r}C_i|=\sum_{i=1}^{r}|C_i|=\sum_{i=1}^{s}|C_i|+\sum_{j=s+1}^{r}|C_j|=s+\sum_{j=s+1}^{r}n_j$$

因此 ^{r} $\sum_{j=s+1}^{r}n_j=n-s$。

Suppose that $\sum_{g\in\bigcup_{i=s+1}^{r}C_i\setminus\{x_i\}}\lambda_g D_g=0$ for $\lambda_g\in\mathbb{F}$ $(g\in\bigcup_{i=s+1}^{r}C_i\setminus\{x_i\})$.

$\Rightarrow D_{\sum_{g\in\bigcup_{i=s+1}^{r}C_i\setminus\{x_i\}}\lambda_g g}=0.$

$\Rightarrow\left(\sum_{g\in\bigcup_{i=s+1}^{r}C_i\setminus\{x_i\}}\lambda_g g\right)\tau(\alpha)=\sigma(\alpha)\left(\sum_{g\in\bigcup_{i=s+1}^{r}C_i\setminus\{x_i\}}\lambda_g g\right),\ \forall\,\alpha\in\mathbb{F}G.$

$\Rightarrow \sum_{g\in\bigcup_{i=s+1}^{r} C_i\setminus\{x_i\}} \lambda_g g \in Z_{(\sigma,\tau)}(\mathbb{F}G)$.

$\Rightarrow \sum_{g\in\bigcup_{i=s+1}^{r} C_i\setminus\{x_i\}} \lambda_g g = \sum_{i=1}^{r} \mu_i \hat{C}_i$ for some unique $\mu_i \in \mathbb{F}$ $(1 \le i \le r)$.

$\Rightarrow \sum_{i=1}^{s} \mu_i x_i + \sum_{i=s+1}^{r} \mu_i x_i + \sum_{i=s+1}^{r} \left(\sum_{g\in C_i\setminus\{x_i\}} (\mu_i - \lambda_g) g \right) = 0.$

由于 G 是 $\mathbb{F}G$ 的一个 $\mathbb{F}$-线性无关子集，且 (σ,τ)-共轭类 C_i 的 $(1 \le i \le r)$ 两两不相交，因此我们得到

$$\lambda_g = 0, \quad \forall\ g \in \bigcup_{i=s+1}^{r} (C_i \setminus \{x_i\}).$$

因此，集合 $\mathcal{B}_0$ 是 $\mathbb{F}$-线性无关的。

此外，由于集合 $C_{s+1} \setminus \{x_{s+1}\}$、...、$C_r \setminus \{x_r\}$ 两两不相交，因此，

$$|\mathcal{B}_0| = \sum_{i=s+1}^{r} |C_i \setminus \{x_i\}| = \sum_{i=s+1}^{r} (|C_i| - 1) = \left(\sum_{i=s+1}^{r} n_i \right) - (r-s) = (n-s) - (r-s) = n - r.$$

所以 $|\mathcal{B}_0| = \dim(\mathrm{Inn}^{(\sigma,\tau)}(\mathbb{F}G))$。因此，$\mathcal{B}_0$ 是 $\mathrm{Inn}^{(\sigma,\tau)}(\mathbb{F}G)$ 的一组基。

证毕。 □

注意，集合

$$\{D_\gamma \mid \gamma \in \{g - x_i \mid g \in \cup_{i=s+1}^{r} (C_i \setminus \{x_i\})\}\}$$

是 $\mathrm{Inn}^{(\sigma,\tau)}(\mathbb{F}G)$ 在 $\mathbb{F}$ 上的另一组基。

下面，我们证明一个重要结果。

定理 4.17. 设 R 是含幺环，G 是阶为 n 的有限群，且 n 在 R 中可逆。设 σ、τ 是 RG 上任意的幺 R-代数自同态。那么，RG 的每个 (σ,τ)-导子都是内导子。

证明. 设 $D \in \mathcal{D}_{(\sigma,\tau)}(RG)$。令

$$\gamma = \frac{1}{|G|} \sum_{g\in G} D(g^{-1})\tau(g) \qquad \left(\text{or} - \frac{1}{|G|} \sum_{g\in G} \sigma(g^{-1}) D(g) \right).$$

于是 $\gamma \in RG$。

由于 $D\colon RG \to RG$ 是一个 (σ,τ)-导子，因此对任意的 α、$\beta \in RG$，

$$D(\alpha\beta) = D(\alpha)\tau(\beta) + \sigma(\alpha)D(\beta)$$

从而

$$\sigma(\alpha)D(\beta) = D(\alpha\beta) - D(\alpha)\tau(\beta).$$

现在，对于任意的 $x \in G$，

$$\begin{aligned} D_\gamma(x) &= \gamma\tau(x) - \sigma(x)\gamma \\ &= \frac{1}{|G|} \sum_{g\in G} D(g^{-1})\tau(gx) - \frac{1}{|G|} \sum_{g\in G} (D(xg^{-1}) - D(x)\tau(g^{-1}))\tau(g) \end{aligned}$$

$$= \frac{1}{|G|}\sum_{y\in G} D(xy^{-1})\tau(y) - \frac{1}{|G|}\sum_{g\in G} D(xg^{-1})\tau(g) + \frac{1}{|G|}\sum_{g\in G} D(x)$$
$$= D(x).$$

因此 $D = D_\gamma$。所以， D 是内的。证毕。 □

推论 4.18。设 R 是含幺交换环， G 是阶在 R 中可逆的有限群。设 C_1，...， C_r 是 G 的所有可能的互不相同的 (σ,τ)-共轭类，其代表元分别为 x_1，...， x_r。那么， RG 的每个 (σ,τ)-导子都是内导子，即 $\mathcal{D}_{(\sigma,\tau)}(RG) = \mathrm{Inn}_{(\sigma,\tau)}(RG)$。此外，若 s 是一个正整数，使得对所有 $i \in \{1,...,s\}$ 都有 $|C_i| = 1$，且对所有 $i \in \{s+1,...,r\}$ 都有 $|C_i| \geq 2$，那么集合

$$\mathcal{B}_0 = \left\{ D_g \mid g \in \bigcup_{i=s+1}^{r} (C_i \setminus \{x_i\}) \right\}$$

是 $\mathcal{D}_{(\sigma,\tau)}(RG)$ 的一个 R-基。

证明。由推论 4.15 和定理 4.17得出。 □

最后，我们将本节的结果与文献中已有的结果进行比较。定理 4.13 是一个范围广得多的结果，它刻画了任意群 G 上、任意交换含幺环 R 上的群代数 RG 的所有内 (σ,τ)-导子，其中 σ,τ 是 RG 上的 R-代数自同态，并且是群自同态的 R-线性延拓。推论 4.16 还推广了 [38], 中的定理 2.17；该定理针对普通导子得到了证明。在 [1], 中，作者研究了离散可数群 G 的群代数 $\mathbb{C}G$ 上的 (σ,τ)-导子和 (σ,id)-导子，其中 σ,τ 是 $\mathbb{C}G$ 上的 $\mathbb{C}$-代数自同态，并且是群自同态的 $\mathbb{C}$-线性延拓。定理 4.17 推广了 [1, 推论 5], 该推论证明了有限群 G 的群代数 $\mathbb{C}G$ 上的每个 (σ,τ)-导子都是内导子。在 [1, 推论 7], 中，作者给出了一个判据，用以判断有限生成 (σ,τ)-FC 群 G 的群代数 $\mathbb{C}G$ 上的 (σ,τ)-导子是否为内导子。在 [1, 第 4], 节中，作者借助特征研究了 $\mathbb{C}G$ 上的拟内 (σ,τ)-导子；这些导子由作者在 [1, 定义 6] 中定义。在 [1, 命题 2] 和 [1, 定义 8], 中，作者定义了 (σ,τ)-中心 (σ,τ)-导子。在 [1, 命题 3], 中，作者证明了非零的 (σ,τ)-中心 (σ,τ)-导子不是拟内导子。在 [1, 定理 2], 中，作者给出了计算拟内 (σ,τ)-导子的方法。此外，在 [3] 中，作者运用拓扑和特征方法研究了有限群和 FC 群的普通内导子。在 [3, 定理 4.3], 中，作者给出了一个刻画条件：对于有限群 G 和有限交换含幺环 A，该条件成立时， AG 的所有普通导子都是内导子。在[3, 推论 4.2.4], 中，作者证明，对于无挠交换含幺环 A 和有限群 G， AG 的所有导子都是内导子。在 [6], 中，作者用群的伴随作用所对应的 2-群胚的特征空间，描述了有限呈示离散群的群代数的所有内导子和外导子构成的空间。定理 4.17 还推广了 [15, 定理 1.1]。还需指出的是， [2, 引理 3] 以及更早的 [29, 定理 2.1] 得到了一个类似于定理 4.17 的结果，该结果表明普通导子是局部内的。更多详情，请参阅引言部分（第 1 节）的第三段；我们在那里提到了文献中关于以下问题的研究：

确定群代数的导子或扭导子为内导子的条件，这一问题一直受到研究者的关注，这也说明了该问题始终备受关注。我们还请读者参阅小节 3.4 的末尾，以了解更多相关内容。

5 应用： σ-导子与二面体群代数

在本节中，我们将第 3 节和4 节中得到的结果应用于明确分类二面体群代数 σ 的所有内导子和外导子，其中 $\mathbb{F}D_{2n}$， $\mathbb{F}$ 是任意域，且

$$D_{2n} = \langle a, b \mid a^n = 1 = b^2, (ab)^2 = 1 \rangle$$

$(n \geq 3)$ 。在[32], 中，作者给出了从 D_{2m} 到 D_{2n} 的所有群同态，其中 m 和 n为任意正整数。当 n 为奇数时， D_{2n} 恰有 $n^2 + 1$ 个群自同态，其形式如下:

- $\sigma_{-1}(a) = 1$ 和 $\sigma_{-1}(b) = 1$。
- $\sigma_0(a) = a^s (1 \leq s \leq n-1)$ 和 $\sigma_0(b) = a^t b (0 \leq t \leq n-1)$。

当 n 为偶数时， D_{2n} 恰有 $(n+2)^2$ 个群自同态，其形式如下:

- $\sigma_1(a) = a^s \ (0 \leq s \leq n-1, s \neq 0, \frac{n}{2})$ and $\sigma_1(b) = a^t b \ (0 \leq t \leq n-1)$.
- $\sigma_2(a) = a^s \ (s = 0, \frac{n}{2})$ and $\sigma_2(b) = a^t \ (t = 0, \frac{n}{2})$.
- $\sigma_3(a) = a^s \ (s = 0, \frac{n}{2})$ and $\sigma_3(b) = a^t b \ (0 \leq t \leq n-1)$.
- $\sigma_4(a) = a^s b \ (0 \leq s \leq n-1)$, $\sigma_4(b) = a^t b \ (t = s, s + \frac{n}{2})$.
- $\sigma_5(a) = a^s b \ (0 \leq s \leq n-1)$, $\sigma_5(b) = a^t \ (t = 0, \frac{n}{2})$.

我们只推导 σ_0 在 n 为奇数时以及 σ_1 在 n 为偶数时的结果，因为其余情形的结果可作为练习题。

5.1 σ-导出 $\mathbb{F}D_{2n}$ 在 $\mathrm{char}(\mathbb{F}) = 0$ 或为奇素数时的结果 p

定义 5. 1. 设 R 是一个含幺环， G 是一个群。设 $\beta \in RG$。那么这个集合 t

$$\bar{C}(\beta) = \{\alpha \in RG \mid \alpha\beta = -\beta\alpha\}$$

称为 β 在 RG 中的反中心化子。

$C(\beta)$ 是 R-模 RG 的子模。若 $R = \mathbb{F}$ 是特征为 0 的域，或是奇有理素数 p，且 $g \in G \cap Z(\mathbb{F}G)$，则 $C(g) = \{0\}$。这是因为若 $\alpha \in C(g)$，则 $\alpha g = -g\alpha$，从而 $\alpha g = -\alpha g$ （因为 $g\alpha = \alpha g$）。这就得到 $2\alpha g = 0$，从而 $2\alpha = 0$。但是¯，由于 $\mathrm{char}(\mathbb{F}) \neq 2$，因此 $\alpha = 0$。因此， $C(g) = \{0\}$。

引理 5.2。设 $\mathbb{F}$ 是特征为 0 的域，或是奇有理素数 p，且 $\sigma = \sigma_0$ 或σ_1。

(i) 集合

$$\bar{\mathcal{B}}(\sigma(b)) = \{(a^i - a^{-i}),\ a^t(a^i - a^{-i})b \mid 1 \le i \le \lfloor \frac{n-1}{2} \rfloor\}$$

¯是 $\mathbb{F}$ 上 $C(\sigma(b))$ 的一组基。

(ii) 集合

$$\bar{\mathcal{B}}(\sigma(ab)) = \{(a^i - a^{-i}),\ a^{s+t}(a^i - a^{-i})b \mid 1 \le i \le \lfloor \frac{n-1}{2} \rfloor\}$$

¯是 $\mathbb{F}$ 上 $C(\sigma(ab))$ 的一组基。

证明。首先，设 n 为奇数。

¯(i) 容易验证， $\mathcal{B}(\sigma_0(b))$ 是 $C(\sigma_0(b))$ 的一个 $\mathbb{F}$- 线性无关子集。¯现在，设 $\alpha \in C(\sigma_0(b))$ 且

$$\alpha = \sum_{\substack{0 \le i \le n-1 \\ 0 \le j \le 1}} \lambda_{i,j} a^i b^j$$

对于某个 $\lambda_{i,\ j} \in \mathbb{F}$ $(0 \le i \le n-1, 0 \le j \le 1)$。

我们作出以下假设 (A*)，以简化计算：

(A*): For each $j \in \{0, 1\}$, $\lambda_{i,j} = \lambda_{i',j}$ whenever $i \equiv i' \pmod{n}$.

Now,

$$\alpha\sigma_0(b) = \sum_{0 \le i \le n-1} \lambda_{i,0} a^{i+t} b + \sum_{0 \le i \le n-1} \lambda_{i,1} a^{i-t}$$

and

$$\sigma_0(b)\alpha = \sum_{0 \le i \le n-1} \lambda_{i,0} a^{t-i} b + \sum_{0 \le i \le n-1} \lambda_{i,1} a^{t-i}.$$

因此，由 $\alpha\sigma_0(b) = -\sigma_0(b)\alpha$，可得

$$\sum_{0 \le i \le n-1} \lambda_{i,0} a^{i+t} b = -\sum_{0 \le i \le n-1} \lambda_{i,0} a^{t-i} b \quad \text{and} \quad \sum_{0 \le i \le n-1} \lambda_{i,1} a^{i-t} = -\sum_{0 \le i \le n-1} \lambda_{i,1} a^{t-i}.$$

由第一个等式并利用 (A*),

$$\sum_{0 \le i \le n-1} \lambda_{i,0} a^i = -\sum_{0 \le i \le n-1} \lambda_{(n-i),0} a^i.$$

因此，对于所有 $i \in \{0, 1, ..., n-1\}$，$\lambda_{i,0} = -\lambda_{(n-i),0}$。特别地，$\lambda_{0,0} = 0$。因此，

$$\begin{aligned} \sum_{0 \le i \le n-1} \lambda_{i,0} a^i &= \sum_{1 \le i \le n-1} \lambda_{i,0} a^i = \sum_{1 \le i \le \frac{n-1}{2}} \lambda_{i,0} a^i + \sum_{\frac{n-1}{2}+1 \le i \le n-1} \lambda_{i,0} a^i \\ &= \sum_{1 \le i \le \frac{n-1}{2}} \lambda_{i,0} a^i + \sum_{1 \le i \le \frac{n-1}{2}} \lambda_{(n-i),0} a^{-i} \end{aligned}$$

$$= \sum_{1\le i\le \frac{n-1}{2}} \lambda_{i,0}a^i - \sum_{1\le i\le \frac{n-1}{2}} \lambda_{i,0}a^{-i}$$
$$= \sum_{1\le i\le \frac{n-1}{2}} \lambda_{i,0}(a^i - a^{-i}).$$

由第二个等式可得

$$\sum_{0\le i\le n-1} \lambda_{i,1}a^{i-t} = -\sum_{0\le i\le n-1} \lambda_{i,1}a^{n-i+t}.$$

$\Rightarrow \sum_{-t\le j\le -t+n-1} \lambda_{(t+j),1}a^j = -\sum_{t+1\le j\le t+n} \lambda_{(n-j+t),1}a^j.$

$\Rightarrow \sum_{0\le i\le n-1} \lambda_{(t+i),1}a^i = -\sum_{0\le i\le n-1} \lambda_{(n-i+t),1}a^i$ 鉴于 (A*)。

因此，$\lambda_{(t+i),1} = -\lambda_{(n-i+t),1}$ 对所有 $i \in \{0, 1, ..., n-1\}$均成立。注意，$\lambda_{t,1} = 0$ （对于 $i = 0$）。因此，

$$\sum_{0\le i\le n-1} \lambda_{i,1}a^ib = \sum_{1\le i\le \frac{n-1}{2}} \lambda_{i,1}a^ib + \sum_{1\le i\le \frac{n-1}{2}} \lambda_{(n-i),1}a^{-i}b.$$

鉴于 (A*)，这个和

$$\sum_{1\le i\le \frac{n-1}{2}} \lambda_{i,1}a^ib + \sum_{1\le i\le \frac{n-1}{2}} \lambda_{(n-i),1}a^{-i}b$$

实际上等于

$$\sum_{1\le i\le \frac{n-1}{2}} \lambda_{(t+i),1}a^{t+i}b + \sum_{1\le i\le \frac{n-1}{2}} \lambda_{(n-i+t),1}a^{t-i}b.$$

因此，

$$\begin{aligned}\sum_{0\le i\le n-1} \lambda_{i,1}a^ib &= \sum_{1\le i\le \frac{n-1}{2}} \lambda_{(t+i),1}a^{t+i}b + \sum_{1\le i\le \frac{n-1}{2}} \lambda_{(n-i+t),1}a^{t-i}b \\ &= \sum_{1\le i\le \frac{n-1}{2}} \lambda_{(t+i),1}a^{t+i}b - \sum_{1\le i\le \frac{n-1}{2}} \lambda_{(t+i),1}a^{t-i}b \\ &= \sum_{1\le i\le \frac{n-1}{2}} \lambda_{(t+i),1}a^t(a^i - a^{-i})b.\end{aligned}$$

因此，

$$\begin{aligned}\alpha &= \sum_{0\le i\le n-1} \lambda_{i,0}a^i + \sum_{0\le i\le n-1} \lambda_{i,1}a^ib \\ &= \sum_{1\le i\le \frac{n-1}{2}} \lambda_{i,0}(a^i - a^{-i}) + \sum_{1\le i\le \frac{n-1}{2}} \lambda_{(t+i),1}a^t(a^i - a^{-i})b.\end{aligned}$$

因此，集合 $\mathcal{B}(\sigma_0(b))$ 在 $\mathbb{F}$ 上张成 $C(\sigma_0(b))$。因此，$\mathcal{B}(\sigma_0(b))$ 是 $C(\sigma_0(b))$ 的一个 $\mathbb{F}$-基.

(ii) 映射 $\theta: D_{2n} \to D_{2n}$ 定义为

$$\theta(a^ib^j) = a^i(a^sb)^j \qquad (0 \le i \le n-1,\ 0 \le j \le 1),$$

是 D_{2n}的自同构。将其线性扩张到整个 $\mathbb{F}D_{2n}$ 上，得到 θ ，它是群代数 $\mathbb{F}D_{2n}$的一个自同构。注意， $\theta(a) = a$ 且 $\theta(b) = a^s b$。

我们证明，当且仅当 $\alpha \in C(\sigma_0(b))$ 时， $\theta(\alpha) \in C(\sigma_0(ab))$。

首先，设 $\alpha \in C(\sigma_0(b))$。那么存在 $\alpha \in \mathbb{F}D_{2n}$ 使得

$$\alpha\sigma_0(b) = -\sigma_0(b)\alpha, \quad \text{that is,} \quad \alpha(a^t b) = -(a^t b)\alpha.$$

注意到， α 可写为 $\alpha = c_0 + c_1 b$，其中 $c_0, c_1 \in \mathbb{F}\langle a\rangle$。于是 $\theta(\alpha) = c_0 + c_1 a^s b$。由于 $\alpha(a^t b) = -(a^t b)\alpha$，因此 $c_0 a^t b + c_1 b a^t b = -a^t b c_0 - a^t b c_1 b$，使得

$$c_0 a^t b = -a^t b c_0 \qquad \text{and} \qquad c_1 b a^t = -a^t b c_1.$$

因此，

$$\begin{aligned}\theta(\alpha)\sigma_0(ab) &= (c_0 + c_1 a^s b)(a^{s+t} b)\\ &= a^s c_0 a^t b + c_1 b a^t b\\ &= -a^s a^t b c_0 - a^t b c_1 b\\ &= -a^{s+t} b(c_0 + c_1 a^s b)\\ &= -\sigma_0(ab)\theta(\alpha).\end{aligned}$$

因此， $\theta(\alpha) \in C(\sigma_0(ab))$。

反之，设 $\theta(\alpha) \in \bar{C}(\sigma_0(ab))$。于是 $\theta(\alpha)\sigma_0(ab) = -\sigma_0(ab)\theta(\alpha)$。由此得到

$$a^{s+t} c_0 b + c_1 b a^t b = -a^{s+t} b c_0 - a^t b c_1 b$$

使得

$$c_0 b = -b c_0 \qquad \text{and} \qquad c_1 b a^t = -a^t b c_1.$$

因此，

$$\begin{aligned}\alpha\sigma_0(b) &= (c_0 + c_1 b)a^t b\\ &= a^t c_0 b + c_1 b a^t b\\ &= -a^t b c_0 - a^t b c_1 b\\ &= -\sigma_0(b)(c_0 + c_1 b)\\ &= -\sigma_0(b)\alpha.\end{aligned}$$

因此， $\alpha \in C(\sigma_0(b))$。

因此，集合 $\theta(\mathcal{B}(\sigma_0(b))) = \mathcal{B}(\sigma_0(ab))$ 是 $\mathbb{F}$ 的一组基，属于 $C(\sigma_0(ab))$。

n偶数的证明与 n奇数的证明类似。 □

设 $\mathbb{F}$ 是一个域， σ 是一个 $\mathbb{F}$-代数端同态，作用于 $\mathbb{F}D_{2n}$ ，并且它是 $\mathbb{F}$-线性延拓，是群 D_{2n}的群自同态。集合 $X = \{a, b\}$ 是 D_{2n}的生成集，且 a^n、 b^2、$(ab)^2$ 是其关系子。设 $f\colon X \to \mathbb{F}D_{2n}$ 是一个映射，可将其延拓为 σ-导子，作用于 $\mathbb{F}D_{2n}$。根据定理 3.4，这成立当且仅当

$$\tilde{f}(a^n) = 0, \qquad \tilde{f}(b^2) = 0 \qquad \text{and} \qquad \tilde{f}((ab)^2) = 0,$$

˜其中 $f\colon F(X)\to \mathbb{F}D_{2n}$ 是 f 在（3.2）和（3.3）中定义且满足（3.1）的唯一延拓，而 $F(X)$ 是以 X为生成集的自由群。

现在，根据引理 3.3 和（3.1），

$$\tilde{f}(b^2)=\tilde{f}(b)\tilde{\sigma}(b)+\tilde{\sigma}(b)\tilde{f}(b)=f(b)\sigma(b)+\sigma(b)f(b)$$

在 G 上为 $\tilde{\sigma}=\sigma$。因此， $\tilde{f}(b^2)=0$ 当且仅当 $f(b)\sigma(b)=-\sigma(b)f(b)$，也就是说， $f(b)\in\bar{C}(\sigma(b))$。类似地， $\tilde{f}((ab)^2)=0$ 当且仅当 $\tilde{f}(ab)\in\bar{C}(\sigma(ab))$。由于 $f(a)\in\mathbb{F}D_{2n}$，所以 $f(a)$ 可写为 $f(a)=c_0+c_1b$，其中 $c_0,c_1\in\mathbb{F}\langle a\rangle$。现在，利用（3.3），

$$\begin{aligned}\tilde{f}(a^n)&=\sum_{i=1}^{n}(\prod_{j=1}^{i-1}\sigma(a))\tilde{f}(a)(\prod_{j=i+1}^{n}\sigma(a))\\&=\sum_{i=1}^{n}(\sigma(a))^{i-1}f(a)(\sigma(a))^{n-i}\\&=\sum_{j=0}^{n-1}(\sigma(a))^{j}c_0(\sigma(a))^{n-(j+1)}+\sum_{j=0}^{n-1}(\sigma(a))^{j}c_1b(\sigma(a))^{n-(j+1)}.\end{aligned}\tag{5.1}$$

˜ ˜ ¯此外，由于 $f(ab)=f(a)\tilde{\sigma}(b)+\tilde{\sigma}(a)f(b)=f(a)\sigma(b)+\sigma(a)f(b)$，所以

$$f(a)=\tilde{f}(ab)\sigma(b)-\sigma(a)f(b)\sigma(b)\tag{5.2}$$

注意到，群代数 $\mathbb{F}D_{2n}$ 的任意 σ-导子 D 都由其在生成元 a 和 b 上的像 $D(a)$ 和 $D(b)$ 唯一确定。我们将这样的导子记为

$$D_{(\sigma;\bar{a},\bar{b})},$$

¯其中 $\bar{a}=D(a)$ 且 $b=D(b)$。此外，我们知道 $\mathcal{D}_\sigma(\mathbb{F}D_{2n})$ 是 $\mathbb{F}$ 上的向量空间。我们将在以下定理中确定该向量空间的维数和基。

¯ ¯考虑 $\sigma=\sigma_0$ 或 σ_1。由于 $f(b)\in C(\sigma(b))$，并由引理 5.2， $\mathcal{B}(\sigma(b))$ 是$C(\sigma(b))$ 在 $\mathbb{F}$上的一组基，因此，

$$f(b)=\sum_{i=1}^{\lfloor\frac{n-1}{2}\rfloor}\mu_i(a^i-a^{-i})+\sum_{i=1}^{\lfloor\frac{n-1}{2}\rfloor}\nu_ia^t(a^i-a^{-i})b\tag{5.3}$$

对于某个 μ_i， $\nu_i\in\mathbb{F}(1\le i\le\lfloor\frac{n-1}{2}\rfloor)$。

˜ ¯ ¯ ¯此外，由于 $f(ab)\in C(\sigma(ab))$，并由引理5.2， $\mathcal{B}(\sigma(ab))$ 是 $C(\sigma(ab))$ 在$\mathbb{F}$上，因此，

$$\tilde{f}(ab)=\sum_{i=1}^{\lfloor\frac{n-1}{2}\rfloor}\delta_i(a^i-a^{-i})+\sum_{i=1}^{\lfloor\frac{n-1}{2}\rfloor}\gamma_ia^{s+t}(a^i-a^{-i})b\tag{5.4}$$

对于某些 δ_i、 $\gamma_i\in\mathbb{F}$ （$1\le i\le\lfloor\frac{n-1}{2}\rfloor$）。

定理 5.3. 设 n 为奇数，且 $\mathbb{F}$ 是特征为 0 的域或奇有理素数p。记 $|\sigma_0(a)|=m$、 $d=\frac{n}{m}$ 和 $t\equiv j_0$（模 s），其中 $j_0\in\{0,1,...,s-1\}$。

(i) 假设 $\mathbb{F}$ 的特征 $= 0$ 或 p，且最大公因数$(n, p) = 1$。那么 $\mathcal{D}_{\sigma_0}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为 $\frac{1}{2}(3n - d) - 1$，并且

$$\mathcal{S}_0 = \{D_{(\sigma_0;\bar{a},\bar{b})} \mid (\bar{a},\bar{b}) \in \{(a^t(a^i - a^{-i})b, 0), \quad (a^{s+t}(a^i - a^{-i})b, (a^i - a^{-i})),$$
$$(0, a^t(a^i - a^{-i})b) \mid 1 \le i \le \frac{n-1}{2}\}\}$$

是一个生成集。

(ii) 假设 $\mathbb{F}$ 的特征为 $= p$，且 n 与 p 的最大公因数为 $\neq 1$。

(a) 若 g cd$(d, p) = 1$，则 $\mathcal{D}_{\sigma_0}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为 $2n - \frac{1}{2}(d + 3)$，且

$$\mathcal{S}_0' = \{D_{(\sigma_0;\bar{a},\bar{b})} \mid (\bar{a},\bar{b}) \in \{(a^s(a^i - a^{-i}), 0), \quad (a^s(a^i - a^{-i}), a^t(a^i - a^{-i})b),$$
$$(a^t(a^i - a^{-i})b, 0), \quad (a^{s+t}(a^i - a^{-i})b, (a^i - a^{-i})) \mid 1 \le i \le \frac{n-1}{2}\}\}$$

是一个生成集。

(b) 若 d 与 p 的最大公因数为 $\neq 1$，则 $\mathcal{D}_{\sigma_0}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为 $4(\frac{n-1}{2})$，且集合 $\mathcal{S}_0'$ 是一个基。

证明。 根据（5.1），

$$\tilde{f}(a^n) = nc_0a^{s(n-1)} + \sum_{j=0}^{n-1} a^{2sj}c_1ba^{s(n-1)}.$$

˜因此，$f(a^n) = 0$ 当且仅当

$$nc_0 = 0 \qquad \text{and} \qquad \sum_{j=0}^{n-1} a^{sj}c_1 = 0$$

（因为 n 是奇数）。令 $c_1' = a^{-t}c_1$。则

$$\sum_{j=0}^{n-1} a^{sj}c_1 = 0 \qquad \text{if and only if} \qquad \sum_{j=0}^{n-1} a^{sj}c_1' = 0.$$

˜因此，$f(a^n) = 0$ 当且仅当

$$nc_0 = 0 \qquad \text{and} \qquad \sum_{j=0}^{n-1} a^{sj}c_1' = 0.$$

现在有两种可能的情形。

(i) char$(\mathbb{F}) = 0$ 或 p，且最大公因数$(n, p) = 1$。

于是有 $nc_0 = 0 \Leftrightarrow c_0 = 0$。

由于 $c_1' \in \mathbb{F}\langle a\rangle$，因此

$$c_1' = \sum_{i=1}^{n} \lambda_i a^i$$

对于某个 $\lambda_i \in \mathbb{F}\ (1 \le i \le n)$。

代入 $\lambda_0 = \lambda_n$。由于 $|\sigma_0(a)| = |a^s| = m$ 且 $d = \frac{n}{m}$，因此，

$$0 = \sum_{j=0}^{n-1} a^{sj} c_1' = \sum_{j=1}^{n} a^{sj} c_1' = (\sum_{j=1}^{dm} a^{sj}) c_1' = d(\sum_{j=1}^{m} a^{sj}) c_1'.$$

由于 d 整除 n，且 $\mathbb{F}$ 的特征 $= 0$ 或 p，并且 $\gcd(n, p) = 1$，因此，

$$d(\sum_{j=1}^{m} a^{sj}) c_1' = 0 \quad \text{if and only if} \quad (\sum_{j=1}^{m} a^{sj}) c_1' = 0.$$

现在，$|a^s| = m$ 且 $|a| = n$，所以 n 必须整除 sm，也就是说，对于某个 $l \in \{1, ..., m-1\}$，有 $sm = nl$。由此得到 $s = dl$。此外，$|a^d| = m$。因此，

$$\begin{aligned}
0 &= c_1'(\sum_{j=1}^{m} a^{sj}) = (\sum_{i=1}^{n} \lambda_i a^i)(\sum_{j=1}^{m} a^{sj}) = \sum_{i=1}^{n} \lambda_i (\sum_{j=1}^{m} a^{sj+i}) = \sum_{i=1}^{md} \lambda_i (\sum_{j=1}^{m} a^{dj+i}) \\
&= [\lambda_1(\sum_{j=1}^{m} a^{dj+1}) + \lambda_2(\sum_{j=1}^{m} a^{dj+2}) + ... + \lambda_d(\sum_{j=1}^{m} a^{dj+d})] + [\lambda_{d+1}(\sum_{j=1}^{m} a^{dj+d+1}) \\
&\quad + \lambda_{d+2}(\sum_{j=1}^{m} a^{dj+d+2}) + ... + \lambda_{d+d}(\sum_{j=1}^{m} a^{dj+d+d})] + ... + [\lambda_{(m-1)d+1}(\sum_{j=1}^{m} a^{dj+(m-1)d+1}) \\
&\quad + \lambda_{(m-1)d+2}(\sum_{j=1}^{m} a^{dj+(m-1)d+2}) + ... + \lambda_{(m-1)d+d}(\sum_{j=1}^{m} a^{dj+(m-1)d+d})] \\
&= [\lambda_1(\sum_{j=1}^{m} a^{dj+1}) + \lambda_2(\sum_{j=1}^{m} a^{dj+2}) + ... + \lambda_d(\sum_{j=1}^{m} a^{dj+d})] + [\lambda_{d+1}(\sum_{j=1}^{m} a^{dj+1}) + \lambda_{d+2}(\sum_{j=1}^{m} a^{dj+2}) \\
&\quad + ... + \lambda_{d+d}(\sum_{j=1}^{m} a^{dj+d})] + ... + [\lambda_{(m-1)d+1}(\sum_{j=1}^{m} a^{dj+1}) + \lambda_{(m-1)d+2}(\sum_{j=1}^{m} a^{dj+2}) \\
&\quad + ... + \lambda_{(m-1)d+d}(\sum_{j=1}^{m} a^{dj+d})] \\
&= (\sum_{i=0}^{m-1} \lambda_{di+1})(\sum_{j=1}^{m} a^{dj+1}) + (\sum_{i=0}^{m-1} \lambda_{di+2})(\sum_{j=1}^{m} a^{dj+2}) + ... + (\sum_{i=0}^{m-1} \lambda_{di+d})(\sum_{j=1}^{m} a^{dj+d}).
\end{aligned}$$

因此，

$$(\sum_{j=1}^{m} a^{sj}) c_1' = 0 \qquad \text{if and only if} \qquad \sum_{i=0}^{m-1} \lambda_{di+j} = 0$$

对于所有 $j \in \{1, 2, ..., d\}$。

现在，利用（5.2）、（5.3）和（5.4），

$$\begin{aligned} c_0 + c_1 b &= f(a) \\ &= \tilde{f}(ab)a^t b - a^s f(b)a^t b \\ &= \sum_{i=1}^{\frac{n-1}{2}} (\gamma_i - \nu_i)a^s(a^i - a^{-i}) + a^t(\sum_{i=1}^{\frac{n-1}{2}} \delta_i(a^i - a^{-i}) - \sum_{i=1}^{\frac{n-1}{2}} \mu_i a^s(a^i - a^{-i}))b. \end{aligned}$$

因此，

$$c_0 = \sum_{i=1}^{\frac{n-1}{2}} (\gamma_i - \nu_i)a^s(a^i - a^{-i}) \quad \text{and} \quad c_1 = a^t(\sum_{i=1}^{\frac{n-1}{2}} \delta_i(a^i - a^{-i}) - \sum_{i=1}^{\frac{n-1}{2}} \mu_i(a^{s+i} - a^{s-i})).$$

由于 $c_0 = 0$，因此，对于所有 $i \in \{1, ..., \frac{n-1}{2}\}$，$\gamma_i = \nu_i$。此外，

$$c_1' = a^{-t}c_1 = \sum_{i=1}^{\frac{n-1}{2}} \delta_i(a^i - a^{-i}) - \sum_{i=1}^{\frac{n-1}{2}} \mu_i(a^{s+i} - a^{s-i}).$$

注意，λ_i 属于集合 $\{\delta_i, \mu_i \mid 1 \le i \le \frac{n-1}{2}\}$。

断言：对于每个 $j \in \{1, 2, ..., d\}$，方程

$$\sum_{i=0}^{m-1} \lambda_{di+j} = 0 \qquad \text{and} \qquad \sum_{i=0}^{m-1} \lambda_{di+(d-j)} = 0$$

是冗余的。

断言的证明：首先，作出以下观察：

- 对于每个 $j \in \{1, 2, ..., d\}$，

  $$\sum_{i=0}^{m-1} \lambda_{di+j}$$

  是分别对应于 a^j、a^{d+j}、...、$a^{(m-1)d+j}$ 的系数 λ_j、λ_{d+j}、...、$\lambda_{(m-1)d+j}$ 之和。

- $\sum_{i=0}^{m-1} \lambda_{n-(di+j)}$ 是对应于系数 λ_{n-j}、$\lambda_{n-(d+j)}$ ...、$\lambda_{n-((m-1)d+j)}$ 的和

  $$a^{n-j} = a^{-j}, \quad a^{n-(d+j)} = a^{-(d+j)}, \quad ..., \quad a^{n-((m-1)d+j)} = a^{-((m-1)d+j)}$$

  分别。

- 由于 $n - (di + j) = (m - 1 - i)d + (d - j)$，因此，

  $$\sum_{i=0}^{m-1} \lambda_{n-(di+j)} = \sum_{i=0}^{m-1} \lambda_{di+(d-j)}.$$

- 由表达式可得

$$c_1' = \sum_{i=1}^{\frac{n-1}{2}} \delta_i (a^i - a^{-i}) - \sum_{i=1}^{\frac{n-1}{2}} \mu_i (a^{s+i} - a^{s-i}),$$

显然，如果 δ_i $1 \le i \le \frac{n-1}{2}$ a^{di_0+j} $i_0 \in$ ( ) 是（对于某个，）的 $\{0,1,...,m-1\}$ $j \in \{1,...,d\}$ $-\delta_i$ $a^{n-(di_0+j} = a^{-(di_0+j}$ 系数，那么它就是( )的系数。

- 标量 $-\mu_i$ ($1 \le i \le \frac{n-1}{2}$) 是 a^{s+i} 的系数。设

$$s + i \equiv i_1 \pmod{n},$$

其中 $i_1 \in \{0,1,...,n-1\}$。那么 $s+i = i_1 + nk$，其中 k 是某个非负整数。令 $i_1 = di_0 + j$，其中某个 $i_0 \in \{0,1,...,m-1\}$, $j \in \{1,...,d\}$。因此 $-\mu_i$ 是

$$a^{s+i} = a^{i_1} = a^{di_0+j}.$$

此外， μ_i 是

$$a^{s-i} = a^{s+(n-i)}$$

and

$$s + (n-i) = n - (di_0' + j),$$

其中 $i_0' = mk + i_0 - 2l$。现在，由于 m 是正整数，根据除法算法，存在某个 $i_0'' \in \{0,1,...,m-1\}$ 使得 $i_0' = mq + i_0''$。于是

$$a^{s-i} = a^{s+(n-i)} = a^{n-(di_0'+j)} = a^{n-(d(mq+i_0'')+j)} = a^{n-(di_0''+j)}.$$

根据上述观察，我们可以得出结论：如果和中出现一个标量（取自 δ_i、$-\delta_i$、μ_i、$-\mu_i$，其中 $1 \le i \le \frac{n-1}{2}$ ）

$$\sum_{i=0}^{m-1} \lambda_{di+j},$$

那么这个标量的相反数也会出现在和中

$$\sum_{i=0}^{m-1} \lambda_{n-(di+j)} = \sum_{i=0}^{m-1} \lambda_{di+(d-j)}$$

反之亦然。因此，方程

$$\sum_{i=0}^{m-1} \lambda_{di+j} = 0 \qquad \text{and} \qquad \sum_{i=0}^{m-1} \lambda_{di+(d-j)} = 0$$

是冗余的。因此，命题得证。

d 是奇数且 $d = 1 + \underbrace{2+2+...+2}_{r_0\text{-times}}$。因此，如果 $j \in \{1,...,d-1\}$，那么 $d-j \in \{1,...,d-1\}$，$j \ne d-j$，这些和

$$\sum_{i=0}^{m-1} \lambda_{di+j} \qquad \text{and} \qquad \sum_{i=0}^{m-1} \lambda_{di+(d-j)}$$

互不相同，且满足

$$\sum_{i=0}^{m-1} \lambda_{di+(d-j)} = -\sum_{i=0}^{m-1} \lambda_{di+j}$$

因此这些方程

$$\sum_{i=0}^{m-1} \lambda_{di+j} = 0 \qquad \text{and} \qquad \sum_{i=0}^{m-1} \lambda_{di+(d-j)} = 0$$

是冗余的。但对于 $j = d$，这些和

$$\sum_{i=0}^{m-1} \lambda_{di+j} \qquad \text{and} \qquad \sum_{i=0}^{m-1} \lambda_{di+(d-j)}$$

相同，因为

$$\sum_{i=0}^{m-1} \lambda_{di+j} = \sum_{i=1}^{m} \lambda_{di}, \qquad \sum_{i=0}^{m-1} \lambda_{di+(d-j)} = \sum_{i=0}^{m-1} \lambda_{di} \quad \text{and} \quad \sum_{i=1}^{m} \lambda_{di} = \sum_{i=0}^{m-1} \lambda_{di}$$

（因为 $\lambda_0 = \lambda_n$）。因此，对于 $j = d$，只有一个恒成立的方程，因为对于和 $\sum_{i=0}^{m-1} \lambda_{di}$ 中出现的每个系数 λ_{dj} （对应于 a^{dj}），其相反数（即 $-\lambda_{dj}$，对应于 a^{-dj}）也出现在和 $\sum_{i=0}^{m-1} \lambda_{di}$ 中。

因此总的来说，我们有 $r_0 = \frac{d-1}{2}$ 个不同的方程，每个方程都包含 m 个不同的系数（来自 δ_i、$-\delta_i$、μ_i、$-\mu_i$，对应 $1 \le i \le \frac{n-1}{2}$）。因此，在这 r_0 个不同的方程中，每个方程里的一个系数都可以表示为该方程中其他 $m-1$ 个不同系数的线性组合。此外，这 r_0 个不同的方程中，任意两个方程都没有共同的系数。

最后，$f(a) = c_1 b$ （作为 $c_0 = 0$），其中我们已在上面获得了出现在 c_1 表达式中的系数条件，其形式为 r_0 个不同的方程。这与 $f(b)$ 在（5.3）中的表达式共同给出如下集合。

$$\mathcal{S}_0 = \{D_{(\sigma_0;\bar{a},\bar{b})} \mid (\bar{a},\bar{b}) \in \{(a^t(a^i - a^{-i})b, 0),\ (a^{s+t}(a^i - a^{-i})b, (a^i - a^{-i})),\ (0, a^t(a^i - a^{-i})b) \mid 1 \le i \le \frac{n-1}{2}\}\},$$

¯其中 $\bar{a} = D(a) = f(a) = c_1 b$ 且 $b = D(b) = f(b)$。

如果 c_1、$c_2 \in \mathbb{F}$ 以及 α_1、α_2、β_1、$\beta_2 \in \mathbb{F}D_{2n}$，则

$$\begin{aligned}\left(c_1 D_{(\sigma_0;\alpha_1,\beta_1)} + c_2 D_{(\sigma_0;\alpha_2,\beta_2)}\right)(a) &= c_1 D_{(\sigma_0;\alpha_1,\beta_1)}(a) + c_2 D_{(\sigma_0;\alpha_2,\beta_2)}(a) \\ &= c_1\alpha_1 + c_2\alpha_2 \\ &= D_{(\sigma_0;c_1\alpha_1+c_2\alpha_2,c_1\beta_1+c_2\beta_2)}(a).\end{aligned}$$

类似地，

$$D_{(\sigma_0;c_1\alpha_1+c_2\alpha_2,c_1\beta_1+c_2\beta_2)}(b) = \left(c_1 D_{(\sigma_0;\alpha_1,\beta_1)} + c_2 D_{(\sigma_0;\alpha_2,\beta_2)}\right)(b).$$

由于任意 σ_0导子都完全由其在 $D(a)$和 $D(b)$上的像值确定，因此，由上文可得

$$c_1 D_{(\sigma_0;\alpha_1,\beta_1)} + c_2 D_{(\sigma_0;\alpha_2,\beta_2)} = D_{(\sigma_0;c_1\alpha_1+c_2\alpha_2,c_1\beta_1+c_2\beta_2)}.$$

因此， $\mathcal{S}_0$ 张成了 $\mathcal{D}_{\sigma_0}(\mathbb{F}D_{2n})$关于 $\mathbb{F}$的空间。此外，根据上述观察可知， $\mathcal{D}_{\sigma_0}(\mathbb{F}D_{2n})$关于 $\mathbb{F}$的维数为

$$|\mathcal{S}_0| - r_0 = 3(\frac{n-1}{2}) - (\frac{d-1}{2}) = \frac{1}{2}(3n-d) - 1.$$

(ii) $\mathbb{F}$ 的特征为 $= p$ ，且 n 与 p 的最大公因数为 $= p$。

于是等式 $nc_0 = 0$ 成立。根据 (i) 部分的计算， $f(a) = c_0 + c_1 b$，其中

$$c_0 = \sum_{i=1}^{\frac{n-1}{2}} (\gamma_i - \nu_i) a^s (a^i - a^{-i}) \quad \text{and} \quad c_1 = a^t (\sum_{i=1}^{\frac{n-1}{2}} \delta_i (a^i - a^{-i}) - \sum_{i=1}^{\frac{n-1}{2}} \mu_i (a^{s+i} - a^{s-i})).$$

在这种情形下，我们仍有两种子情形。

(a) d 与 p 的最大公因数为 $= 1$。此子情形的证明与 (i) 部分的证明类似。

令

$$\mathcal{S}_0' = \{D_{(\sigma_0;\bar{a},\bar{b})} \mid (\bar{a},\bar{b}) \in \{(a^s(a^i - a^{-i}), 0),\ (a^s(a^i - a^{-i}), a^t(a^i - a^{-i})b),\ (a^t(a^i - a^{-i})b, 0),$$
$$(a^{s+t}(a^i - a^{-i})b, (a^i - a^{-i})) \mid 1 \le i \le \frac{n-1}{2}\}\}.$$

于是，如 (i) 部分所示，可以证明 $\mathcal{S}_0'$ 是 $\mathbb{F}$ 上 $\mathcal{D}_{\sigma_0}(\mathbb{F}D_{2n})$ 的生成集，因此 $\mathbb{F}$ 上 $\mathcal{D}_{\sigma_0}(\mathbb{F}D_{2n})$ 的维数为

$$|\mathcal{S}_0'| - r_0 = 4(\frac{n-1}{2}) - (\frac{d-1}{2}) = 2n - \frac{1}{2}(d+3).$$

(b) d 与 p 的最大公因数为 $= p$。

由于

$$\sum_{j=0}^{n-1} a^{sj} c_1 = d(\sum_{j=1}^{m} a^{sj}) c_1,$$

$\mathbb{F}$的特征为 $= p$ ，且 p 整除 d，因此，在此子情形下，方程

$$\sum_{j=0}^{n-1} a^{sj} c_1 = 0$$

成立。因此，集合 $\mathcal{S}_0'$ 成为$\mathcal{D}_{\sigma_0}(\mathbb{F}D_{2n})$在 $\mathbb{F}$上的一组基。因此，$\mathcal{D}_{\sigma_0}(\mathbb{F}D_{2n})$在 $\mathbb{F}$上的维数为 $|\mathcal{S}_0'| = 4(\frac{n-1}{2})$。

□

在定理 5.3 中令 σ_0 为恒等端同态，可得当 n 为奇数时， $\mathbb{F}D_{2n}$ 的普通导子构成的 $\mathbb{F}$-向量空间 $\mathcal{D}(\mathbb{F}D_{2n})$ 的维数：若 $\mathrm{char}(\mathbb{F}) = 0$ 或 p 且 $\gcd(n,p) = 1$，则为 $3(\frac{n-1}{2})$；若 $\mathrm{char}(\mathbb{F}) = p$ 且 $\gcd(n,p) \neq 1$，则为 $2(n-1)$。此外，我们还可得到 $\mathcal{D}(\mathbb{F}D_{2n})$ 的一个 $\mathbb{F}$-基。

定理 5.4. 设 n 为偶数， $\mathbb{F}$ 为特征为 0 的域或奇有理素数p。记 $|\sigma_1(a)| = m$, $d = \frac{n}{m}$ 和 $t \equiv j_0$(模 s)，其中 $j_0 \in \{0, 1, ..., s-1\}$。

(i) 假设 m 为奇数。

(a) 假设 $\mathbb{F}$ 的特征为 $= 0$ 或 p，且 n 与 p 的最大公因数为 $= 1$。那么， $\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为 $\frac{1}{2}(3n - d) - 2$，并且

$$\mathcal{S}_1 = \{D_{(\sigma_1;\bar{a},\bar{b})} \mid (\bar{a},\bar{b}) \in \{(a^t(a^i - a^{-i})b, 0), \quad (a^{s+t}(a^i - a^{-i})b, (a^i - a^{-i})), \\ (0, a^t(a^i - a^{-i})b) \mid 1 \le i \le \frac{n}{2} - 1\}\}$$

是一个生成集。

(b) 假设 $\mathbb{F}$ 的特征为 $= p$，且 n 与 p 的最大公因数为 $\neq 1$。

(b1) 如果 $\gcd(d, p) = 1$，那么 $\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为 $2n - \frac{d}{2} - 3$，并且 d

$$\mathcal{S}_1' = \{D_{(\sigma_1;\bar{a},\bar{b})} \mid (\bar{a},\bar{b}) \in \{(a^s(a^i - a^{-i}), 0), \quad (a^s(a^i - a^{-i}), a^t(a^i - a^{-i})b), \\ (a^t(a^i - a^{-i})b, 0), \quad (a^{s+t}(a^i - a^{-i})b, (a^i - a^{-i})) \mid 1 \le i \le \frac{n}{2} - 1\}\}$$

是一个生成集。

(b2) 若 $\gcd(d, p) \neq 1$，则 $\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为 $2(n-2)$，且集合 $\mathcal{S}_1'$ 是一个基。

(ii) 假设 m 是偶数。

(a) 假设 $\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为 $\frac{3n}{2} - d - 2$，且 $\mathcal{S}_1$ 是一个生成集，其中 $\mathrm{char}(\mathbb{F}) = 0$ 或 p，且 $\gcd(n, p) = 1$。(b) 假设 $\mathrm{char}(\mathbb{F}) = p$，且 $\gcd(n, p) \neq 1$。(b1) 若 $\gcd(d, p) = 1$，则 $\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为 $2n - d - 3$，且 $\mathcal{S}_1'$ 是一个生成集。(b2) 若 $\gcd(d, p) \neq 1$，则 $\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为 $2(n-2)$，且集合 $\mathcal{S}_1'$ 是一个基。

证明。(i) 设 m 为奇数。

(a) $\mathbb{F}$ 的特征为 $= 0$ 或 p，且 n 与 p 的最大公因数为 $= 1$。

按照定理 5 的证明3 进行。由于 d 为偶数，因此 $d = \underbrace{2 + ... + 2}_{} = 2r_0$ 对某个r_0次正整数 r_0，利用定理 5.3 的证明，我们在此得到以下观察：

- 若 $j \in \{1, ..., d-1\} \setminus \{\frac{d}{2}\}$，则 $d - j \in \{1, ..., d-1\}$、 $d - j \neq \frac{d}{2}$ 和 $j \neq d - j$。对于这样的 j，我们将得到两个冗余方程

$$\sum_{i=0}^{m-1} \lambda_{di+j} = 0$$

（对应于 j）以及

$$\sum_{i=0}^{m-1} \lambda_{di+(d-j)} = 0$$

（对应于 $d-j$）。

- 对于 $j = \frac{d}{2}$，

$$\sum_{i=0}^{m-1} \lambda_{di+j} = \sum_{i=0}^{m-1} \lambda_{di+(d-j)} = \sum_{i=0}^{m-1} \lambda_{di+\frac{d}{2}}.$$

因此，对于 $j = \frac{d}{2}$，只有一个方程，即

$$\sum_{i=0}^{m-1} \lambda_{di+\frac{d}{2}} = 0.$$

这个方程总是成立，因为如果某个标量（在 $\delta_i, -\delta_i, \mu_i, -\mu_i$ 中，对于 $1 \le i \le \frac{n}{2}-1$）出现在求和中

$$\sum_{i=0}^{m-1} \lambda_{di+\frac{d}{2}},$$

那么这个标量的相反数也会出现在求和中

$$\sum_{i=0}^{m-1} \lambda_{n-(di+\frac{d}{2})} = \sum_{i=0}^{m-1} \lambda_{di+(d-\frac{d}{2})} = \sum_{i=0}^{m-1} \lambda_{di+\frac{d}{2}}$$

因此，这个和总是等于 0。

- 此外，正如定理 5.3的证明中所见，与$j = d$ 对应的方程只有一个，而且它也总是成立。

因此，在 d 个方程中，分别对应于 $j = \frac{d}{2}$ 和 $j = d$ 的两个方程总是成立。在 j（$j \in \{1, ..., d-1\} \setminus \{\frac{d}{2}\}$）的其余 $d-2$ 个值中，恰好有 $\frac{d-2}{2}$ 个不同的方程，因为对应于 j 和 $d-j$ 的方程是冗余的。因此，总共有 $\frac{d-2}{2} = \frac{d}{2} - 1 = r_0 - 1$ 个不同的方程，每个方程都含有 m 个不同系数（对于 $1 \le i \le \frac{n}{2}-1$，从 δ_i、$-\delta_i$、μ_i、$-\mu_i$ 中取值），使得其中一个系数可以线性地表示为该方程中其余 $m-1$ 个不同系数的线性组合。此外，这 $r_0 - 1$ 个不同方程中，任意两个方程都没有共同的系数。因此，集合 $\mathcal{S}_1$（定理陈述中给出的）成为 $\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的生成集。此外，根据上述观察，$\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为

$$|\mathcal{S}_1| - (r_0 - 1) = 3(\frac{n}{2} - 1) - (\frac{d}{2} - 1) = \frac{1}{2}(3n - d) - 2.$$

(b) 特征$(\mathbb{F}) = p$ 与最大公因数$(n, p) = p$。

于是等式 $nc_0 = 0$ 成立。因此 $f(a) = c_0 + c_1 b$，其中

$$c_0 = \sum_{i=1}^{\frac{n}{2}-1} (\gamma_i - \nu_i) a^s (a^i - a^{-i}) \quad \text{and} \quad c_1 = a^t (\sum_{i=1}^{\frac{n}{2}-1} \delta_i (a^i - a^{-i}) - \sum_{i=1}^{\frac{n}{2}-1} \mu_i (a^{s+i} - a^{s-i})).$$

同样，我们有两种子情形。

(b1) 最大公因数$(d, p) = 1$。

此子情形的证明与第 (i) 部分 (a) 的证明类似。显然，集合 $\mathcal{S}_1'$ （定理陈述中给出）是 $\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的生成集，而$\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为

$$|\mathcal{S}_1'| - (r_0 - 1) = 4(\frac{n}{2} - 1) - (\frac{d}{2} - 1) = 2n - \frac{d}{2} - 3.$$

(b2) 最大公因数$(d, p) = p$。

如定理 5.3 (ii) (b) 的证明所示，在此子情形中，方程

$$\sum_{j=0}^{n-1} a^{sj} c_1 = 0$$

成立。于是，集合 $\mathcal{S}_1'$ 成为 $\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的一组基，因此$\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为 $|\mathcal{S}_1'| = 2(n-2)$。

(ii) 我们略去这一部分的证明，因为其证明与第 (i) 部分类似。所有步骤都类似。需要注意的是， s、 d、 l 和 m 分别被 $2s$、 $2d$、$\frac{l}{2}$ 和 $\frac{m}{2}$ 取代。

□

若取 σ_1 为恒等端同态，则由定理 5.4 (ii) 可知，当 n 为偶数时， $\mathbb{F}$-向量空间 $\mathcal{D}(\mathbb{F}D_{2n})$（即 $\mathbb{F}D_{2n}$ 的普通导子空间）的维数为 $3(\frac{n}{2} - 1)$，若 $\text{char}(\mathbb{F}) = p$ 且 $\gcd(n, p) = 1$；若 $\text{char}(\mathbb{F}) = p$ 且 $\gcd(n, p) = p$，则维数为 $2(n-2)$。此外，我们还得到 $\mathcal{D}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的一组基。

5.2 σ-导子 $\mathbb{F}D_{2n}$ （当 $\text{char}(\mathbb{F}) = 2$ 时）

在本小节中，我们对域 $\mathbb{F}$（其特征为 2）上的 $\mathbb{F}D_{2n}$ 的所有 σ-导子进行分类（当 n 为奇数时针对 $\sigma = \sigma_0$，当 n 为偶数时针对 $\sigma = \sigma_1$）。

首先，让我们回顾以下定义。

定义 5.5。设 G 为一个群， R 为一个含幺交换环。设 $\beta \in RG$。则集合

$$C(\beta) = \{\alpha \in RG \mid \alpha\beta = \beta\alpha\}$$

称为 β 在 RG中的中心化子。

N注意， $C(\beta)$ 是 RG 的子代数，且如果 $\beta \in Z(RG)$，那么 $C(\beta) = RG$.

引理 5.6. 设 $\mathbb{F}$ 是特征为 2 的域。

(i) 设 n 为奇数。

(a) 该集合

$$\mathcal{B}(\sigma_0(b)) = \{1,\ a^t b\} \cup \{(a^i + a^{-i}),\ a^t(a^i + a^{-i})b \mid 1 \le i \le \frac{n-1}{2}\}$$

是 $C(\sigma_0(b))$在 $\mathbb{F}$ 上的一组基。

(b) 该集合

$$\mathcal{B}(\sigma_0(ab)) = \{1,\ a^{s+t} b\} \cup \{(a^i + a^{-i}),\ a^{s+t}(a^i + a^{-i})b \mid 1 \le i \le \frac{n-1}{2}\}$$

是 $C(\sigma_0(ab))$在 $\mathbb{F}$ 上的一组基。

(ii) 设 n 为偶数。

(a) 集合

$$\mathcal{B}(\sigma_1(b)) = \{1,\ a^{\frac{n}{2}},\ a^t b,\ a^{t+\frac{n}{2}} b\} \cup \{(a^i + a^{-i}),\ a^t(a^i + a^{-i})b \mid 1 \le i \le \frac{n}{2} - 1\}$$

is a basis of $C(\sigma_1(b))$ *over* $\mathbb{F}$.

(b) 集合

$$\mathcal{B}(\sigma_1(ab)) = \{1,\ a^{\frac{n}{2}},\ a^{s+t} b, a^{s+t+\frac{n}{2}} b\} \cup \{(a^i + a^{-i}),\ a^{s+t}(a^i + a^{-i})b \mid 1 \le i \le \frac{n}{2} - 1\}$$

is a basis of $C(\sigma_1(ab))$ *over* $\mathbb{F}$.

证明。 与引理的证明类似 5.2。 □

回顾定理之前的讨论 5。3。这里，由于特征$(\mathbb{F}) = 2$，因此

$$\tilde{f}(b^2) = f(b)\sigma(b) + \sigma(b)f(b) = 0$$

当且仅当

$$f(b)\sigma(b) = \sigma(b)f(b), \quad \text{that is,} \quad f(b) \in C(\sigma(b)).$$

类似地，$\tilde{f}((ab)^2) = 0$当且仅当 $\tilde{f}(ab) \in C(\sigma(ab))$。此外，(5.2) 化为

$$f(a) = \tilde{f}(ab)\sigma(b) + \sigma(a)f(b)\sigma(b). \tag{5.5}$$

定理 5.7。设 n 为奇数，$\mathbb{F}$ 为特征为 2 的域。记 $|\sigma_0(a)| = m$、$d = \frac{n}{m}$ 和 $t \equiv j_0$（模 s），其中 $j_0 \in \{0, 1, ..., s-1\}$。则 $\mathcal{D}_{\sigma_0}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为 $\frac{1}{2}(3n - d) + 1$，且集合

$$\mathcal{S}_0 = \{D_{(\sigma_0;\bar{a},\bar{b})} \mid (\bar{a}, \bar{b}) \in \{(a^t(1 + a^s)b, 1),\ \ (0, a^t b)\} \ \cup\ \{(a^t(a^i + a^{-i})b, 0),$$
$$(a^{s+t}(a^i + a^{-i})b, (a^i - a^{-i})),\ \ (0, a^t(a^i + a^{-i})b) \mid 1 \le i \le \frac{n-1}{2}\}\}$$

是一个生成集。

证明。 由于 $f(b) \in C(\sigma_0(b))$，并根据引理 5。6 (i) (a)， $\mathcal{B}(\sigma_0(b))$ 是一个 $\mathbb{F}$-基 $C(\sigma_0(b))$，因此，

$$f(b) = \mu_0 + \nu_0 a^t b + \sum_{i=1}^{\frac{n-1}{2}} \mu_i (a^i + a^{-i}) + \sum_{i=1}^{\frac{n-1}{2}} \nu_i a^t (a^i + a^{-i}) b$$

对于某些 $\mu_i, \nu_i \in \mathbb{F}$ $(1 \leq i \leq \frac{n-1}{2})$。

˜此外，由于 $f(ab) \in C(\sigma_0(ab))$，且根据引理 5.6 (i) (b)， $\mathcal{B}(\sigma_0(ab))$ 是 $\mathbb{F}$-基$C(\sigma(ab))$，因此，

$$\tilde{f}(ab) = \delta_0 + \gamma_0 a^{s+t} b + \sum_{i=1}^{\frac{n-1}{2}} \delta_i (a^i + a^{-i}) + \sum_{i=1}^{\frac{n-1}{2}} \gamma_i a^{s+t} (a^i + a^{-i}) b$$

对于某些 $\delta_i, \gamma_i \in \mathbb{F}$ $(1 \leq i \leq \frac{n-1}{2})$。

˜如定理 5.3的证明所示， $f(a^n) = 0$ 当且仅当

$$nc_0 = 0 \qquad \text{and} \qquad \sum_{j=0}^{n-1} a^{sj} c_1' = 0,$$

其中 $c_1' = a^{-t} c_1$。

此外，如果

$$c_1' = \sum_{i=1}^{n} \lambda_i a^i$$

对于某个 $\lambda_i \in \mathbb{F}$ $(1 \leq i \leq n)$ $(\lambda_0 = \lambda_n)$，则

$$\sum_{j=0}^{n-1} a^{sj} c_1' = 0$$

当且仅当

$$\sum_{i=0}^{m-1} \lambda_{di+j} = 0 \quad \text{for all} \quad 1 \leq j \leq d.$$

由（5.5），

$$c_0 + c_1 b = f(a) = \tilde{f}(ab) a^t b + a^s f(b) a^t b.$$

因此，

$$c_0 = (\gamma_0 + \nu_0) a^s + \sum_{i=1}^{\frac{n-1}{2}} (\gamma_i + \nu_i) a^s (a^i + a^{-i})$$

and

$$c_1 = a^t (\delta_0 + \mu_0 a^s + \sum_{i=1}^{\frac{n-1}{2}} \delta_i (a^i + a^{-i}) + \sum_{i=1}^{\frac{n-1}{2}} \mu_i (a^{s+i} + a^{s-i})).$$

但由于 $c_0 = 0$，所以我们必须有 $\gamma_i = \nu_i$ 对所有 $0 \le i \le \frac{n-1}{2}$ 都成立。此外，

$$c_1' = a^{-t}c_1 = \delta_0 + \mu_0 a^s + \sum_{i=1}^{\frac{n-1}{2}} \delta_i (a^i + a^{-i}) + \sum_{i=1}^{\frac{n-1}{2}} \mu_i (a^{s+i} + a^{s-i}).$$

现在，完全按照定理 5.3 的证明（情形（i）：$\mathrm{char}(\mathbb{F}) = 0$ 或 p 满足最大公因数$(n, p) = 1$），并利用 $\mathrm{char}(\mathbb{F}) = 2$这一事实，可得：若某个标量（取自 δ_i, μ_i，其中$0 \le i \le \frac{n-1}{2}$）出现在和式中

$$\sum_{i=0}^{m-1} \lambda_{di+j},$$

那么该标量也会出现在和式中

$$\sum_{i=0}^{m-1} \lambda_{n-(di+j)} = \sum_{i=0}^{m-1} \lambda_{di+(d-j)}$$

反之亦然。因此，

$$\sum_{i=0}^{m-1} \lambda_{di+j} = \sum_{i=0}^{m-1} \lambda_{di+(d-j)}$$

从而，方程

$$\sum_{i=0}^{m-1} \lambda_{di+j} = 0$$

（对应于 j）和

$$\sum_{i=0}^{m-1} \lambda_{di+(d-j)} = 0$$

（对应于 $d - j$）完全相同。因此，对于 $j \in \{1, ..., d-1\}$，恰有 $\frac{d-1}{2}$ 个不同的方程。此外，对于 $j = d$，只有一个方程，其形式为

$\frac{n-1}{2}\delta_0 + \mu_0 + \sum$（与 a^{di} 相对应的系数，出现在求和式 $\sum \delta_i(a^i + a^{-i})$ 和$_{i=1}$

$$\sum_{i=1}^{\frac{n-1}{2}} \mu_i (a^{s+i} + a^{s-i})) = 0.$$

注意，　　求和中出现的幂 a^{di} 所对应的系数之和　　s

$$\sum_{i=1}^{\frac{n-1}{2}} \delta_i (a^i + a^{-i}) \qquad \text{and} \qquad \sum_{i=1}^{\frac{n-1}{2}} \mu_i (a^{s+i} + a^{s-i})$$

为 0，因为求和中出现的每个系数 λ_{dj} （对应于 a^{dj}）

$$\sum_{i=0}^{m-1} \lambda_{di},$$

系数 λ_{dj} （对应于 a^{-dj}）也出现在求和中

$$\sum_{i=0}^{m-1} \lambda_{n-(di+d)} = \sum_{i=0}^{m-1} \lambda_{di+(d-d)} = \sum_{i=0}^{m-1} \lambda_{di}.$$

因此， $\delta_0 + \mu_0 = 0$ 使得 $\delta_0 = \mu_0$。因此，对于 $j = d$，我们只有一个方程，即 $\delta_0 + \mu_0 = 0$。

因此，总体而言，我们有 $r_0 = \frac{d-1}{2}$ 个不同的方程，每个方程都包含 m个不同的系数（从 δ_i、 μ_i 中取出，用于 $1 \leq i \leq \frac{n-1}{2}$ ），此外还有方程 $\delta_0 = \mu_0$。而且，这 r_0 个不同的方程中，任意两个方程都没有共同的系数。此外，在这 r_0 个不同的方程中，每个方程的一个系数都可以表示为该方程中其他 $m-1$ 个不同系数的线性组合。又因为 $\delta_0 = \mu_0$, 所以 c_1 的表达式变为

$$c_1 = a^t(\mu_0(1+a^s) + \sum_{i=1}^{\frac{n-1}{2}} \delta_i(a^i + a^{-i}) + \sum_{i=1}^{\frac{n-1}{2}} \mu_i(a^{s+i} + a^{s-i})).$$

因此，集合 $\mathcal{S}_0$ （定理陈述中给出的）成为 $\mathcal{D}_{\sigma_0}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的生成集。此外，根据上述观察可知， $\mathcal{D}_{\sigma_0}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为

$$|\mathcal{S}_0| - r_0 = 3(\frac{n-1}{2}) + 2 - (\frac{d-1}{2}) = \frac{1}{2}(3n-d) + 1.$$

□

由定理 5.7，可知当 n 为奇数且特征$(\mathbb{F}) = 2$ 时， $\mathbb{F}$-向量空间 $\mathcal{D}(\mathbb{F}D_{2n})$ 中 $\mathbb{F}D_{2n}$ 的普通导子维数为 $\frac{3n+1}{2}$ ，其中取 σ_0 为恒等端同态。

定理 5.8. 设 n 为偶数， $\mathbb{F}$ 是特征为 2 的域。记 $|\sigma_1(a)| = m$, $d = \frac{n}{m}$ 以及 $t \equiv j_0$(模 s)，其中 $j_0 \in \{0, 1, ..., s-1\}$。则$\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$在 $\mathbb{F}$上的维数为 $2(n+2)$，一组基为

$$\begin{aligned}\mathcal{B}_1 = \{D_{(\sigma_1;\bar{a},\bar{b})} \mid (\bar{a},\bar{b}) \in \{&(a^{s+t}b, 1), \quad (a^{s+t+\frac{n}{2}}b, a^{\frac{n}{2}}), \quad (a^s, a^t b), \quad (a^{s+\frac{n}{2}}, a^{t+\frac{n}{2}}b),\\ &(a^t b, 0), \quad (a^{t+\frac{n}{2}}b, 0), \quad (1, 0), \quad (a^{s+\frac{n}{2}}, 0)\} \cup \{(a^{s+t}(a^i + a^{-i})b, (a^i + a^{-i})),\\ &(a^s(a^i + a^{-i}), a^t(a^i + a^{-i})b), \quad (a^t(a^i + a^{-i})b, 0), \quad (a^s(a^i + a^{-i}), 0) \mid 1 \leq i \leq \frac{n}{2} - 1\}\}.\end{aligned}$$

证明。 由于 $f(b) \in C(\sigma_1(b))$，并由引理 5。6 (ii) (a)， $\mathcal{B}(\sigma_1(b))$ 是 $\mathbb{F}$-基 $C(\sigma_1(b))$，因此，

$$f(b) = \mu_{-1} + \mu_0 a^{\frac{n}{2}} + \nu_{-1} a^t b + \nu_0 a^{t+\frac{n}{2}} b + \sum_{i=1}^{\frac{n}{2}-1} \mu_i(a^i + a^{-i}) + \sum_{i=1}^{\frac{n}{2}-1} \nu_i a^t(a^i + a^{-i})b$$

对于某些 $\mu_i, \nu_i \in \mathbb{F}$ $(1 \leq i \leq \frac{n}{2} - 1)$。

˜此外，由于 $f(ab) \in C(\sigma_1(ab))$，并由引理 5.6 (ii) (b)， $\mathcal{B}(\sigma_1(ab))$ 是 $\mathbb{F}$-基$C(\sigma_1(ab))$，因此，

$$\tilde{f}(ab) = \delta_{-1} + \delta_0 a^{\frac{n}{2}} + \gamma_{-1} a^t b + \gamma_0 a^{s+t+\frac{n}{2}} b + \sum_{i=1}^{\frac{n}{2}-1} \delta_i (a^i + a^{-i}) + \sum_{i=1}^{\frac{n}{2}-1} \gamma_i a^{s+t} (a^i + a^{-i}) b$$

对某些 $\delta_i, \gamma_i \in \mathbb{F}$ $(1 \leq i \leq \frac{n}{2} - 1)$。

现在，根据 (5.1)， $\tilde{f}(a^n) = 0$ 当且仅当

$$nc_0 = 0 \qquad \text{and} \qquad \sum_{j=0}^{n-1} a^{2sj} c_1 = 0.$$

由于 n 是偶数， $nc_0 = 0$ 成立，且

$$\sum_{j=0}^{n-1} a^{2sj} = (\sum_{j=0}^{n-1} a^{sj})^2 = n(\sum_{j=0}^{n-1} a^{sj})$$

从而

$$\sum_{j=0}^{n-1} a^{2sj} c_1 = 0$$

˜ ˜成立。因此， $f(a^n) = 0$成立。由 (5.5)， $f(a) = f(ab)\, a^t b + a^s f(b)$ $a^t b$从而

$$\begin{aligned} f(a) = {} & \delta_{-1} a^t b + \delta_0 a^{t+\frac{n}{2}} b + \gamma_{-1} + \gamma_0 a^{s+\frac{n}{2}} + \sum_{i=1}^{\frac{n}{2}-1} \delta_i a^t (a^i + a^{-i}) b + \sum_{i=1}^{\frac{n}{2}-1} \gamma_i a^s (a^i + a^{-i}) \\ & + \mu_{-1} a^{s+t} b + \mu_0 a^{s+t+\frac{n}{2}} b + \nu_{-1} a^s + \nu_0 a^{s+\frac{n}{2}} + \sum_{i=1}^{\frac{n}{2}-1} \mu_i a^{s+t} (a^i + a^{-i}) b \\ & + \sum_{i=1}^{\frac{n}{2}-1} \nu_i a^s (a^i + a^{-i}). \end{aligned}$$

因此，集合 $\mathcal{B}_1$ （定理陈述中给出）是 $\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的一组基。因此， $\mathcal{D}_{\sigma_1}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为 $|\mathcal{B}_1| = 2(n+2)$。 □

若取 σ_1 为定理5.8中的恒等端同态，则当 n 为偶数且 $\mathrm{char}(\mathbb{F}) = 2$时， $\mathbb{F}$-向量空间上 的普通导子空间的维数为 $2(n+2)$。

5.3 σ- D_{2n}的共轭类

在本小节中，我们计算 σ-共轭类 D_{2n}，这将在下一小节中用于确定 D_{2n}的所有内 σ-导子。

定理 5.9. 设 n 为奇数。记 $|\sigma_0(a)| = m$, $d = \frac{n}{m}$和 $t \equiv j_0$(模 s)为某个$j_0 \in \{0, 1, ..., s-1\}$。那么 D_{2n} 恰有$\frac{1}{2}(n+d)$个 $+1$ σ_0-共轭类，由下式给出

$$\{1\},\ \ \{a^k,\ a^{-k}\}\ for\ 1 \le k \le \frac{n-1}{2},\ \ (a^{j_0}b)^{D_{2n}}_{\sigma_0} = \{a^{2si}a^{j_0}b \mid 0 \le i \le m-1\},$$

$$(a^u b)^{D_{2n}}_{\sigma_0} = \{a^{2si}a^u b,\ a^{2si}a^{2j_0-u}b \mid 0 \le i \le m-1\}\ for\ j_0+1 \le u \le j_0 + (\frac{d-1}{2}).$$

证明。显然 $1^{D_{2n}}_{\sigma_0} = \{1\}$。令 $k \in \{1, ..., \frac{n-1}{2}\}$。若 $g = a^i$，则 $\sigma_0(g)a^k(\sigma_0(g))^{-1} = a^k$；若 $g = a^i b$，则 $\sigma_0(g)a^k(\sigma_0(g))^{-1} = a^{-k}$。因此，

$$(a^k)^{D_{2n}}_{\sigma_0} = \{\sigma_0(g)a^k(\sigma_0(g))^{-1} \mid g \in D_{2n}\} = \{a^k, a^{-k}\}.$$

进一步，令 $u \in \{j_0, j_0+1, ..., j_0+r_0\}$，其中 r_0是一个正整数，满足 $d = 1 + \underbrace{2 + ... + 2}_{r_0次}$（因为 d是奇数）。那么

$$\begin{aligned}(a^u b)^{D_{2n}}_{\sigma_0} &= \{a^{2si}a^u b,\ a^{2si}a^{2t-u}b \mid 0 \le i \le m-1\} \\ &= \{a^{2si}a^u b,\ a^{2si}a^{2j_0-u}b \mid 0 \le i \le m-1\}\end{aligned}$$

（作为 $t \equiv j_0$ （模 s））。

注意，对于 $u = j_0$, $a^{2si}a^{j_0} = a^{2si}a^{2j_0-u}$对所有 $0 \le i \le m-1$均成立，因此

$$(a^{j_0}b)^{D_{2n}}_{\sigma_0} = \{a^{2si}a^{j_0}b \mid 0 \le i \le m-1\}.$$

所以 $|(a^{j_0}b)^{D_{2n}}_{\sigma_0}| = m$。现在，令 $u \in \{j_0+1, ..., j_0+r_0\}$，使得 $u = j_0 + k$对某个 $1 \le k \le r_0$成立。若可能，假设对于某个 i_1, $a^{2si_1}a^u = a^{2si_2}a^{2j_0-u}$ $i_2 \in \{0, 1, ..., m-1\}$。

$\Rightarrow a^{2s(i_2-i_1)} = a^{2(u-j_0)}$.

$\Rightarrow 2s(i_2-i_1) \equiv 2(u-j_0) \pmod n$.

$\Rightarrow s(i_2-i_1) \equiv u-j_0 \pmod n$ as n is odd.

$\Rightarrow a^{s(i_2-i_1)} = a^{(u-j_0)}$.

$\Rightarrow a^{s(i_2-i_1)} = a^k$ as $u = j_0+k$.

$\Rightarrow a^k \in \langle a^s \rangle$.

由于 $|a^s| = m$ 和 $d = \frac{n}{m}$，因此 d 是满足 $a^d \in \langle a^s \rangle$的最小正整数。此外，由于 $r_0 < d = 1 + 2r_0$和 $k \in \{1, ..., r_0\}$，因此 $k < d$。综上，我们得到$a^k \in \langle a^s \rangle$，且 k 是满足 $k < d$的正整数。但这与 d 是满足 $a^d \in \langle a^s \rangle$的最小正整数相矛盾。因此，对于 $u \in \{j_0+1, ..., j_0+r_0\}$，集合 $(a^u b)^{D_{2n}}_{\sigma_0}$中的元素$a^{2si}a^{j_0}b$和 $a^{2sj}a^{2j_0-u}b$ $(0 \le i, j \le m-1)$彼此不同。因此，对于所有 $u \in \{j_0+1, ..., j_0+r_0\}$, $|(a^u b)^{D_{2n}}_{\sigma_0}| = 2m$。

此外，对于 $u \in \{j_0, j_0+1, ..., j_0+r_0\}$，这些集合 $(a^u b)^{D_{2n}}_{\sigma_0}$彼此不相交，并且

$$|1^{D_{2n}}_{\sigma_0}| + \sum_{k=1}^{\frac{n-1}{2}} |(a^k)^{D_{2n}}_{\sigma_0}| + |(a^{j_0}b)^{D_{2n}}_{\sigma_0}| + \sum_{k=1}^{r_0} |(a^{j_0+k}b)^{D_{2n}}_{\sigma_0}| = 1 + 2(\frac{n-1}{2}) + m + 2mr_0 = 2n = |D_{2n}|$$

因此，结合推论 $m + 2mr_0 = n$，我们得到所需结果。此外，这些不同的 σ_0-共轭类的数量为

$$1 + (\frac{n-1}{2}) + 1 + r_0 = \frac{1}{2}(n+d) + 1$$

作为 $r_0 = \frac{d-1}{2}$。 □

定理 5.10。设 n 为偶数。对于某个 $j_0 \in \{0,1,...,s-1\}$，记 $|\sigma_1(a)| = m$、 $d = \frac{n}{m}$ 和 $t \equiv j_0$ （模 s）。那么，以下结论成立。

(i) 若 m 为奇数（因此 d 为偶数），则 D_{2n} 恰有 $\frac{1}{2}(n+d)$ 个 $+2$ σ_1-共轭类，其表示为 by

$$\{1\},\ \{a^{\frac{n}{2}}\},\ \{a^k, a^{-k}\}\ for\ 1 \le k \le \frac{n}{2} - 1,$$

$$(a^u b)_{\sigma_1}^{D_{2n}} = \{a^{2si}a^u b \mid 0 \le i \le m-1\}\ for\ u = j_0, \frac{d}{2},$$

$$(a^u b)_{\sigma_1}^{D_{2n}} = \{a^{2si}a^u b, a^{2si}a^{2j_0-u}b \mid 0 \le i \le m-1\}\ for\ j_0+1 \le u \le j_0 + \frac{d}{2} - 1.$$

(ii) 若 m 为偶数，则 D_{2n} 恰有 $\frac{n}{2} + d + 2$ σ_1 个共轭类，其表示为

$$\{1\},\ \{a^{\frac{n}{2}}\},\ \{a^k, a^{-k}\}\ for\ 1 \le k \le \frac{n}{2} - 1,$$

$$(a^u b)_{\sigma_1}^{D_{2n}} = \{a^{2si}a^u b \mid 0 \le i \le m-1\}\ for\ u = j_0, d,$$

$$(a^u b)_{\sigma_1}^{D_{2n}} = \{a^{2si}a^u b, a^{2si}a^{2j_0-u}b \mid 0 \le i \le m-1\}\ for\ j_0+1 \le u \le j_0 + d - 1.$$

证明。注意 $1_{\sigma_1}^{D_{2n}} = \{1\}$ 和 $(a^{\frac{n}{2}})_{\sigma_1}^{D_{2n}} = \{a^{\frac{n}{2}}\}$。此外，对于 $1 \le k \le \frac{n}{2} - 1$，有 $(a^k)_{\sigma_1}^{D_{2n}} = \{a^k, a^{-k}\}$。

(i) 我们有

$$(a^u b)_{\sigma_1}^{D_{2n}} = \{a^{2si}a^u b,\ a^{2si}a^{2j_0-u}b \mid 0 \le i \le m-1\}$$

对所有 $u \in \{j_0, j_0+1, ..., j_0+r_0\}$，其中 r_0 是满足 $d = \underbrace{2+...+2}_{r_0 \text{次的正整数}}$ （作为 d 为偶 n)。注意， d 是满足 $a^d \in \langle a^s \rangle = \langle a^{2s} \text{的最小正整数} \rangle$.

对于 $u = j_0$，对所有 $0 \le i \le m-1$，都有 $a^{2si}a^u b = a^{2si}a^{2j_0-u}b$，使得

$$(a^{j_0} b)_{\sigma_1}^{D_{2n}} = \{a^{2si}a^{j_0} b \mid 0 \le i \le m-1\}.$$

因此， $|(a^{j_0}b)_{\sigma_1}^{D_{2n}}| = m$，因为 $|a^{2s}| = m = |a^s|$。现在，令 $u \in \{j_0+1, ..., j_0+r_0\}$。则对于某个 $k \in \{1, ..., r_0\}$，有 $u = j_0 + k$。任取一个固定的 $i_1 \in \{0,1,...,m-1\}$。那么存在某个 $i_2 \in \{0,1,...,m-1\}$，使得

$$a^{2si_1}a^u b = a^{2si_2}a^{2j_0-u}b \Leftrightarrow a^{2s(i_2-i_1)} = a^{2(u-j_0)} \Leftrightarrow a^{2s(i_2-i_1)} = a^{2k}$$

当 $u = j_0 + k \Leftrightarrow a^{2si_3} = a^{2k}$时，其中 $i_3 = i_2 - i_1 \Leftrightarrow a^{2k} \in \langle a^{2s} \rangle$。

由于 $1 \le k \le r_0$，因此 $2 \le 2k \le 2r_0 = d$。所以 $2k$ 是一个正整数 $\le d$。现在，若 $a^{2k} \in \langle a^{2s} \rangle$，那么由于 $2k \in \mathbb{N}$，且 $2k \le d$ 和 d 是满足 $a^d \in \langle a^{2s} \rangle$ 的最小正整数，因此，上述蕴含式成立当且仅当 $2k = d$，也就是说，$k = \frac{d}{2} = r_0$，从而 $u = j_0 + k = j_0 + r_0$。

由于 $a^{2k} \in \langle a^{2s} \rangle$ 对于 $k = r_0 = \frac{d}{2}$，因此根据上述推论，对于 $u = j_0 + r_0$，对每个 $i_1 \in \{0,1,...,m-1\}$，都存在某个 $i_2 \in \{0,1,...,m-1\}$使得 $a^{2si_1}a^u b = a^{2si_2}a^{2j_0-u}b$。因此，

$$\{a^{2si}a^u b \mid 0 \le i \le m-1\} = \{a^{2si}a^{2j_0-u}b \mid 0 \le i \le m-1\}$$

从而

$$(a^{j_0+r_0}b)_{\sigma_1}^{D_{2n}} = \{a^{2si}a^{j_0+r_0}b \mid 0 \le i \le m-1\}.$$

那么 $|(a^{j_0+r_0}b)_{\sigma_1}^{D_{2n}}| = m$。此外，对于 $2k < d$，也就是说，对于 k的其他取值，即对于 $k \in \{1, ..., r_0 - 1\}$，也就是说，对于 $u \in \{j_0 + 1, ..., j_0 + r_0 - 1\}$，我们有：对于每个$i$，$j \in \{0, 1, ..., m-1\}$、$a^{2si}a^ub$和 $a^{2sj}a^{2j_0-u}b$ $(0 \le i, j \le m-1)$ 都是 $(a^ub)_{\sigma_1}^{D_{2n}}$ 中互不相同的元素。因此，

$$(a^ub)_{\sigma_1}^{D_{2n}} = \{a^{2si}a^ub,\ a^{2si}a^{2j_0-u}b \mid 0 \le i \le m-1\}$$

因此 $|(a^ub)_{\sigma_1}^{D_{2n}}| = 2m$。

此外，当 $u \in \{j_0, j_0+1, ..., j_0+r_0\}$ 时，这些集合 $(a^ub)_{\sigma_1}^{D_{2n}}$ 彼此不相交。由于$d = 2r_0$ 且 $n = md = 2mr_0$，所以

$$\begin{aligned}
&|1_{\sigma_1}^{D_{2n}}| + |(a^{\frac{n}{2}})_{\sigma_1}^{D_{2n}}| + \sum_{k=1}^{\frac{n}{2}-1} |(a^k)_{\sigma_1}^{D_{2n}}| + |(a^{j_0}b)_{\sigma_1}^{D_{2n}}| + \sum_{k=1}^{r_0-1} |(a^{j_0+k}b)_{\sigma_1}^{D_{2n}}| + |(a^{j_0+r_0}b)_{\sigma_1}^{D_{2n}}| \\
&= 1 + 1 + 2(\frac{n}{2} - 1) + m + 2m(r_0 - 1) + m \\
&= 2n = |D_{2n}|.
\end{aligned}$$

因此，根据推论4.3，我们得到该结果。此外，这些不同的 σ_1-共轭类的数量为

$$1 + 1 + (\frac{n}{2} - 1) + 1 + (r_0 - 1) + 1 = \frac{n}{2} + r_0 + 2 = \frac{1}{2}(n + d) + 2.$$

(ii) 证明过程与 (i) 部分类似。 □

5.4 σ 的内导子与外导子 $\mathbb{F}D_{2n}$

定理 5.11. 设 n 为奇数，$\mathbb{F}$ 为任意域。记 $|\sigma_0(a)| = m$、$d = \frac{n}{m}$ 和 $t \equiv j_0$ (模 s)，其中 $j_0 \in \{0, 1, ..., s-1\}$。则 $\mathrm{Inn}_{\sigma_0}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$ 上的维数为$\frac{1}{2}(3n - d) - 1$，且一组基为

$$\mathcal{B}_0 = \{D_g \mid g \in \{a^k \mid 1 \le k \le \frac{n-1}{2}\} \cup \bigcup_{u=j_0}^{j_0+(\frac{d-1}{2})} \{a^{2si}a^ub \mid 1 \le i \le m-1\}$$
$$\cup \bigcup_{u=j_0+1}^{j_0+(\frac{d-1}{2})} \{a^{2si}a^{2j_0-u}b \mid 0 \le i \le m-1\}\}.$$

证明。由定理 5.9可知，当 n为奇数时，D_{2n}有 $r = \frac{1}{2}(n+d)+1$ σ_0-共轭类。于是，由推论 4.16可知，$\mathrm{Inn}_{\sigma_0}(\mathbb{F}D_{2n})$ 在 $\mathbb{F}$上的维数为$|D_{2n}| - r = \frac{1}{2}(3n - d)$，$-1$而集合 $\mathcal{B}_0$ 显然是一个 $\mathbb{F}$-基。

□

当 n 为奇数时，通过在定理 $\mathbb{F}$5$\mathbb{F}D_{2n}$.11中取 σ_0 为恒等端同态，可得普通内导子的 $\mathbb{F}D_{2n}$ -向量空间 Inn($\mathbb{F}D_{2n}$) 的维数为 3($\frac{n-1}{2}$)。此外，我们还得到 Inn($\mathbb{F}D_{2n}$) 的一个 $\mathbb{F}$-基。

定理 5.12。设 n 为偶数， $\mathbb{F}$ 为任意域。记 $|\sigma_1(a)| = m$, $d = \frac{n}{m}$ 和$t \equiv j_0$ (模 s)，其中 $j_0 \in \{0, 1, ..., s-1\}$为某个元素。则以下结论成立。

(i) 若 m为奇数，则 Inn$_{\sigma_1}$($\mathbb{F}D_{2n}$) 在 $\mathbb{F}$ 上的维数为 $_{12}(3n-d)$ − 2，且一组基为 i s

$$\mathcal{B}_{o,1} = \{D_g \mid g \in \{a^k \mid 1 \le k \le \frac{n}{2} - 1\} \cup \bigcup_{u=j_0}^{j_0+\frac{d}{2}} \{a^{2si}a^u b \mid 1 \le i \le m-1\}$$
$$\cup \bigcup_{u=j_0+1}^{j_0+\frac{d}{2}-1} \{a^{2si}a^{2j_0-u}b \mid 0 \le i \le m-1\}\}.$$

(ii) 若 m 为偶数，则 Inn$_{\sigma_1}$($\mathbb{F}D_{2n}$) 在 $\mathbb{F}$ 上的维数为 $\frac{3n}{2} - d - 2$，且一组基为

$$\mathcal{B}_{e,1} = \{D_g \mid g \in \{a^k \mid 1 \le k \le \frac{n}{2} - 1\} \cup \bigcup_{u=j_0}^{j_0+d} \{a^{2si}a^u b \mid 1 \le i \le m-1\}$$
$$\cup \bigcup_{u=j_0+1}^{j_0+d-1} \{a^{si}a^{2j_0-u}b \mid 0 \le i \le m-1\}\}.$$

证明。 由推论 4.16 和定理 5.10. □

在定理 σ_1 中取恒等端同态 5。12 可得，当 n 为偶数时，普通内导子 $\mathbb{F}$-向量空间 Inn($\mathbb{F}D_{2n}$) 的维数为 3($\frac{n}{2} - 1$)。此外，我们还得到 Inn($\mathbb{F}D_{2n}$) 的一组 $\mathbb{F}$-基。

根据注记 2.7以及本节得到的定理，下面给出一个必要推论，解答二面体群代数 σ的扭导子问题，其中 $\mathbb{F}D_{2n}$ 是任意特征的 $\mathbb{F}$ 域。

推论 5.13. 设 $\mathbb{F}$ 是特征为 0 的域，或特征为有理素数 p 的域，且 $\sigma = \sigma_0$ 或 σ_1。

(i) 若 char($\mathbb{F}$) $= 0$ 或为奇素数 p ，且 gcd(n, p) $= 1$，则 $\mathbb{F}D_{2n}$ 的所有 σ-导子都是内导子，即 Inn$_\sigma$($\mathbb{F}D_{2n}$) $= \mathcal{D}_\sigma$($\mathbb{F}D_{2n}$)。换言之， $\mathbb{F}D_{2n}$ 没有非零外σ-导子，即 Out$_\sigma$($\mathbb{F}D_{2n}$) $= \{0\}$。

(ii) 若 char($\mathbb{F}$) $= 2$ 或 char($\mathbb{F}$) $= p$ 且 gcd(n, p) $\neq 1$，则 Inn$_\sigma$($\mathbb{F}D_{2n}$) $\subsetneq \mathcal{D}_\sigma$($\mathbb{F}D_{2n}$)。换言之，$\mathbb{F}D_{2n}$ 存在非零外 σ-导子，即 Out$_\sigma$($\mathbb{F}D_{2n}$) $\neq \{0\}$。

6 编码理论中的应用：IDD 码

在 [18, 例 3.16 和例 3.17], 中，作者通过将扩展二元戈莱 [24, 12, 8] 码和扩展二元二次剩余 [48, 24, 12] 码分别构造为群代数 $\mathbb{F}_2C_{24}$和 $\mathbb{F}_2C_{48}$ 的导子像，展示了导子在编码理论中的应用。这里 $\mathbb{F}_2$ 表示一个阶为 2 的特征为 2 的域，而 C_{24}， C_{48} 分别是阶为 24 和 48 的循环群。关于编码理论基础，读者可参阅[21, 28, 37]。

本节将上述例子统一为导子像导出码理论，记作 IDD 码。设 R 是含幺交换环， G 是阶为 n的有限群。我们给出一种群环 RG 码的一般构造，该码源自某个扭导子像的子集。随后，我们在 $R^n(=\underbrace{R\times ...\times R}_{n}$ ）上构造一个 R-模。为说明上述构造，我们给出次一些示例，通过使用有限域上群代数的扭导子来构造若干码。

6.1 构造与定义

设 R是交换含幺环， $G=\{g_1,g_2,...,g_n\}$是一个阶为 n且元素顺序已给定的有限群。设 σ、τ是群代数RG上的 R-代数自同态。设 D是 RG的一个（σ， τ）-导子。

D 的像 Im(D) 是 R-模 RG 的一个 R-子模，其生成集为 $D(G)=\{D(g_i)\mid 1\le i\le n\}$。它在 RG 中生成一个 (n,r)-码，其中 $r=$ rank(Im(D))，即 R-模 Im(D) 的秩。

假设 $S=\{D(g_{i_1})\ D(g_{i_2})\ ...,D(g_{i_s})\}$ 是 Im(D) 的一个 R-线性无关子集。那么 S 生成 Im(D) 的一个秩为 s 的子模。因此， S 生成一个 (n,s)-码。

定义 6.1. 设 D 是 RG 的一个 (σ,τ)-扭导子，且 $T=\{g_{k_1},g_{k_2},...,g_{k_t}\}$, $t<n$ 是 G 的一个子集，使得 $D(T)$ 是 RG 的一个 R-线性无关子集。那么，子模 $W=\langle D(T)\rangle$ 生成一个 (n,t)-码，称为导子像导出码，记作 IDD 码。码 W 的长度为 n ，维数为 t ，即 R-模 W 的秩。

6.2 R^n中的等价IDD码

下面，我们给出 R^n中一个等价码的构造。

我们使用 $\underline{\alpha}$ 来表示 $\underline{\alpha}$ 是一个向量，而不是群环 RG的元素 α 。对于 $\underline{\alpha}=(\lambda_1,\lambda_2,...,\lambda_n)\in R^n$, 由下式定义的映射 ζ: $R^n\to RG$

$$\zeta(\underline{\alpha})=\sum_{i=1}^{n}\lambda_i g_i=\alpha$$

根据 G给定的列示，它是 RG中的一个元素。

对于每个 $i\in\{1,2,...,n\}$，假设 $D(g_i)=\sum_{j=1}^{n}\lambda_{ij}g_j$。那么

$$\zeta^{-1}(D(g_i))=(\lambda_{i1},\lambda_{i2},...,\lambda_{in}).$$

构造一个 $n \times n$ 矩阵 B，其前 n 行为

$$\zeta^{-1}(D(g_1)),\ \zeta^{-1}(D(g_2)),\ ...,\ \zeta^{-1}(D(g_n)).$$

更确切地说，

$$B = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & ... & \alpha_{nn} \end{pmatrix}.$$

定理 6.2. 群 G 的任意行 $i_1, i_2, ..., i_t$ 线性无关，当且仅当集合 $\{D(\theta_{i_1})\ D(\theta_{i_2})\ ..., D(\theta_{i_t})\}$ 线性无关。

下面给出构造步骤：

(i) 假设 W 是一个 IDD 码。那么，对于群 G 的某个线性无关子集 S，有 $W = \langle S \rangle$，例如 $S = \{D(g_{k_1})\ D(g_{k_2})\ ..., D(g_{k_s})\}$。

(ii) 选取 $\underline{w} \in R^s$ 和 $\underline{w} = (\lambda_1, \lambda_2, ..., \lambda_s)$。

(iii) 将 $\underline{w}$ 写作 $\underline{\alpha}$，其中 λ_j 位于位置 k_j，其余位置为零。

(iv) $\underline{\alpha}$ 可以是 通过 $\alpha = \zeta(\underline{\alpha}) = \sum_{j=1}^{s} \lambda_j g_{k_j}$ 映射为 RG 中的一个元素和一个码字

$$D(\alpha) = D(\zeta(\underline{\alpha})) = D(\sum_{j=1}^{s} \lambda_j g_{k_j}) = \sum_{j=1}^{s} \lambda_j D(g_{k_j})$$

等同于 $\mathcal{E}$ 中由下式给出的一个码字

$$\zeta^{-1}(D(\alpha)) = \underline{\alpha} B.$$

(v) 因此，根据定理 6.2，我们得到一个 $(n,\ s)$ 码

$$\mathcal{E} = \{\underline{x}B \mid \underline{x} \text{ extends } \underline{w} \in \mathbb{F}^s \text{ to } \mathbb{F}^n\}.$$

6.3 示例

在本小节中，我们使用 SAGE-MATH 构造一些 IDD 码，从而举例说明上述构造。

例6.3。考虑一个特征为2的有限域 $\mathbb{F}_{2^t}$ 以及 $G = C_{18} = \langle x \mid x^{18} = 1 \rangle = \{1, x, ..., x^{17}\}$，后者是一个阶为18的循环群。

(i) 映射 $D:\ \mathbb{F}_{2^t}C_{18} \to \mathbb{F}_{2^t}C_{18}$ 定义为

$$D(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^8 + x^{11}$$

and

$$D(x^k) = k(\sigma(x))^{k-1}D(x)$$

$(1 \leq k \leq 17)$ 是 σ-导子，作用于 $\mathbb{F}_{2^t}C_{18}$，对每个 σ 上的群自同态 C_{18}（将其 $\mathbb{F}_{2^t}$-线性扩张到整个 $\mathbb{F}_{2^t}C_{18}$），根据定理 3.15。下面，我们取 $\sigma = id$（恒等映射），由此得到以下二元 IDD 码。

基 S_i	**Code** 描述: $[n.k.d]$	**Code** 性质	对偶码 描述: $[n,k,d]$
$S_1 = \{D(x^i) \mid i \in \{1,5,7,9,11,13,15,17\}\}$	$[18,8,6]$	最优 & 非 LCD	$[18,10,4]$
$S_1 \setminus \{D(x^{13})\}$	$[18,7,6]$	非 LCD	$[18,11,3]$
$S_2 \setminus \{D(x^7)\}$	$[18,6,6]$	非 LCD	$[18,12,2]$
$S_3 \setminus \{D(x^9)\}$	$[18,5,6]$	非 LCD	$[18,13,2]$
$S_1 = \{D(x^i) \mid i \in \{1,5,9,13\}\}$	$[18,4,8]$	最优 & 非 LCD	$[18,14,2]$ (最优)

使用基 S_1 生成的二元 $[18,8,6]$ 最优非 LCD IDD 码的生成矩阵 8×18 为

$$\begin{pmatrix}
1&1&1&1&1&1&0&0&1&0&0&1&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&1&1&0&0&1&0&0&1&0&0\\
0&0&0&0&0&0&1&1&1&1&1&1&0&0&1&0&0&1\\
0&1&0&0&0&0&0&0&1&1&1&1&1&1&0&0&1&0\\
1&0&0&1&0&0&0&0&0&0&1&1&1&1&1&1&0&0\\
0&0&1&0&0&1&0&0&0&0&0&0&1&1&1&1&1&1\\
1&1&0&0&1&0&0&1&0&0&0&0&0&0&1&1&1&1\\
1&1&1&1&0&0&1&0&0&1&0&0&0&0&0&0&1&1
\end{pmatrix}.$$

(ii) 类似地，映射 D_2： $\mathbb{F}_{2^t}C_{18} \to \mathbb{F}_{2^t}C_{18}$ 定义为

$$D(x) = 1 + x + x^3 + x^4 + x^7 + x^9 + x^{13} + x^{16} + x^{17}$$

对于 C_1的任意群自同态 σ，它都将是 $\mathbb{F}_{2^t}C_{18}$ 的一个 σ-导子 $_{8.}$
考虑 σ de 由 $\sigma(x) = x^2$ 定义。然后，我们得到以下二元 IDD 码表 .

基 S_i	**Code** 描述: $[n.k.d]$	**Code** 性质	对偶码 描述: $[n,k,d]$
$S_1 = \{D(x^i) \mid i \in \{1,3,5,7,9,11,13,15,17\}\}$	$[18,9,5]$	非 LCD	$[18,9,5]$
$S_2 = S_1 \setminus \{D(x^{15})\}$	$[18,8,5]$	非 LCD	$[18,10,3]$
$S_3 = S_2 \setminus \{D(x^{11})\}$	$[18,7,5]$	LCD	$[18,11,3]$
$S_4 = S_3 \setminus \{D(x^3)\}$	$[18,6,5]$	非 LCD	$[18,12,3]$
$S_5 = S_4 \setminus \{D(x^7)\}$	$[18,5,5]$	LCD	$[18,13,3]$ （最优）
$S_6 = S_5 \setminus \{D(x^{17})\}$	$[18,4,8]$	最优 & 非 LCD	$[18,14,2]$ （最优）
$S_7 = S_4 \setminus \{D(x^{17})\}$	$[18,5,6]$	非 LCD	$[18,13,2]$
$S_8 = S_7 \setminus \{D(x^{13})\}$	$[18,4,7]$	非 LCD	$[18,14,2]$ (最优)
$S_9 = S_6 \setminus \{D(x^{13})\}$	$[18,3,9]$	LCD	$[18,15,1]$
$S_{10} = S_8 \setminus \{D(x)\}$ 或 $S_8 \setminus \{D(x^5)\}$	$[18,3,8]$	LCD	$[18,15,1]$
$S_{11} = S_8 \setminus \{D(x^9)\}$	$[18,3,7]$	LCD	$[18,15,1]$
$S_{12} = S_{11} \setminus \{D(x^7)\}$	$[18,2,9]$	LCD	$[18,16,1]$

由基 S_1 生成的二元非 LCD IDD 码的 9×18 生成矩阵为 $[18,9,5]$

$$\begin{pmatrix} 1&1&0&1&1&0&0&1&0&1&0&0&0&1&0&0&1&1 \\ 0&0&1&1&1&1&0&1&1&0&0&1&0&1&0&0&0&1 \\ 0&0&0&1&0&0&1&1&1&1&0&1&1&0&0&1&0&1 \\ 0&1&0&1&0&0&0&1&0&0&1&1&1&1&0&1&1&0 \\ 0&1&1&0&0&1&0&1&0&0&0&1&0&0&1&1&1&1 \\ 1&1&1&1&0&1&1&0&0&1&0&1&0&0&0&1&0&0 \\ 0&1&0&0&1&1&1&1&0&1&1&0&0&1&0&1&0&0 \\ 0&1&0&0&0&1&0&0&1&1&1&1&0&1&1&0&0&1 \\ 1&0&0&1&0&1&0&0&0&1&0&0&1&1&1&1&0&1 \end{pmatrix}.$$

例 6.4. 设 $\mathbb{F}_{2^t}$ 是特征为2的有限域，$G = C_{14} = \langle x \mid x^{14} = 1\rangle = \{1, x, ..., x^{13}\}$ 是一个阶为14的循环群。

以下每个映射 D_i 定义了一个 σ-导子 $\mathbb{F}_{2^t}C_{14}$，根据定理 3.15，对于任意端同态 σ 从 C_{14}。

下文取 $\sigma = id$ （恒等映射）。下表列出使用群环 $\mathbb{F}_{2^t}C_{14}$ 的不同导子构造的、具有不同参数和性质的一些 IDD 码。

$D_i(x)$ 带基	**Code** 描述: $[n,k,d]$	其他 性质 的码	对偶码 描述: $[n,k,d]$
$1+x+x^2+x^3+x^4+x^6+x^9$ 基 $=\{D(x^i) \mid i\in\{1,3,5,7,9,11,13\}\}$	$[14,7,4]$	最优 & LCD	$[14,7,4]$ (最优)
$1+x+x^2+x^3+x^4+x^9$ 基 $=\{D(x^i) \mid i\in\{1,3,5,7,9,11,13\}\}$	$[14,7,4]$	最优 & 非 LCD	$[14,7,4]$ (最优)
$1+x+x^2+x^3+x^5+x^8+x^{11}$ 基 $=\{D(x^i) \mid i\in\{1,3,5,7,9,11,13\}\}$	$[14,7,3]$	LCD	$[14,7,3]$
$1+x+x^3+x^4+x^5+x^6+x^9$ 基 $=\{D(x^i) \mid i\in\{1,3,5,7\}\}$	$[14,4,7]$	最优 & 非 LCD	$[14,10,3]$ (最优)
$1+x+x^2+x^4+x^5+x^8$ 基 $=\{D(x^i) \mid i\in\{1,3,5,7,9,11\}\}$	$[14,6,4]$	LCD	$[14,8,3]$
$1+x+x^2+x^4+x^5+x^7+x^{10}$ 基 $=\{D(x^i) \mid \{i\in\{1,3,5,7,9,11,13\}\}$	$[14,7,3]$	非 LCD	$[14,7,3]$

使用 D_1 得到的二元 $[14,7,4]$ 最优 LCD IDD 码的 7×14 生成矩阵为

$$\begin{pmatrix} 1&1&1&1&1&0&1&0&0&1&0&0&0&0\\ 0&0&1&1&1&1&1&0&1&0&0&1&0&0\\ 0&0&0&0&1&1&1&1&1&0&1&0&0&1\\ 0&1&0&0&0&0&1&1&1&1&1&0&1&0\\ 1&0&0&1&0&0&0&0&1&1&1&1&1&0\\ 1&0&1&0&0&1&0&0&0&0&1&1&1&1\\ 1&1&1&0&1&0&0&1&0&0&0&0&1&1 \end{pmatrix}.$$

此外，使用D_3 得到的二元 $[14,7,3]$ LCD IDD 码的 7×14 生成矩阵为

$$\begin{pmatrix} 1&1&1&1&0&1&0&0&1&0&0&1&0&0\\ 0&0&1&1&1&1&0&1&0&0&1&0&0&1\\ 0&1&0&0&1&1&1&1&0&1&0&0&1&0\\ 1&0&0&1&0&0&1&1&1&1&0&1&0&0\\ 0&0&1&0&0&1&0&0&1&1&1&1&0&1\\ 0&1&0&0&1&0&0&1&0&0&1&1&1&1\\ 1&1&0&1&0&0&1&0&0&1&0&0&1&1 \end{pmatrix}.$$

(i) 考虑 D_1。我们得到以下二元 IDD 码。

基 S_i ,1	**Code** 描述: $[n,k,d]$	其他 性质 的码	对偶码 描述: $[n,k,d]$
$\{D(x^i) \mid i \in \{1,3,5,7,11,13\}\}$	$[14,6,4]$	LCD	$[14,8,3]$
$\{D(x^i) \mid i \in \{1,3,5,7,13\}\}$, $\{D(x^i) \mid i \in \{1,3,5,11,13\}\}$	$[14,5,5]$	LCD	$[14,9,3]$
$\{D(x^i) \mid i \in \{1,3,5,7\}\}$, $\{D(x^i) \mid i \in \{1,3,5,13\}\}$	$[14,4,6]$	非 LCD	$[14,10,2]$
$\{D(x^i) \mid i \in \{1,5,13\}\}$	$[14,3,6]$	非 LCD	$[14,11,1]$
$\{D(x^i) \mid i \in \{1,3,5\}\}$	$[14,3,6]$	LCD	$[14,11,1]$
$\{D(x^i) \mid i \in \{1,3,7,11\}\}$	$[14,4,4]$	非 LCD	$[14,10,2]$
$\{D(x^i) \mid i \in \{1,3,9,13\}\}$	$[14,4,5]$	LCD	$[14,10,2]$
$\{D(x^i) \mid i \in \{1,5\}\}$	$[14,2,7]$	LCD	$[14,12,1]$

(ii) 考虑 D_3。我们得到以下二元 IDD 码。

基 S_i ,3	**Code** 描述: $[n,k,d]$	其他 性质 的码	对偶码 描述: $[n,k,d]$
$\{D(x^i) \mid i \in \{1,3,5,7,9,13\}\}$	$[14,6,3]$	LCD	$[14,8,2]$
$\{D(x^i) \mid i \in \{1,3,5,9,13\}\}$	$[14,5,3]$	LCD	$[14,9,2]$
$\{D(x^i) \mid i \in \{1,3,5\}\}$	$[14,3,7]$	LCD	$[14,11,2]$ (最优)
$\{D(x^i) \mid i \in \{1,3,5,9\}\}$	$[14,4,4]$	LCD	$[14,10,2]$
$\{D(x^i) \mid i \in \{1,3,11,13\}\}$	$[14,4,3]$	LCD	$[14,10,2]$
$\{D(x^i) \mid i \in \{1,5\}\}$	$[14,2,7]$	LCD	$[14,12,1]$

例 6.5。设 $\mathbb{F}_{3^t}$ 为特征 3 的有限域, $G = C_{24} = \langle x \mid x^{24} = 1\rangle = \{1, x, ..., x^{23}\}$为阶 24 的循环群。

映射 D：由 $\mathbb{F}_{3^t}C_{24} \to \mathbb{F}_{3^t}C_{24}$ 定义为

$$D(x) = 1 + x + x^3 + x^4 + x^5 + x^7 + x^9 + x^{12} + x^{14}$$

and

$$D(x^k) = k(\sigma(x))^{k-1}D(x)$$

$(1 \le k \le 23)$ 是 σ-导子，对 $\mathbb{F}_{3^t}C_{24}$ 中的每个群自同态 σ （ C_{24} 将其 $\mathbb{F}_{3^t}$-线性延拓至 $\mathbb{F}_{3^t}C_{24}$的整个空间后），由定理 3.15可知。

下文中，我们取 $\sigma(x) = x^5$。由此得到以下三元 IDD 码。

基 S_i	**Code** 描述: $[n,k,d]$	其他 性质 的码	对偶码 描述: $[n,k,d]$
$S_1=\{D(x^i) \mid 1\le i\le 23,\ i\notin\{3,6,9,12,15,18,21\}\}$	$[24,16,3]$	LCD	$[24,8,7]$
$S_2=S_1\setminus\{D(x)\}$	$[24,15,4]$	LCD	$[24,9,7]$
$S_3=S_1\setminus\{D(x^2)\}$	$[24,15,3]$	LCD	$[24,9,7]$
$S_4=S_1\setminus\{D(x)\ D(x^2)\}$	$[24,14,4]$	非 LCD	$[24,10,6]$
$S_5=S_1\setminus\{D(x)\ D(x^4)\}$	$[24,14,4]$	LCD	$[24,10,7]$
$S_6=S_1\setminus\{D(x)\ D(x^7)\}$	$[24,14,5]$	LCD	$[24,10,7]$
$S_7=S_1\setminus\{D(x)\ D(x^{19})\}$	$[24,14,5]$	非 LCD	$[24,10,7]$
$S_8=S_1\setminus\{D(x)\ D(x^2)\ D(x^7)\}$	$[24,13,5]$	非 LCD	$[24,11,5]$
$S_9=S_1\setminus\{D(x)\ D(x^4)\ D(x^7)\}$	$[24,13,5]$	非 LCD	$[24,11,7]$
$S_{10}=S_1\setminus\{D(x^7)\ D(x^{11})\ D(x^{14})\}$	$[24,13,5]$	LCD	$[24,11,6]$
$S_{11}=S_1\setminus\{D(x)\ D(x^4)\ D(x^7)\ D(x^{11})\}$	$[24,12,6]$	非 LCD	$[24,12,6]$
$S_{12}=S_1\setminus\{D(x)\ D(x^4)\ D(x^7)\ D(x^{14})\}$	$[24,12,6]$	LCD	$[24,12,6]$
$S_{13}=S_1\setminus\{D(x)\ D(x^4)\ D(x^7)\ D(x^{23})\}$	$[24,12,5]$	LCD	$[24,12,5]$
$S_{14}=S_1\setminus\{D(x^4)\ D(x^7)\ D(x^{16})\ D(x^{23})\}$	$[24,12,4]$	LCD	$[24,12,4]$
$S_{15}=S_1\setminus\{D(x)\ D(x^2)\ D(x^4)\ D(x^7)\ D(x^{14})\}$	$[24,11,7]$	非 LCD	$[24,13,5]$
$S_{16}=S_1\setminus\{D(x)\ D(x^4)\ D(x^7)\ D(x^{14})\ D(x^{23})\}$	$[24,11,6]$	LCD	$[24,13,5]$
$S_{17}=S_1\setminus\{D(x)\ D(x^2)\ D(x^4)\ D(x^5)\ D(x^7)\ D(x^{14})\}$	$[24,10,7]$	LCD	$[24,14,5]$
$S_{18}=\{D(x^i) \mid i\in\{8,10,11,16,17,19,20,22,23\}\}$	$[24,9,8]$	LCD	$[24,15,3]$
$S_{19}=\{D(x^i) \mid i\in\{8,10,11,13,16,19,20,22,23\}\}$	$[24,9,7]$	LCD	$[24,15,3]$
$S_{20}=\{D(x^i) \mid i\in\{8,10,11,16,17,19,20,23\}\}$	$[24,8,8]$	LCD	$[24,16,3]$
$S_{21}=\{D(x^i) \mid i\in\{8,11,16,17,19,20,23\}\}$	$[24,7,9]$	LCD	$[24,17,2]$
$S_{22}=\{D(x^i) \mid i\in\{11,16,17,19,20,23\}\}$	$[24,6,9]$	LCD	$[24,18,2]$
$S_{23}=\{D\ (x^i) \mid i\in\{11,16,17,19,23\}\}$	$[24,5,9]$	LCD	$[24,19,1]$
$S_{43}=\{D(x^i) \mid i\in\{16,17,19,23\}\}$	$[24,4,9]$	LCD	$[24,20,1]$

一个 16×24 ge 使用基 S_1 得到的三元 $[24,16,3]$ LCD IDD 码的生成矩阵为

$$\begin{pmatrix}
1&1&0&1&1&1&0&1&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&2&2&0&2&2&2&0&2&0&2&0&0&2&0&2&0&0&0&0\\
1&0&0&1&0&1&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&1&0\\
2&2&0&2&0&2&0&0&2&0&2&0&0&0&0&0&0&0&0&0&2&2&0&2\\
0&0&0&0&0&0&1&1&0&1&1&1&0&1&0&1&0&0&1&0&1&0&0&0\\
0&2&0&0&0&0&0&0&0&0&0&2&2&0&2&2&2&0&2&0&2&0&0&2\\
1&1&1&0&1&0&1&0&0&1&0&1&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&2&2&0&2&2&2&0&2&0&2&0&0&2&0&2&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&1&0&1&0&0\\
2&0&2&0&0&2&0&2&0&0&0&0&0&0&0&0&0&0&2&2&0&2&2&2&0\\
0&0&0&1&1&0&1&1&1&0&1&0&1&0&0&1&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&2&2&0&2&2&2&0&2&0&2&0&0&2&0&2&0\\
0&1&0&1&0&0&1&0&1&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1\\
2&0&2&2&2&0&2&0&2&0&0&2&0&2&0&0&0&0&0&0&0&0&0&2\\
0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&1&0&1&0&0&1&0&1\\
0&0&2&0&2&0&0&0&0&0&0&0&0&0&2&2&0&2&2&2&0&2&0&2
\end{pmatrix}.$$

例6.6。设 $\mathbb{F}_{2^t}$ 为特征为2的有限域，且

$$G = D_{12} = \langle a, b \mid a^6 = 1 = b^2, b^{-1}ab = a^{-1} \rangle = \{1, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\}$$

阶为12的二面体群。

根据定理 5.8，映射 $D : \mathbb{F}_{2^t}D_{12} \to \mathbb{F}_{2^t}D_{12}$ 定义为

$$D(a) = 1 + a + a^3 + a^4 + ab + a^2b + a^4b + a^5b$$

and

$$D(b) = a + a^2 + a^4 + a^5 + b + a^2b + a^3b + a^5b$$

是群自同态 σ_1 （定义在 D_{12} 上）的 σ_1-导子，定义为 $\sigma_1(a) = a^2$ 和$\sigma_1(b) = ab$。

以下每个集合

基 S_i
$S_1 = \{D(a)\ D(a^2)\ D(a^3)\ D(b)\}$
$S_2 = \{D(a^2)\ D(a^3)\ D(a^5)\ D(a^2b)\}$
$S_3 = \{D(a)\ D(a^2)\ D(a^5)\ D(b)\}$
$S_4 = \{D(a^3)\ D(a^5)\ D(b)\ D(a^2b)\}$
$S_5 = \{D(a)\ D(a^5)\ D(b)\ D(a^2b)\}$

生成一个 $[12, 4, 4]$ 二元自正交非 LCD IDD 码。

7 结论

本文研究了交换含幺环R 上的群 G的 RG 的（σ, τ）-导子。在第 3 节中，我们首先得到了一个必要且充分的条件，该条件说明群的生成集上定义的映射何时可以扩张为群环的 σ-和（σ, τ）-导子；随后刻画了正特征域上的交换群代数的 σ-导子。在第 4 节中，我们利用群中的（σ, τ）-共轭类研究了群代数的内（σ, τ）-导子。我们根据相应的、由所有内（σ, τ）-导子构成的 R-模的秩和基，刻画了任意交换环 R 上任意群 G 的群代数 RG 的所有内（σ, τ）-导子。此外，我们发现，如果群 G 的阶在（含幺）环 R中可逆，那么群环 RG 的（σ, τ）-导子就是内导子。最后，在第 5 节中，我们将第3节和第4节所得结果应用于任意特征域上的二面体群代数，明确分类了其所有内导子和外导子。因此，我们解决了二面体群代数中的σ-扭导子问题。在第 6 节中，我们提出了 IDD 码的概念（给出了定义及构造），并通过在 SAGEMATH 中实现该构造、生成具有不同参数的码来加以说明。

致谢

作者谨向审稿人和编辑致以诚挚谢意，感谢他们提出的批评性评审意见、评论和建议，这些意见极大地改善了论文的表述和质量。第二作者是 ConsenSys 区块链讲席教授。他感谢 ConsenSys AG 给予这一荣誉。

参考文献

[1] Aleksandr Alekseev、Andronick Arutyunov 和 Sergei Silvestrov。关于群代数的（σ,τ）-导子作为范畴特征。载于随机过程与代数结构国际会议，第 81–99 页，2019年。[2] Orest D. Artemovych、Victor A. Bovdi 和 Mohamed A. Salim。群环的导子。《数学科学学报》，86(1):51–72，2020。[3] A. A. Arutyunov 和 Lev M. Kosolapov。有限群和 FC 群的群环导子。《有限域及其应用》，76:101921，2021年。[4] A. A. Arutyunov、A. S. Mishchenko 和 A. I. Shtern。群代数的导子。数学科学杂志，248(6):709–718，2020。[5] Andronick Arutyunov。群代数中的导子与群的组合不变量。欧洲数学杂志，9(2):39，2023年。[6] Andronick Arutyunov 和 Aleksandr Alekseev。n-范畴复形与群代数中的导子。拓扑学及其应用，275:107002，2020。[7] Andronick Aramovich Arutyunov。群代数中导子的组合描述。俄罗斯数学，64(12):67–73，2020。[8] Andronick Aramovich Arutyunov。非交换群代数中的导子代数。斯捷克洛夫数学研究所报告，308(1):22–34，2020。[9] Andronick Aramovich Arutyunov 和 Alexandr Sergeevich Mishchenko。关于群代数导子 Johnson 问题的光滑版本。《数学文集》，210(6):756，2019年。[10] Mehsin Jabel Atteya。新型置换 n-导子及其在结合环上的应用。《对称性》，12(1):46，2019。[11] CJK Batty。 C^*-代数张量积的导子。《伦敦数学会杂志》，2(1):129–140，1978。[12] M. Bresar。关于环的（α,β）-导子的复合及其在冯·诺伊曼代数中的应用。《数学科学学报》，56:369–375，1992。[13] Muhammad Anwar Chaudhry 和 Zafar Ullah。关于格上的广义（α, β）-导子。《数学问题》，34(4):417–424，2011。[14] Dishari Chaudhuri。关于交换代数上的（σ,τ）-导子的一则注记。arXiv 预印本 arXiv:1912.12812，2019年。[15] Dishari Chaudhuri。群环的（σ,τ）-导子。《代数通讯》，47(9):3800–3807，2019年。

[16] Dishari Chaudhuri. 群环的扭曲导子问题. Archiv der Math- ematik, 116(4):391–401, 2021年.[17] Chen-Lian Chuang 和 Tsiu-Kwen Lee. 单个斜导子的恒等式. 《代数杂志》, 288(1):59–77, 2005.[18] Leo Creedon 和 Kieran Hughes. 具有编码理论应用的群代数上的导子. 《有限域及其应用》, 56:247–265, 2019年.[19] Boucher Delphine 和 Felix Ulmer. 利用具有自同构和导子的斜多项式构造线性码. 《设计、码与密码学》, 70:405–431, 2014.[20] Basudeb Dhara、Sukhendu Kar 和 Swarup Kuila. 关于素环中2阶广义导子和多重线性多项式的注记. 《越南数学学报》, 47(4):755–773, 2022.[21] Steven T Dougherty. 有限交换环上的代数编码理论. 施普林格, 2017.[22] M¨unevver Pınar Ero˘glu 和 Tsiu-Kwen Lee. 导子多项式的像. 《代数通讯》, 45(10):4550–4556, 2017.[23] Miguel Ferrero、Antonio Giambruno 和 C´esar Polcino Milies. 关于群环的导子的注记. 《加拿大数学通报》, 38(4):434–437, 1995.[24] Martin Liebeck Gordon James. 《群的表示与特征标》. 剑桥大学出版社, 第二版, 2003.[25] M. Haetinger、C. Ashraf 和 S. Ali. 关于高阶导子：综述. 《国际数学、博弈论与代数杂志》, 18:359–379, 2011.[26] Adrienne A Hall. 某些 C^*-代数的导子. Journal of the London Mathematical Society, 2(2):321–329, 1972.[27] Jonas T Hartwig、Daniel Larsson 和 Sergei D Silvestrov. 利用 σ-导子的李代数的变形. 《代数杂志》, 295(2):314–361, 2006.[28] Raymond Hill. 《编码理论入门》. 牛津大学出版社, 1986.[29] Toshiharu Ikeda 和 N Kawamoto. 关于群代数的导子代数. Non- Associative Algebra and Its Applications, 第188–192页, 1994.[30] Kwalombota Ilwale. 《扭曲导子的非交换黎曼几何》. 博士学位论文, Link¨oping University Electronic Press, 2023年.[31] N. Jacobson. 《环的结构》. CP37. 美国数学会 , 1964.[32] Jeremiah William Johnson. 从 D_m 到 D_n 的群同态数目 . 《大学数学杂志》 , 44(3):190–192, 2013.

[33]L. Kamali Ardakani 和 Bijan Davvaz. MV-代数的 f-导子和 (f,g)-导子. 代数系统杂志, 1(1):11–31, 2013.[34] Kyung Ho Kim. 关于倾斜代数的 (f,g)- 导子 . 忠清数学会杂志 , 27(4):643–649, 2014.[35] Slawomir Klimek 和 Matt McBride. 与单生成群相关代数中的无界导子. 澳大利亚数学会杂志, 111(3):345– 371, 2021年.[36] Daniel Larsson. （算术）概形上的等变 hom-Lie 代数和扭曲导子. 数论杂志, 176(249-278), 2017.[37] San Ling 和 Chaoping Xing. 编码理论：入门课程. 剑桥大学出版社, 2004.[38] Praveen Manju 和 Rajendra Kumar Sharma. 非交换群代数的导子. 代数及其应用杂志, doi: 10.1142/S0219498825503712.[39] Philip Miles. B^* 代数上的导子. 太平洋数学杂志, 14(4):1359– 1366, 1964.[40] C´esar Polcino Milies 和 S.K. Sehgal. 《群环导论》. 代数与应用. 施普林格, 2002.[41] Alexander S Mishchenko. 群代数的外导子的描述. Topology and its Applications, 275:107013, 2020.[42] Ashraf Mohammad、Ali Shakir 和 Haetinger Claus. 关于环中的导子及其应用. 阿里格尔数学通报, 25(2):79–107, 2006.[43] G Muhiuddin 和 Abdullah M Al-Roqi. BCI-代数中的 (α, β)-导子. 自然与社会中的离散动力学, 2012:11, 2012.[44] AS.CI Mustafa 和 S.ahin Ceran. 格的广义 (f, g)-导子. 数学科学与应用电子札记, 1(2):56–62, 2013.[45] Richard S Pierce 和 Richard S Pierce. 结合代数. 施普林格 , 1982.[46] Balchand Prajapati 、 Shailesh Kumar Tiwari 和 Charu Gupta. b-广义导子在素环上充当乘子. 《代数通讯》, 50(8):3498–3515, 2022.[47] Mohd Arif Raza 和 Nadeem Ur Rehman. 关于具有广义导子和非交换巴拿赫代数的素环与半素环. 数学科学学报, 126(3):389–398, 2016.[48] Lionel Richard 和 Sergei D Silvestrov. σ-导子在 $\mathbb{C}[t^{\pm 1}]$上的拟李结构. 《代数杂志》, 319(3):1285–1304, 2008.

[49] Shˆoichirˆo Sakai. 群代数的导子。《数学年刊》，第 273–279 页，1966 年。[50] Thomas Siebert. 特征为 0 的域上的导子李代数与仿射代数几何。《数学年刊》，305(2):271–286，1996 年。[51] Martha K Smith. 有限生成无挠幂零群的群代数的导子。《休斯敦数学杂志》，4(2):277–288，1978 年。[52]Eugene Spiegel. 整数群环的导子。《代数通讯》，22(8):2955–2959，1994 年。[53] Morris Weisfeld. 除环中的导子。《太平洋数学杂志》，10(4):335–343，1960 年。