

Advances in Group Theory and Applications
© 2025 AGTA - www.advgrouptheory.com/journal
21 (2025), pp. 125–154 ISSN: 2499-1287
DOI: 10.32037/agta-2025-007

Inner and Outer Derivations of $\mathbb{F}V_{8n}$

P. Manju — R.K. Sharma

(*Received Jul. 21, 2023; Accepted Mar. 11, 2024 — Communicated by E. Jespers*)

Abstract

Let $\mathbb{F}$ be a field of characteristic 0 or an odd rational prime p. In this article, we give an explicit classification of all the inner and outer derivations of the group algebra $\mathbb{F}V_{8n}$, where V_{8n} is a group of order $8n$ (n a positive integer) with presentation

$$\langle a, b \mid a^{2n} = b^4 = 1, ba = a^{-1}b^{-1}, b^{-1}a = a^{-1}b\rangle.$$

First, we explicitly classify all the $\mathbb{F}$-derivations of $\mathbb{F}V_{8n}$ by giving the dimension and a basis of the derivation algebra consisting of all $\mathbb{F}$-derivations of $\mathbb{F}V_{8n}$. Consequently, we classify all inner and outer derivations of $\mathbb{F}V_{8n}$ when $\mathbb{F}$ is an algebraic extension of a prime field. Thus, we establish that all the derivations of $\mathbb{F}V_{8n}$ are inner when the characteristic of $\mathbb{F}$ is 0 or p with p relatively prime to n, and that non-zero outer derivations exist only in the case when the characteristic of $\mathbb{F}$ is p with p dividing n.

Mathematics Subject Classification (2020): 16S34, 16W25, 20C05

Keywords: derivation; $\mathbb{F}$-derivation; group ring; group algebra; inner derivation; outer derivation

1 Introduction

Let R be a ring. A derivation d of R is a map $d : R \to R$ satisfying

$$d(a + b) = d(a) + d(b) \quad \text{and} \quad d(ab) = d(a)b + ad(b)$$

for all $a, b \in R$. The map $d_b : R \to R$ ($b \in R$) defined by

$$d_b(a) = ab - ba$$

for all $a \in R$, is a derivation of R. A derivation d of R is called inner if $d = d_b$ for some $b \in R$, and outer if it is not inner. If S is a subring of R, then a derivation d of R is called an S-derivation if $d(s) = 0$ for all $s \in S$. We denote the set of all derivations of R by $\mathrm{Der}(R)$, the set of all inner derivations of R by $\mathrm{Der}_{\mathrm{Inn}}(R)$, and the set of all S-derivations of R by $\mathrm{Der}_S(R)$. If R has unity 1, then $d(1) = 0$. If R is commutative, then $\mathrm{Der}(R)$ becomes an R-module concerning the componentwise sum and module action, and $\mathrm{Der}_{\mathrm{Inn}}(R)$ and $\mathrm{Der}_S(R)$ become its submodules. If G is a group, then the group ring RG of G over R is defined as the set of all formal linear combinations of the form $\alpha = \sum_{g \in G} a_g g$ with finite support, where the support of α is defined to be the set $\mathrm{supp}(\alpha) = \{g \in G \mid a_g \neq 0\}$. RG is a ring concerning the componentwise addition and multiplication defined by $\alpha\beta = \sum_{g,h \in G} a_g b_h gh$ for $\alpha = \sum_{g \in G} a_g g$, $\beta = \sum_{g \in G} b_g g$ in RG. If R is commutative with unity and G is abelian, then RG becomes a commutative unital algebra over R. If R is commutative, then $\mathrm{Der}(RG)$ is both an RG- as well as R-module concerning the componentwise sum and module action, and $\mathrm{Der}_{\mathrm{Inn}}(RG)$ and $\mathrm{Der}_S(RG)$ are its submodules. Derivations play an essential role in many important branches of mathematics and physics. Understanding the structures of rings and algebras has involved extensive study of derivations. The notion of derivation in rings has been applied to various algebras, for example, BCI-algebras [20], von Neumann algebras [9], incline algebras [17], MV-algebras [16, 21], Banach algebras [22], and lattices which play an important role in information theory and recovery, management of information access, and cryptanalysis [10]. Differentiable manifolds, operator algebras, $\mathbb{C}^*$-algebras, and representation theory of Lie groups are studied using derivations [18]. Coding theory also makes use of derivations. For example, in [14], codes have been built as modules over skew polynomial rings, where a derivation and an automorphism define multiplication. In [13], authors have studied codes as images of derivations on group algebras. For more applications of derivations, we refer the reader to [8].

More research is expected on the derivations of group rings. In the literature, one can find only a few articles that concern derivations of group rings. The serious study of derivations of group rings begins with Smith's 1978 paper [25], in which the author studies

derivations of a finitely generated torsion-free nilpotent group over a field. For instance, it is shown that such group rings always contain an outer derivation. The second major work in this direction can be seen in [26] and [15]. In [26], it is shown that every derivation of an integral group ring is inner, and in [15], it is shown that every R-derivation of the group ring RG is inner if R is a semiprime ring with $\mathrm{char}(R)$, either 0 or does not divide the order of any element of G, where G is a torsion group with its center $Z(G)$ having finite index in it. Further evidence of the research in this direction is found only in 2019 in the works of Dishari Chaudhuri and Leo Creedon et al. Dishari Chaudhari, in her papers, [11] and [12], generalizes the above results of [26] and [15] respectively to (σ,τ)-derivations of group rings of finite groups over a field and an integral domain where σ,τ satisfy certain conditions. In recent years, more tools have been used to study derivations of group rings. For instance, A.A. Arutyunov uses topological and character theory techniques to study derivations of group algebras [1, 2, 6, 7, 4, 5, 3]. In [13], the authors study derivations of group rings in terms of the generators and relators of a group and, further, as applications, classify derivations of commutative group algebras over fields of positive characteristic and that of dihedral group algebras over a characteristic 2 field. In [19], the authors explicitly classify all inner derivations of a group algebra $\mathbb{F}G$ of a finite group G over an arbitrary field $\mathbb{F}$. This result generalizes Theorem 3.13 of [13] where the authors have classified all inner derivations of dihedral group algebras over fields of characteristic 2. In [19], the authors also classify all inner and outer derivations of dihedral, dicyclic, and semi-dihedral group algebras over fields of characteristic 0 or an odd rational prime p. The work in this article concerns the derivations of the non-commutative group algebra $\mathbb{F}V_{8n}$ of one of the essential non-abelian groups V_{8n} over a field $\mathbb{F}$. The group ring $\mathbb{F}V_{8n}$ is important concerning its applications in coding theory (for reference, see [24]). Recently, the applications of derivations in coding theory have been discovered. For instance, in [13], it has been found that some well-known codes occur as images of derivations. Thus, the derivations of the group ring $\mathbb{F}V_{8n}$ are interesting concerning their applications in coding theory; the explicit description of the derivation algebra of $\mathbb{F}V_{8n}$ can prove to be valuable in constructing some good group ring codes using different techniques.

We divide the article into three sections. Section 2 includes some preliminary results and definitions that we need to prove our main results in Section 3. The results already proved in the literature are

just stated (with reference) without proof, and the new results are stated with proof. In Section 3, we study the derivations of the group algebra $\mathbb{F}V_{8n}$, where

$$V_{8n} = \langle a, b \mid a^{2n} = b^4 = 1, ba = a^{-1}b^{-1}, b^{-1}a = a^{-1}b \rangle$$

is a group of order $8n$ (n a positive integer) and $\mathbb{F}$, unless otherwise stated, is a field of characteristic 0 or an odd rational prime p. We classify all the $\mathbb{F}$-derivations of $\mathbb{F}V_{8n}$ by giving the dimension and a basis of the derivation algebra $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n})$ consisting of all $\mathbb{F}$-derivations of $\mathbb{F}V_{8n}$. Therefore, we classify all the derivations of $\mathbb{F}V_{8n}$ when $\mathbb{F}$ is an algebraic extension of a prime field. It is thus established that when $\mathbb{F}$ is an algebraic extension of a prime field, then all derivations of $\mathbb{F}V_{8n}$ are inner provided $\mathrm{char}(\mathbb{F})$ is either 0 or an odd prime p with $\gcd(n, p) = 1$ and non-zero outer derivations of $\mathbb{F}V_{8n}$ exist only when $\mathrm{char}(\mathbb{F}) = p$ with $\gcd(n, p) \neq 1$. Here $\mathrm{char}(\mathbb{F})$ denotes the characteristic of field $\mathbb{F}$ and $\gcd(n, p)$ denotes the greatest common divisor of n and p.

2 Preliminary Results

Let R be a commutative unital ring and $G = \langle X \mid Y \rangle$ be a group with X as its set of generators and Y as the set of relators. In [13], the authors have studied the derivations of the group ring RG in terms of the generators and relators of the group G. They have given a necessary and sufficient condition under which a map $f : X \to RG$ can be extended to a derivation of RG.

Theorem 1 (see [13], Theorem 2.5) *Let $G = \langle X \mid Y \rangle$ be a group with X as its set of generators and Y the set of relators. Let F_X denote the free group on X and $\phi : F_X \to G$ the natural onto homomorphism. Let R be a commutative ring with unity and $f : X \to RG$ be a map. Then*

(i) *f can be uniquely extended to a map $\widetilde{f} : F_X \to RG$ satisfying*

$$\widetilde{f}(vw) = \widetilde{f}(v)\phi(w) + \phi(v)\widetilde{f}(w), \ \forall \ v, w \in F_X. \tag{2.1}$$

(ii) *f can be uniquely extended to an R-derivation of RG if and only if $\widetilde{f}(y) = 0$ for all $y \in Y$.*

The map $\widetilde{f} : F_X \to RG$ is defined as

$$\widetilde{f}(x) = \begin{cases} f(x) & \text{if } x \in X \\ -xf(x^{-1})x & \text{if } x \in X^{-1} \\ 0 & \text{if } x = 1 \end{cases} \tag{2.2}$$

and then on the whole of F_X as

$$\widetilde{f}(v) = \sum_{i=1}^{k} \left(\prod_{j=1}^{i-1} x_j \right) \widetilde{f}(x_i) \left(\prod_{j=i+1}^{k} x_j \right), \tag{2.3}$$

if $v = \prod_{i=1}^{k} x_i$. Any derivation d of a group algebra RG is uniquely determined by the image set $\{d(x) \mid x \in X\}$. If the generating set X is finite, say, $X = \{x_1, \ldots, x_t\}$, then we denote such a derivation by $d_{(\overline{x_1}, \ldots, \overline{x_t})}$, where $\overline{x_i} = d(x_i)$ $(1 \leqslant i \leqslant t)$. The following theorem guarantees that for a K-algebra $\mathcal{A}$ where K is an algebraic extension of a prime field $\mathbb{F}$, $\mathrm{Der}(\mathcal{A}) = \mathrm{Der}_K(\mathcal{A})$:

Theorem 2 (see [13], Theorem 2.2) *Let $\mathcal{A}$ be a K-algebra where K is an algebraic extension of a prime field $\mathbb{F}$ and let $d \in \mathrm{Der}(\mathcal{A})$. Then $d(K) = \{0\}$ and d is a K-linear map.*

In [19], the authors have given an explicit classification of all the inner derivations of a group algebra $\mathbb{F}G$ of a finite group G over a field $\mathbb{F}$ of arbitrary characteristic.

Theorem 3 (see [19], Theorem 2.15) *Let $\mathbb{F}$ be a field of any characteristic and G be a finite group of order n having r conjugacy classes. Then the dimension of $\mathrm{Der}_{\mathrm{Inn}}(\mathbb{F}G)$ over $\mathbb{F}$ is $n - r$. Moreover, if $C_1, \ldots, C_r$ are the all distinct conjugacy classes of G with representatives $x_1, \ldots, x_r$ respectively and s is a positive integer such that $|C_i| = 1$ for all $i \in \{1, \ldots, s\}$ and $|C_i| \geqslant 2$ for all $i \in \{s+1, \ldots, r\}$, then the set*

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

forms a basis of $\mathrm{Der}_{\mathrm{Inn}}(\mathbb{F}G)$ over $\mathbb{F}$.

For a commutative unital ring R and a group G, the homomor-

phism $\varepsilon : RG \to R$ defined by

$$\varepsilon\Big(\sum_{g\in G} \lambda_g g\Big) = \sum_{g\in G} \lambda_g$$

is called the augmentation mapping of RG, and its kernel

$$\Delta(G) = \Big\{\sum_{g\in G} \lambda_g g \in RG \mid \sum_{g\in G} \lambda_g = 0\Big\}$$

is called the augmentation ideal of RG. We require the following generalized notion:

Definition 4 For a subgroup H of G, define

$$\Delta'(H) = \Big\{\sum_{g\in G} \lambda_g g \in RG \mid \sum_{g\in H} \lambda_g = 0 \quad \text{and} \quad \sum_{g\in G\setminus H} \lambda_g = 0\Big\}.$$

Notice that $\Delta'(H)$ is an R-submodule of the R-module RG and $\Delta'(G) = \Delta(G)$.

For an element $\beta \in RG$, the subalgebra

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

of RG is called the *centralizer* of β in RG.

Definition 5 We call the set

$$\overline{C}(\beta) = \big\{\alpha \in \mathbb{F}G \mid \alpha\beta = -\beta\alpha\big\}$$

as the *anti-centralizer* of β in RG. It is an R-submodule of the R-module RG.

The proof of the following lemma can be found in [23] (see Proposition 2.4).

Lemma 6 (i) *If n is even, then V_{8n} has $2n+6$ conjugacy classes given by*

$$\{1\},\ \{a^n\},\ \{b^2\},\ \{a^n b^2\},\ \{a^{2k}, a^{-2k}\} \text{ for } 1 \leqslant k \leqslant \frac{n}{2} - 1,$$
$$\{a^{2k-1}, a^{-2k+1}b^2\} \text{ for } 1 \leqslant k \leqslant n,$$
$$\{a^{2k}b^2, a^{-2k}b^2\} \text{ for } 1 \leqslant k \leqslant \frac{n}{2} - 1,$$

$$
\begin{aligned}
b^{V_{8n}} &= \{a^{4k}b, a^{4k+2}b^{-1} \mid 1 \leqslant k \leqslant n/2\},\\
(ab)^{V_{8n}} &= \{a^{4k+1}b, a^{4k+3}b^{-1} \mid 1 \leqslant k \leqslant n/2\},\\
(b^3)^{V_{8n}} &= \{a^{4k+2}b, a^{4k}b^{-1} \mid 1 \leqslant k \leqslant n/2\},\\
(ab^3)^{V_{8n}} &= \{a^{4k+3}b, a^{4k+1}b^{-1} \mid 1 \leqslant k \leqslant n/2\}.
\end{aligned}
$$

(ii) *If* n *is odd, then* V_{8n} *has* $2n+3$ *conjugacy classes given by*

$$
\begin{aligned}
&\{1\}, \quad \{b^2\}, \quad \{a^{2k}, a^{-2k}\} \textit{ for } 1 \leqslant k \leqslant \frac{n-1}{2},\\
&\{a^{2k-1}, a^{-2k+1}b^2\} \textit{ for } 1 \leqslant k \leqslant n,\\
&\{a^{2k}b^2, a^{-2k}b^2\} \textit{ for } 1 \leqslant k \leqslant \frac{n-1}{2},\\
&b^{V_{8n}} = \{a^{2k}b, a^{2k}b^{-1} \mid 1 \leqslant k \leqslant n\},\\
&(ab)^{V_{8n}} = \{a^{2k+1}b, a^{2k+1}b^{-1} \mid 1 \leqslant k \leqslant n\}.
\end{aligned}
$$

The following lemma is used in the proof of Lemma 8.

Lemma 7 *Let* $\mathbb{F}$ *be a field with* $\mathrm{char}(\mathbb{F}) \neq 2$, G *be a finite group, and* $g \in G$ *be an element of order* n. *If* n *is even, then* $\overline{C}(g^{-1}) = \overline{C}(g)$. *Conversely, if* $\overline{C}(g) \neq \{0\}$ *and* $\overline{C}(g^{-1}) = \overline{C}(g)$, *then* n *is even.*

Proof — First, let n be even and $\alpha \in \overline{C}(g)$. Then $\alpha g = -g\alpha$. By induction, $\alpha g^k = (-1)^k g^k \alpha$ for all $k \in \mathbb{N}$. So

$$\alpha g^{-1} = \alpha g^{n-1} = (-1)^{n-1} g^{n-1} \alpha = -g^{-1}\alpha.$$

Therefore, $\alpha \in \overline{C}(g^{-1})$. Conversely, let $\alpha \in \overline{C}(g^{-1})$. Now replacing the role of g by that of g^{-1} above (as $|g| = n = |g^{-1}|$), we get that $\alpha \in \overline{C}(g)$.

For the converse of the lemma, let $\overline{C}(g) \neq \{0\}$ and $\overline{C}(g) = \overline{C}(g^{-1})$. Then, some non-zero $\alpha \in \overline{C}(g)$ exists. Since $\alpha g = -g\alpha$, as seen above,

$$\alpha g^{-1} = (-1)^{n-1} g^{-1} \alpha.$$

But again, since $\alpha \in \overline{C}(g^{-1})$, so $\alpha g^{-1} = -g^{-1}\alpha$. So we get that

$$(-1)^{n-1} g^{-1} \alpha = -g^{-1}\alpha.$$

Pre-multiplying both sides by g, we have $(-1)^{n-1}\alpha = -\alpha$. This gives that $(-1)^{n-1} = -1$ because $\{\alpha\}$ is an $\mathbb{F}$-linearly independent subset

of $\mathbb{F}G$. Therefore, n is even. □

The following lemma is crucial in proving our main Theorem 9.

Lemma 8 *Let $\mathbb{F}$ be a field of characteristic 0 or p, where p is an odd rational prime. Then, the following statements hold:*

(i) *The set*

$$\begin{aligned}\overline{\mathcal{B}}(b) = &\left\{(a^{2k} - a^{-2k})b^j \mid 1 \leqslant k \leqslant \left\lfloor \frac{n-1}{2} \right\rfloor, 0 \leqslant j \leqslant 3\right\} \\ &\cup \left\{(a^{2k-1} - a^{-(2k-1)}b^2),\ (a^{2k-1} - a^{-(2k-1)}b^2)b \right. \\ &\left. \mid 1 \leqslant k \leqslant \left\lfloor \frac{n+1}{2} \right\rfloor\right\} \bigcup \left\{(a^{-(2k-1)} - a^{2k-1}b^2),\right. \\ &\left.(a^{-(2k-1)} - a^{2k-1}b^2)b \mid 1 \leqslant k \leqslant \left\lceil \frac{n-1}{2} \right\rceil\right\}\end{aligned}$$

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

(ii) $\overline{C}(b^{-1}) = \overline{C}(b)$.

(iii) *The set*

$$\begin{aligned}\overline{\mathcal{B}}(a^{-1}b) = &\left\{(a^{2k} - a^{-2k})b^2, (a^{2k-1} - a^{-(2k+1)})b,\right. \\ &\left.(a^{2k} - a^{-2k}), (a^{2k-1} - a^{-(2k+1)})b^3 \mid 1 \leqslant k \leqslant \left\lfloor \frac{n-1}{2} \right\rfloor\right\} \\ &\bigcup \left\{(a^{2k-1} - a^{-(2k-1)}b^2),\ (a^{2k-2} - a^{-2k}b^2)b \mid 1 \leqslant k \leqslant n\right\}\end{aligned}$$

is a basis of $\overline{C}(a^{-1}b)$ over $\mathbb{F}$.

(iv) $\overline{C}(ba) = \overline{C}(b^{-1}a)$.

Proof — (i) It can be easily verified that $\overline{\mathcal{B}}(b)$ is an $\mathbb{F}$-linearly independent subset of $\mathbb{F}V_{8n}$. Now let $\alpha \in \overline{C}(b)$ and $\alpha = \sum_{i,j} \lambda_{i,j} a^i b^j$ for some $\lambda_{i,j} \in \mathbb{F}$ ($0 \leqslant i \leqslant 2n-1$, $0 \leqslant j \leqslant 3$). Put $\lambda_{(2n),j} = \lambda_{0,j}$ for $j \in \{0,1,2,3\}$. Then from $\alpha b = -b\alpha$, we will get that

$$\lambda_{i,0} = \begin{cases} -\lambda_{(2n-i),2} & \text{if } i \text{ is odd} \\ -\lambda_{(2n-i),0} & \text{if } i \text{ is even} \end{cases}, \quad \lambda_{i,1} = \begin{cases} -\lambda_{(2n-i),3} & \text{if } i \text{ is odd} \\ -\lambda_{(2n-i),1} & \text{if } i \text{ is even} \end{cases},$$

$$\lambda_{i,2} = \begin{cases} -\lambda_{(2n-i),0} & \text{if } i \text{ is odd} \\ -\lambda_{(2n-i),2} & \text{if } i \text{ is even} \end{cases}, \quad \lambda_{i,3} = \begin{cases} -\lambda_{(2n-i),1} & \text{if } i \text{ is odd} \\ -\lambda_{(2n-i),3} & \text{if } i \text{ is even} \end{cases}.$$

Using this information, we can calculate in a finite number of steps that when n is even and n is odd, α is given respectively by

$$\begin{aligned}\alpha = &\sum_{k=1}^{\frac{n}{2}} \lambda_{(2k-1),0}(a^{2k-1} - a^{-(2k-1)}b^2) \\ &+ \sum_{k=1}^{\frac{n}{2}} \lambda_{(2n-(2k-1)),0}(a^{-(2k-1)} - a^{2k-1}b^2) \\ &+ \sum_{k=1}^{\frac{n}{2}} \lambda_{(2k-1),1}(a^{2k-1} - a^{-(2k-1)}b^2)b \\ &+ \sum_{k=1}^{\frac{n}{2}} \lambda_{(2n-(2k-1)),1}(a^{-(2k-1)} - a^{2k-1}b^2)b \\ &+ \sum_{k=1}^{\frac{n}{2}-1} \lambda_{(2k),0}(a^{2k} - a^{-2k}) + \sum_{k=1}^{\frac{n}{2}-1} \lambda_{(2k),1}(a^{2k} - a^{-2k})b \\ &+ \sum_{k=1}^{\frac{n}{2}-1} \lambda_{(2k),2}(a^{2k} - a^{-2k})b^2 + \sum_{k=1}^{\frac{n}{2}-1} \lambda_{(2k),3}(a^{2k} - a^{-2k})b^3,\end{aligned}$$

and

$$\begin{aligned}\alpha = &\sum_{k=1}^{\frac{n+1}{2}} \lambda_{(2k-1),0}\left(a^{2k-1} - a^{-(2k-1)}b^2\right) \\ &+ \sum_{k=1}^{\frac{n-1}{2}} \lambda_{(2n-(2k-1)),0}\left(a^{-(2k-1)} - a^{2k-1}b^2\right) \\ &+ \sum_{k=1}^{\frac{n+1}{2}} \lambda_{(2k-1),1}\left(a^{2k-1} - a^{-(2k-1)}b^2\right)b \\ &+ \sum_{k=1}^{\frac{n-1}{2}} \lambda_{(2n-(2k-1)),1}\left(a^{-(2k-1)} - a^{2k-1}b^2\right)b \\ &+ \sum_{k=1}^{\frac{n-1}{2}} \lambda_{(2k),0}(a^{2k} - a^{-2k}) + \sum_{k=1}^{\frac{n-1}{2}} \lambda_{(2k),1}(a^{2k} - a^{-2k})b\end{aligned}$$

$$+\sum_{k=1}^{\frac{n-1}{2}}\lambda_{(2k),2}(a^{2k}-a^{-2k})b^2+\sum_{k=1}^{\frac{n-1}{2}}\lambda_{(2k),3}(a^{2k}-a^{-2k})b^3.$$

So in both cases, $\alpha\in\overline{C}(b)$ can be written as an $\mathbb{F}$-linear combination of the elements in $\overline{\mathcal{B}}(b)$. Therefore, $\overline{\mathcal{B}}(b)$ is a basis of $\overline{C}(b)$ over $\mathbb{F}$.

(ii) The order of b is 4 which is even. Thus, by Lemma 7, $\overline{C}(b^{-1})=\overline{C}(b)$.

(iii) Let $\alpha\in\overline{C}(a^{-1}b)$, so $\alpha=\sum_{i,j}\lambda_{i,j}a^ib^j$ for some $\lambda_{i,j}\in\mathbb{F}$ $(0\leqslant i\leqslant 2n-1,\ 0\leqslant j\leqslant 3)$. From $\alpha(a^{-1}b)=-(a^{-1}b)\alpha$, we will get

$$\sum_{i=0}^{2n-1}\lambda_{i,1}a^{i+1}=-\sum_{\substack{0\leqslant i\leqslant 2n-1\\ i\text{ odd}}}\lambda_{i,1}a^{-(i+1)}-\sum_{\substack{0\leqslant i\leqslant 2n-1\\ i\text{ even}}}\lambda_{i,3}a^{-(i+1)},$$

$$\sum_{i=0}^{2n-1}\lambda_{i,0}a^{i-1}b=-\sum_{\substack{0\leqslant i\leqslant 2n-1\\ i\text{ even}}}\lambda_{i,0}a^{-(i+1)}b-\sum_{\substack{0\leqslant i\leqslant 2n-1\\ i\text{ odd}}}\lambda_{i,2}a^{-(i+1)}b,$$

$$\sum_{i=0}^{2n-1}\lambda_{i,3}a^{i+1}b^2=-\sum_{\substack{0\leqslant i\leqslant 2n-1\\ i\text{ even}}}\lambda_{i,1}a^{-(i+1)}b^2-\sum_{\substack{0\leqslant i\leqslant 2n-1\\ i\text{ odd}}}\lambda_{i,3}a^{-(i+1)}b^2,$$

$$\sum_{i=0}^{2n-1}\lambda_{i,2}a^{i-1}b^3=-\sum_{\substack{0\leqslant i\leqslant 2n-1\\ i\text{ odd}}}\lambda_{i,0}a^{-(i+1)}b^3-\sum_{\substack{0\leqslant i\leqslant 2n-1\\ i\text{ even}}}\lambda_{i,2}a^{-(i+1)}b^3.$$

From the first equation, we get the following:

- for each i with $1\leqslant i\leqslant 2n-1$ and i odd, $\lambda_{(i-1),1}=-\lambda_{(2n-i-1),3}$;
- for each i with $2\leqslant i\leqslant 2n-2$, $i\neq n$ and i even,

$$\lambda_{(i-1),1}=-\lambda_{(2n-i-1),1};$$

- $\lambda_{(n-1),1}=0$ if n is even and $\lambda_{(2n-1),1}=0$.

Similarly, from the third equation, we will get that:

- for each i with $1\leqslant i\leqslant 2n-1$ and i odd, $\lambda_{(i-1),3}=-\lambda_{(2n-i-1),1}$;
- for each i with $2\leqslant i\leqslant 2n-2$, $i\neq n$ and i even,

$$\lambda_{(i-1),3}=-\lambda_{(2n-i-1),3};$$

- $\lambda_{(n-1),3} = 0$ if n is even and $\lambda_{(2n-1),3} = 0$.

From the second equation, we get the following:

- for each i with $1 \leqslant i \leqslant 2n-1$ and i odd, $\lambda_{i,0} = -\lambda_{(2n-i),2}$;
- for each i with $2 \leqslant i \leqslant 2n-2$, $i \neq n$ and i even, $\lambda_{i,0} = -\lambda_{(2n-i),0}$;
- $\lambda_{n,0} = 0$ if n is even and $\lambda_{0,0} = 0$.

Similarly, from the fourth equation, we will have

- for each i with $1 \leqslant i \leqslant 2n-1$ and i odd, $\lambda_{i,2} = -\lambda_{(2n-i),0}$;
- for each i with $2 \leqslant i \leqslant 2n-2$, $i \neq n$ and i even, $\lambda_{i,2} = -\lambda_{(2n-i),2}$;
- $\lambda_{n,2} = 0$ if n is even and $\lambda_{0,2} = 0$.

Now, using the above information, we can use a finite number of calculations to determine that

$$\begin{aligned}\alpha = &\sum_{\substack{1\leqslant i\leqslant 2n-1\\ i \text{ odd}}} \lambda_{i,0}(a^i - a^{-i}b^2) + \sum_{\substack{2\leqslant i\leqslant n-1\\ i \text{ even}}} \lambda_{i,0}(a^i - a^{-i}) \\ &+ \sum_{\substack{1\leqslant i\leqslant 2n-1\\ i \text{ odd}}} \lambda_{(i-1),1}(a^{i-1} - a^{2n-i-1}b^2)b \\ &+ \sum_{\substack{2\leqslant i\leqslant n-1\\ i \text{ even}}} \lambda_{(i-1),1}(a^{i-1} - a^{2n-i-1})b + \sum_{\substack{2\leqslant i\leqslant n-1\\ i \text{ even}}} \lambda_{i,2}(a^i - a^{-i})b^2 \\ &+ \sum_{\substack{2\leqslant i\leqslant n-1\\ i \text{ even}}} \lambda_{(i-1),3}(a^{i-1} - a^{2n-i-1})b^3.\end{aligned}$$

Therefore, the set $\overline{\mathcal{B}}(a^{-1}b)$ spans $\overline{C}(a^{-1}b)$ over $\mathbb{F}$. Also, $\overline{\mathcal{B}}(a^{-1}b)$ is an $\mathbb{F}$-linearly independent subset of $\overline{C}(a^{-1}b)$. Therefore, $\overline{\mathcal{B}}(a^{-1}b)$ is a basis of $\overline{C}(a^{-1}b)$ over $\mathbb{F}$.

(iv) Let $\alpha \in \overline{C}(ba)$. Then $\alpha(ba) = -(ba)\alpha$. So

$$\alpha(b^{-1}a) = b^2\alpha(ba) = b^2(-(ba)\alpha) = -(b^{-1}a)\alpha$$

(as $b^2 \in Z(V_{8n})$). Thus, $\alpha \in \overline{C}(b^{-1}a)$. Conversely, let $\alpha \in \overline{C}(b^{-1}a)$. Then $\alpha(b^{-1}a) = -(b^{-1}a)\alpha$. So

$$\alpha(ba) = b^2\alpha(b^{-1}a) = b^2(-(b^{-1}a)\alpha) = -(ba)\alpha.$$

Therefore, $\alpha \in \overline{C}(ba)$. □

3 Main Results

The group V_{8n} has the presentation:

$$V_{8n} = \langle a, b \mid a^{2n} = b^4 = 1, ba = a^{-1}b^{-1}, b^{-1}a = a^{-1}b \rangle.$$

So $V_{8n} = \{a^i b^j \mid 0 \leqslant i \leqslant 2n-1, 0 \leqslant j \leqslant 3\}$. In this section, we classify all the derivations, inner as well as outer, of the group algebra $\mathbb{F}V_{8n}$ over a field $\mathbb{F}$ of characteristic 0 or an odd rational prime p.

Theorem 9 *Let $\mathbb{F}$ be a field and p be an odd rational prime.*

(i) *If either* $\mathrm{char}(\mathbb{F}) = 0$, *or* $\mathrm{char}(\mathbb{F}) = p$ *with* $\gcd(n, p) = 1$, *then the dimension of* $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n})$ *over* $\mathbb{F}$ *is* $3(2n-1)$ *if* n *is odd and* $6(n-1)$ *if* n *is even, and a basis is*

$$\mathcal{B} = \left\{ d_{(\bar{a},\bar{b})} \mid (\bar{a},\bar{b}) \in B_1 \cup B_2 \cup B_3 \cup B_4 \right\},$$

where

$$\begin{aligned} B_1 = \Big\{ & \big((a^{-2k} - a^{2k})b, 0\big), \ \big((a^{2k-1} - a^{-(2k+1)})b, (a^{2k} - a^{-2k})\big), \\ & \big((a^{-2k} - a^{2k})b^3, 0\big), \ \big((a^{2k-1} - a^{-(2k+1)})b^3, (a^{2k} - a^{-2k})b^2\big), \\ & \big(0, (a^{2k} - a^{-2k})b\big), \ \big(0, (a^{2k} - a^{-2k})b^3\big) \mid 1 \leqslant k \leqslant \left\lfloor \frac{n-1}{2} \right\rfloor \Big\}, \end{aligned}$$

$$\begin{aligned} B_2 = \Big\{ & \big((a^{2k-2} - a^{-2k}b^2)b, (a^{2k-1} - a^{-(2k-1)}b^2)\big), \\ & \big(0, (a^{-(2k-1)} - a^{2k-1}b^2)b\big) \mid 1 \leqslant k \leqslant \left\lfloor \frac{n+1}{2} \right\rfloor \Big\}, \end{aligned}$$

$$\begin{aligned} B_3 = \Big\{ & \big((a^{-2k} - a^{2k-2}b^2)b, (a^{-(2k-1)} - a^{2k-1}b^2)\big), \\ & \big(0, (a^{-(2k-1)} - a^{2k-1}b^2)b\big) \mid 1 \leqslant k \leqslant \left\lceil \frac{n-1}{2} \right\rceil \Big\}, \end{aligned}$$

$$B_4 = \Big\{ \big((a^{-(2k-1)} - a^{2k-1}b^2)b, 0\big) \mid 1 \leqslant k \leqslant n \Big\}.$$

(ii) *If* $\mathrm{char}(\mathbb{F}) = p$, *with* $\gcd(n, p) \neq 1$, *then the dimension of* $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n})$ *over* $\mathbb{F}$ *is* $4(2n-1)$ *if* n *is odd and* $8(n-1)$ *if* n *is even and a basis is*

$$\mathcal{B}' = \{ d_{(\bar{a},\bar{b})} \mid (\bar{a},\bar{b}) \in B_1' \cup B_2' \cup B_3' \cup B_4' \},$$

where

$$\begin{aligned}
B_1' = \Big\{ & \big((a^{2k-1} - a^{-(2k+1)})b, (a^{2k} - a^{-2k})\big), \\
& \big((a^{2k+1} - a^{-(2k-1)}), (a^{2k} - a^{-2k})b\big), \\
& \big((a^{2k-1} - a^{-(2k+1)})b^3, (a^{2k} - a^{-2k})b^2\big), \\
& \big((a^{2k+1} - a^{-(2k-1)})b^2, (a^{2k} - a^{-2k})b^3\big), \ \big((a^{-2k} - a^{2k})b^3, 0\big), \\
& \big((a^{-2k} - a^{2k})b, 0\big), \ \big((a^{-(2k-1)} - a^{2k+1})b^2, 0\big), \\
& \big((a^{-(2k-1)} - a^{2k+1}), 0\big) \mid 1 \leqslant k \leqslant \left\lfloor \frac{n-1}{2} \right\rfloor \Big\},
\end{aligned}$$

$$\begin{aligned}
B_2' = \Big\{ & \big((a^{2k-2} - a^{-2k}b)b^2, (a^{2k-1} - a^{-(2k-1)}b^2)\big), \\
& \big((a^{2k} - a^{-(2k-2)}b^2), (a^{2k-1} - a^{-(2k-1)}b^2)b\big) \mid 1 \leqslant k \leqslant \left\lfloor \frac{n+1}{2} \right\rfloor \Big\},
\end{aligned}$$

$$\begin{aligned}
B_3' = \Big\{ & \big((a^{-2k} - a^{2k-2}b^2)b, (a^{-(2k-1)} - a^{2k-1}b^2)\big), \\
& \big((a^{-(2k-2)} - a^{2k}b^2), (a^{-(2k-1)} - a^{2k-1}b^2)b\big) \mid 1 \leqslant k \leqslant \left\lceil \frac{n-1}{2} \right\rceil \Big\},
\end{aligned}$$

$$\begin{aligned}
B_4' = \Big\{ & \big((a^{-(2k-1)} - a^{2k-1}b^2)b, 0\big), \big((a^{-(2k-2)} - a^{2k}b^2), 0\big) \\
& \qquad \mid 1 \leqslant k \leqslant n \Big\}.
\end{aligned}$$

Proof — The relators of the group V_{8n} are a^{2n}, b^4, $(ba)^2$, $(b^{-1}a)^2$. Let

$$f : X = \{a, b\} \to \mathbb{F}V_{8n}$$

be a map that can be extended to an $\mathbb{F}$-derivation of $\mathbb{F}V_{8n}$. By Theorem 1, this is possible if and only if $\widetilde{f}(a^{2n}) = 0$, $\widetilde{f}(b^4) = 0$, $\widetilde{f}((ba)^2) = 0$, and $\widetilde{f}((b^{-1}a)^2) = 0$. Write $f(a)$ as $f(a) = c_0 + c_1 b + c_2 b^2 + c_3 b^3$ for some $c_i \in \mathbb{F}\langle a \rangle$ $(0 \leqslant i \leqslant 3)$. Then, using (2.3), we get

$$\begin{aligned}
\widetilde{f}(a^{2n}) = {} & 2n a^{2n-1}(c_0 + c_2 b^2) + \sum_{\substack{1 \leqslant i \leqslant 2n \\ i \text{ odd}}} a^{2i-1} c_1 b^3 + \sum_{\substack{1 \leqslant i \leqslant 2n \\ i \text{ even}}} a^{2i-1} c_3 b^3 \\
& + \sum_{\substack{1 \leqslant i \leqslant 2n \\ i \text{ even}}} a^{2i-1} c_1 b + \sum_{\substack{1 \leqslant i \leqslant 2n \\ i \text{ odd}}} a^{2i-1} c_3 b.
\end{aligned}$$

Since $c_1, c_3 \in \mathbb{F}\langle a \rangle$, so $c_1 = \sum_{i=0}^{2n-1} \lambda_i a^i$ and $c_3 = \sum_{i=0}^{2n-1} \mu_i a^i$ for some $\lambda_i, \mu_i \in \mathbb{F}$ $(0 \leqslant i \leqslant 2n-1)$. Put $\lambda_{2n} = \lambda_0$ and $\mu_{2n} = \mu_0$.

Therefore, $\widetilde{f}(a^{2n}) = 0$ if and only if the following three equations hold:

$$2na^{2n-1}(c_0 + c_2b^2) = 0, \tag{3.1}$$

$$\sum_{\substack{1\leqslant i\leqslant 2n\\ i \text{ odd}}} a^{2i-1}\left(\sum_{j=0}^{2n-1}\lambda_j a^j\right)b^3 + \sum_{\substack{1\leqslant i\leqslant 2n\\ i \text{ even}}} a^{2i-1}\left(\sum_{j=0}^{2n-1}\mu_j a^j\right)b^3 = 0, \tag{3.2}$$

and

$$\sum_{\substack{1\leqslant i\leqslant 2n\\ i \text{ even}}} a^{2i-1}\left(\sum_{j=0}^{2n-1}\lambda_j a^j\right)b + \sum_{\substack{1\leqslant i\leqslant 2n\\ i \text{ odd}}} a^{2i-1}\left(\sum_{j=0}^{2n-1}\mu_j a^j\right)b = 0. \tag{3.3}$$

Now, there are two possibilities: (i) and (ii).

(i) $\mathrm{char}(\mathbb{F}) = 0$ or p with $\gcd(n,p) = 1$: Then, from (3.1), $c_0 = 0$ and $c_2 = 0$. Therefore, $f(a) = c_1b + c_3b^3$. Post multiplying (3.2) by ba and then comparing, we will get

$$\left(\sum_{\substack{0\leqslant j\leqslant 2n-1\\ j \text{ odd}}}\lambda_j a^j\right)\left(\sum_{\substack{1\leqslant i\leqslant 2n\\ i \text{ odd}}} a^{2i}\right) + \left(\sum_{\substack{0\leqslant j\leqslant 2n-1\\ j \text{ odd}}}\mu_j a^j\right)\left(\sum_{\substack{1\leqslant i\leqslant 2n\\ i \text{ even}}} a^{2i}\right) = 0 \tag{3.4}$$

and

$$\left(\sum_{\substack{0\leqslant j\leqslant 2n-1\\ j \text{ even}}}\lambda_j a^j\right)\left(\sum_{\substack{1\leqslant i\leqslant 2n\\ i \text{ odd}}} a^{2i}\right) + \left(\sum_{\substack{0\leqslant j\leqslant 2n-1\\ j \text{ even}}}\mu_j a^j\right)\left(\sum_{\substack{1\leqslant i\leqslant 2n\\ i \text{ even}}} a^{2i}\right) = 0. \tag{3.5}$$

We will get similar equations from (3.3) by just interchanging the roles of λ_i's and μ_i's. Again, we have two possible cases: n odd and n even.

Case 1: n is odd. Since

$$\sum_{\substack{1\leqslant i\leqslant 2n\\ i \text{ odd}}} a^{2i} = \sum_{\substack{1\leqslant i\leqslant 2n\\ i \text{ even}}} a^{2i} = \sum_{k=1}^{n} a^{2k}$$

and

$$\sum_{k=1}^{n} a^{2k+j} = \sum_{\substack{1\leqslant l\leqslant 2n\\ l \text{ odd}}} a^{l}$$

for each odd j in $\{0, 1, \ldots, 2n-1\}$, so by (3.4),

$$\left(\sum_{\substack{0\leqslant j\leqslant 2n-1\\ j \text{ odd}}} (\lambda_j + \mu_j)\right)\left(\sum_{\substack{1\leqslant l\leqslant 2n\\ l \text{ odd}}} a^l\right) = 0.$$

Therefore,

$$\sum_{\substack{0\leqslant j\leqslant 2n-1\\ j \text{ odd}}} (\lambda_j + \mu_j) = 0. \tag{3.6}$$

Further since

$$\sum_{k=1}^{n} a^{2k+j} = \sum_{\substack{1\leqslant l\leqslant 2n\\ l \text{ even}}} a^l$$

for each even j in $\{0, 1, \ldots, 2n-1\}$, so by (3.5),

$$\left(\sum_{\substack{0\leqslant j\leqslant 2n-1\\ j \text{ even}}} (\lambda_j + \mu_j)\right)\left(\sum_{\substack{1\leqslant l\leqslant 2n\\ l \text{ even}}} a^l\right) = 0.$$

Therefore,

$$\sum_{\substack{0\leqslant j\leqslant 2n-1\\ j \text{ even}}} (\lambda_j + \mu_j) = 0. \tag{3.7}$$

(3.6) and (3.7) together imply that $c_1 + c_3 \in \Delta'(\langle a^2\rangle)$. The same outcome is produced from (3.3).

Case 2: n is even.

$$\sum_{\substack{1\leqslant i\leqslant 2n\\ i \text{ odd}}} a^{2i} = 2\left(\sum_{\substack{1\leqslant i\leqslant n\\ i \text{ odd}}} a^{2i}\right)$$

and

$$\sum_{\substack{1\leqslant i\leqslant 2n\\ i \text{ even}}} a^{2i} = 2\left(\sum_{\substack{1\leqslant i\leqslant n\\ i \text{ even}}} a^{2i}\right).$$

Using this in (3.4), we can easily determine that

$$\left(\sum_{s=1}^{\frac{n}{2}} \lambda_{4s-3} + \sum_{t=1}^{\frac{n}{2}} \mu_{4t-1}\right)\left(\sum_{i=1}^{\frac{n}{2}} a^{4i-1}\right) + \\ + \left(\sum_{t=1}^{\frac{n}{2}} \lambda_{4t-1} + \sum_{s=1}^{\frac{n}{2}} \mu_{4s-3}\right)\left(\sum_{i=1}^{\frac{n}{2}} a^{4i-3}\right) = 0.$$

Therefore,

$$\sum_{s=1}^{\frac{n}{2}} \lambda_{4s-3} + \sum_{t=1}^{\frac{n}{2}} \mu_{4t-1} = 0 \tag{3.8}$$

and

$$\sum_{t=1}^{\frac{n}{2}} \lambda_{4t-1} + \sum_{s=1}^{\frac{n}{2}} \mu_{4s-3} = 0 \tag{3.9}$$

Similarly, from (3.5), we will get

$$\left(\sum_{s=1}^{\frac{n}{2}} \lambda_{4s-2} + \sum_{t=1}^{\frac{n}{2}} \mu_{4t}\right)\left(\sum_{i=1}^{\frac{n}{2}} a^{4i}\right) + \\ + \left(\sum_{s=1}^{\frac{n}{2}} \mu_{4s-2} + \sum_{t=1}^{\frac{n}{2}} \lambda_{4t}\right)\left(\sum_{i=1}^{\frac{n}{2}} a^{4i-2}\right) = 0.$$

Therefore,

$$\sum_{s=1}^{\frac{n}{2}} \lambda_{4s-2} + \sum_{t=1}^{\frac{n}{2}} \mu_{4t} = 0 \tag{3.10}$$

and

$$\sum_{t=1}^{\frac{n}{2}} \lambda_{4t} + \sum_{s=1}^{\frac{n}{2}} \mu_{4s-2} = 0 \tag{3.11}$$

We will get the same four equations when we work with (3.3).

Now by (2.1),

$$\widetilde{f}(b^4) = \widetilde{f}(b^2)\phi(b^2) + \phi(b^2)\widetilde{f}(b^2) = \widetilde{f}(b^2)b^2 + b^2\widetilde{f}(b^2) = 2b^2\widetilde{f}(b^2)$$

so that $\widetilde{f}(b^4) = 0 \Leftrightarrow \widetilde{f}(b^2) = 0$. Again,

$$\widetilde{f}(b^2) = \widetilde{f}(b)\phi(b) + \phi(b)\widetilde{f}(b) = f(b)b + bf(b)$$

so

$$\widetilde{f}(b^2) = 0 \Leftrightarrow f(b)b = -bf(b) \Leftrightarrow f(b) \in \overline{C}(b).$$

Therefore, $\widetilde{f}(b^4) = 0$ if and only if $f(b) \in \overline{C}(b)$. Further,

$$\widetilde{f}((ba)^2) = \widetilde{f}(ba)\phi(ba) + \phi(ba)\widetilde{f}(ba) = \widetilde{f}(ba)ba + ba\widetilde{f}(ba)$$

so that $\widetilde{f}((ba)^2) = 0 \Leftrightarrow \widetilde{f}(ba) \in \overline{C}(ba)$. Similarly,

$$\widetilde{f}((b^{-1}a)^2) = 0 \Leftrightarrow \widetilde{f}(b^{-1}a) \in \overline{C}(b^{-1}a).$$

Now,

$$\widetilde{f}(ba) = \widetilde{f}(b)\phi(a) + \phi(b)\widetilde{f}(a) = f(b)a + bf(a)$$

so that $f(a) = b^{-1}\widetilde{f}(ba) - b^{-1}f(b)a$. Also using (2.2) in addition to (2.1), we get

$$\widetilde{f}(b^{-1}a) = f(b^{-1})\phi(a) + \phi(b^{-1})f(a) = -b^{-1}f(b)b^{-1}a + b^{-1}f(a)$$

so that $f(a) = b\widetilde{f}(b^{-1}a) + f(b)b^{-1}a$. Therefore,

$$\begin{aligned} f(a) = b^{-1}\widetilde{f}(ba) - b^{-1}f(b)a &= b\widetilde{f}(b^{-1}a) + f(b)b^{-1}a \\ \Rightarrow b^{-1}\widetilde{f}(ba) - b\widetilde{f}(b^{-1}a) &= \left(f(b)b^{-1} + b^{-1}f(b)\right)a. \end{aligned}$$

Now since $f(b) \in \overline{C}(b)$ and by Lemma 8 (ii), $\overline{C}(b) = \overline{C}(b^{-1})$, therefore, $f(b) \in \overline{C}(b^{-1})$. This gives

$$f(b)b^{-1} + b^{-1}f(b) = 0.$$

Thus, from above, we get that $\widetilde{f}(b^{-1}a) = \widetilde{f}(ba)b^2$. By Lemma 8 (iv), $\overline{C}(ba) = \overline{C}(b^{-1}a)$. Therefore, the conditions

$$\widetilde{f}(ba) \in \overline{C}(ba) \quad \text{and} \quad \widetilde{f}(b^{-1}a) \in \overline{C}(b^{-1}a)$$

are equivalent, provided the condition $f(b) \in \overline{C}(b)$ holds.

Since $f(b) \in \overline{C}(b)$ and by Lemma 8 (i), $\overline{\mathcal{B}}(b)$ is a basis of $\overline{C}(b)$,

therefore,

$$\begin{aligned} f(b) = &\sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \lambda_{k,0}(a^{2k} - a^{-2k}) + \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \lambda_{k,1}(a^{2k} - a^{-2k})b \\ &+ \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \lambda_{k,2}(a^{2k} - a^{-2k})b^2 + \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \lambda_{k,3}(a^{2k} - a^{-2k})b^3 \\ &+ \sum_{k=1}^{\lfloor \frac{n+1}{2} \rfloor} \mu_{k,0}(a^{2k-1} - a^{-(2k-1)}b^2) \\ &+ \sum_{k=1}^{\lfloor \frac{n+1}{2} \rfloor} \mu_{k,1}(a^{2k-1} - a^{-(2k-1)}b^2)b \\ &+ \sum_{k=1}^{\lceil \frac{n-1}{2} \rceil} \delta_{k,0}(a^{-(2k-1)} - a^{2k-1}b^2) \\ &+ \sum_{k=1}^{\lceil \frac{n-1}{2} \rceil} \delta_{k,1}(a^{-(2k-1)} - a^{2k-1}b^2)b \end{aligned}$$

for some $\lambda_{k,j}$ $(1 \leqslant k \leqslant \lfloor \frac{n-1}{2} \rfloor, 0 \leqslant j \leqslant 3)$, $\mu_{k,0}, \mu_{k,1}$ $(1 \leqslant k \leqslant \lfloor \frac{n+1}{2} \rfloor)$, $\delta_{k,0}, \delta_{k,1}$ $(1 \leqslant k \leqslant \lceil \frac{n-1}{2} \rceil)$ in $\mathbb{F}$. Further since $\widetilde{f}(ba) \in \overline{C}(ba)$ and by Lemma 8 (iii), $\overline{\mathcal{B}}(ba)$ is a basis of $\overline{C}(ba)$, therefore,

$$\begin{aligned} \widetilde{f}(ba) = &\sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} c_{k,0}(a^{2k} - a^{-2k}) + \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} c_{k,1}(a^{2k} - a^{-2k})b^2 \\ &+ \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} c_{k,2}(a^{2k-1} - a^{-(2k+1)})b \\ &+ \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} c_{k,3}(a^{2k-1} - a^{-(2k+1)})b^3 \\ &+ \sum_{k=1}^{n} d_{k,0}(a^{2k-1} - a^{-(2k-1)}b^2) + \sum_{k=1}^{n} d_{k,1}(a^{2k-2} - a^{-2k}b^2)b \end{aligned}$$

for some $c_{k,j}$ $(1 \leqslant k \leqslant \lfloor \frac{n-1}{2} \rfloor, 0 \leqslant j \leqslant 3)$, $d_{k,0}, d_{k,1}$ $(1 \leqslant k \leqslant n)$ in $\mathbb{F}$.

As $f(a) = b^{-1}f(ba) - b^{-1}f(b)a$, $f(b) \in \overline{C}(b)$ and $b^{-1}a = a^{-1}b$, we get $f(a) = b^{-1}f(ba) + f(b)a^{-1}b$. So on comparing,

$$c_1 b + c_3 b^3 = f(a) = b^{-1}f(ba) + f(b)a^{-1}b,$$

we will get the following four equations:

$$\begin{aligned}
&\sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor} c_{k,3}(a^{-(2k-1)} - a^{2k+1}) + \sum_{k=1}^{n} d_{k,1}a^{-(2k-2)} \\
&\quad + \sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor} \lambda_{k,1}(a^{2k+1} - a^{-(2k-1)}) + \sum_{k=1}^{\lfloor\frac{n+1}{2}\rfloor} \mu_{k,1}a^{2k} \\
&\quad + \sum_{k=1}^{\lceil\frac{n-1}{2}\rceil} \delta_{k,1}a^{-(2k-2)} = 0;
\end{aligned} \tag{3.12}$$

$$\begin{aligned}
c_1 = &\sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor} c_{k,1}(a^{-2k} - a^{2k}) + \sum_{k=1}^{n} d_{k,0}a^{-(2k-1)} \\
&+ \sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor} \lambda_{k,0}(a^{2k-1} - a^{-(2k+1)}) + \sum_{k=1}^{\lfloor\frac{n+1}{2}\rfloor} \mu_{k,0}a^{2k-2} \\
&+ \sum_{k=1}^{\lceil\frac{n-1}{2}\rceil} \delta_{k,0}a^{-2k};
\end{aligned} \tag{3.13}$$

$$\begin{aligned}
&\sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor} c_{k,2}(a^{-(2k-1)} - a^{2k+1}) - \sum_{k=1}^{n} d_{k,1}a^{2k} \\
&\quad + \sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor} \lambda_{k,3}(a^{2k+1} - a^{-(2k-1)}) - \sum_{k=1}^{\lfloor\frac{n+1}{2}\rfloor} \mu_{k,1}a^{-(2k-2)} \\
&\quad - \sum_{k=1}^{\lceil\frac{n-1}{2}\rceil} \delta_{k,1}a^{2k} = 0;
\end{aligned} \tag{3.14}$$

$$c_3 = \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} c_{k,0}(a^{-2k} - a^{2k}) - \sum_{k=1}^{n} d_{k,0}a^{2k-1} + \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \lambda_{k,2}(a^{2k-1} - a^{-(2k+1)}) - \sum_{k=1}^{\lfloor \frac{n+1}{2} \rfloor} \mu_{k,0}a^{-2k} - \sum_{k=1}^{\lceil \frac{n-1}{2} \rceil} \delta_{k,0}a^{2k-2}. \tag{3.15}$$

Now, we have two possible cases.

Case 1: n is odd. Then

$$\left\lceil \frac{n-1}{2} \right\rceil = \frac{n-1}{2} = \left\lceil \frac{n-1}{2} \right\rceil \quad \text{and} \quad \left\lfloor \frac{n+1}{2} \right\rfloor = \frac{n+1}{2}.$$

From (3.12), we get that

$$\sum_{k=1}^{\frac{n-1}{2}} (c_{k,3} - \lambda_{k,1})a^{-(2k-1)} + \sum_{k=1}^{\frac{n-1}{2}} (\lambda_{k,1} - c_{k,3})a^{2k+1} + \sum_{k=1}^{\frac{n-1}{2}} (d_{k,1} + \delta_{k,1})a^{-(2k-2)} + \sum_{k=1}^{\frac{n+1}{2}} (d_{(n-k+1),1} + \mu_{k,1})a^{2k} = 0.$$

Therefore,

$$\lambda_{k,1} = c_{k,3} \ (1 \leqslant k \leqslant (n-1)/2), \ \delta_{k,1} = -d_{k,1} \ (1 \leqslant k \leqslant (n-1)/2)$$

and

$$\mu_{k,1} = -d_{(n-k+1),1} \ (1 \leqslant k \leqslant (n+1)/2).$$

From (3.14), we get an additional condition that

$$\lambda_{k,3} = c_{k,2} \ (1 \leqslant k \leqslant (n-1)/2).$$

Also observe that for the above determined values of c_1 in (3.13)

and c_3 in (3.15), we have that $c_1 + c_3 \in \Delta'(\langle a^2 \rangle)$. So

$$f(a) = c_1 b + c_3 b^3 = \sum_{k=1}^{\frac{n-1}{2}} c_{k,1}(a^{-2k} - a^{2k})b$$

$$+ \sum_{k=1}^{n} d_{k,0}(a^{-(2k-1)} - a^{2k-1}b^2)b + \sum_{k=1}^{\frac{n-1}{2}} \lambda_{k,0}(a^{2k-1} - a^{-(2k+1)})b$$

$$+ \sum_{k=1}^{\frac{n+1}{2}} \mu_{k,0}(a^{2k-2} - a^{-2k}b^2)b + \sum_{k=1}^{\frac{n-1}{2}} \delta_{k,0}(a^{-2k} - a^{2k-2}b^2)b$$

$$+ \sum_{k=1}^{\frac{n-1}{2}} c_{k,0}(a^{-2k} - a^{2k})b^3 + \sum_{i=1}^{\frac{n-1}{2}} \lambda_{k,2}(a^{2k-1} - a^{-(2k+1)})b^3.$$

Now put

$$\mathcal{B}_o = \{d_{(\bar{a},\bar{b})} \mid (\bar{a},\bar{b}) \in B_{o1} \cup B_{o2} \cup B_{o3}\},$$

where $\bar{a} = d(a) = f(a)$, $\bar{b} = d(b) = f(b)$ and

$$\begin{aligned} B_{o1} = \big\{&((a^{-2k} - a^{2k})b, 0), \quad ((a^{2k-1} - a^{-(2k+1)})b, (a^{2k} - a^{-2k})), \\ &((a^{-2k} - a^{2k})b^3, 0), \quad ((a^{2k-1} - a^{-(2k+1)})b^3, (a^{2k} - a^{-2k})b^2), \\ &(0, (a^{2k} - a^{-2k})b), \quad (0, (a^{2k} - a^{-2k})b^3), \\ &((a^{-2k} - a^{2k-2}b^2)b, (a^{-(2k-1)} - a^{2k-1}b^2)), \\ &(0, (a^{-(2k-1)} - a^{2k-1}b^2)b) \mid 1 \leqslant k \leqslant (n-1)/2\big\}, \end{aligned}$$

$$\begin{aligned} B_{o2} = \big\{&((a^{2k-2} - a^{-2k}b^2)b, (a^{2k-1} - a^{-(2k-1)}b^2)), \\ &(0, (a^{2k-1} - a^{-(2k-1)}b^2)b) \mid 1 \leqslant k \leqslant (n+1)/2\big\}, \end{aligned}$$

$$B_{o3} = \big\{((a^{-(2k-1)} - a^{2k-1}b^2)b, 0) \mid 1 \leqslant k \leqslant n\big\}.$$

Note that

$$|B_{o1}| = 4(n-1), \quad |B_{o2}| = n+1 \quad \text{and} \quad |B_{o3}| = n.$$

We now prove that $\mathcal{B}_o$ is a basis of $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n})$ over $\mathbb{F}$. If $c_1, c_2 \in \mathbb{F}$

and $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{F}V_{8n}$, then

$$\begin{aligned}\big(c_1 d_{(\alpha_1,\beta_1)} + c_2 d_{(\alpha_2,\beta_2)}\big)(a) &= c_1 d_{(\alpha_1,\beta_1)}(a) + c_2 d_{(\alpha_2,\beta_2)}(a)\\ &= c_1\alpha_1 + c_2\alpha_2 = d_{(c_1\alpha_1+c_2\alpha_2, c_1\beta_1+c_2\beta_2)}(a).\end{aligned}$$

Similarly,

$$d_{(c_1\alpha_1+c_2\alpha_2, c_1\beta_1+c_2\beta_2)}(b) = \big(c_1 d_{(\alpha_1,\beta_1)} + c_2 d_{(\alpha_2,\beta_2)}\big)(b).$$

So by using the fact that any $\mathbb{F}$-derivation of $\mathbb{F}V_{8n}$ is completely determined by its image values $d(a)$ and $d(b)$, we get from above that

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

Therefore, $\mathcal{B}_o$ spans $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n})$ over $\mathbb{F}$. Now choose $r_i, s_j, t_k \in \mathbb{F}$ $(1 \leqslant i \leqslant 4(n-1),\ 1 \leqslant j \leqslant n+1,\ 1 \leqslant k \leqslant n)$ such that

$$\sum_{(\alpha_i,\beta_i)\in B_{o1}} r_i d_{(\alpha_i,\beta_i)} + \sum_{(\gamma_j,\delta_j)\in B_{o2}} s_j d_{(\gamma_j,\delta_j)} + \sum_{(\zeta_k,\eta_k)\in B_{o3}} t_k d_{(\zeta_k,\eta_k)} = 0,$$

where 0 on the right denotes the zero derivation. Therefore,

$$d_{\left(\begin{smallmatrix}\sum_{(\alpha_i,\beta_i)\in B_{o1}} r_i\alpha_i + \sum_{(\gamma_j,\delta_j)\in B_{o2}} s_j\gamma_j + \sum_{(\zeta_k,\eta_k)\in B_{o3}} t_k\zeta_k,\\ \sum_{(\alpha_i,\beta_i)\in B_{o1}} r_i\beta_i + \sum_{(\gamma_j,\delta_j)\in B_{o2}} s_j\delta_j + \sum_{(\zeta_k,\eta_k)\in B_{o3}} t_k\eta_k\end{smallmatrix}\right)} = 0.$$

This implies that the function on the left takes zero value at all points in the domain $\mathbb{F}V_{8n}$, in particular, at a and b. Therefore,

$$\sum_{(\alpha_i,\beta_i)\in B_{o1}} r_i\alpha_i + \sum_{(\gamma_j,\delta_j)\in B_{o2}} s_j\gamma_j + \sum_{(\zeta_k,\eta_k)\in B_{o3}} t_k\zeta_k = 0$$

and

$$\sum_{(\alpha_i,\beta_i)\in B_{o1}} r_i\beta_i + \sum_{(\gamma_j,\delta_j)\in B_{o2}} s_j\delta_j + \sum_{(\zeta_k,\eta_k)\in B_{o3}} t_k\eta_k = 0.$$

But then the $\mathbb{F}$-linear independence of the sets

$$\{\alpha_i, \gamma_j, \zeta_k \mid (\alpha_i,\beta_i) \in B_{o1}, (\gamma_j,\delta_j) \in B_{o2}, (\zeta_k,\eta_k) \in B_{o3}\}$$
$$\text{and} \quad \{\beta_i, \delta_j, \eta_k \mid (\alpha_i,\beta_i) \in B_{o1}, (\gamma_j,\delta_j) \in B_{o2}, (\zeta_k,\eta_k) \in B_{o3}\}$$

implies that $r_i = 0$ $(1 \leqslant i \leqslant 4(n-1))$, $s_j = 0$ $(1 \leqslant j \leqslant n+1)$ and $t_k = 0$ $(1 \leqslant k \leqslant n)$. Therefore, $\mathcal{B}_o$ is an $\mathbb{F}$-linearly independent subset of $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n})$. Therefore, $\mathcal{B}_o$ is a basis of $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n})$ over $\mathbb{F}$ when n is odd. Further, since $|\mathcal{B}_o| = 3(2n-1)$, therefore, the dimension of $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n})$ over $\mathbb{F}$ is $3(2n-1)$ when n is odd.

Case 2: n is even. Then

$$\left\lfloor \frac{n-1}{2} \right\rfloor = \frac{n}{2} - 1 \quad \text{and} \quad \left\lceil \frac{n-1}{2} \right\rceil = \frac{n}{2}.$$

As in Case 1, (3.12) and (3.14) yield that $\lambda_{k,1} = c_{k,3}$ $(1 \leqslant k \leqslant \frac{n}{2} - 1)$, $\delta_{k,1} = -d_{k,1}$ $(1 \leqslant k \leqslant \frac{n}{2})$, $\mu_{k,1} = -d_{(n-k+1),1}$ $(1 \leqslant k \leqslant \frac{n}{2})$ and $\lambda_{k,3} = c_{k,2}$ $(1 \leqslant k \leqslant \frac{n}{2} - 1)$. The relations (3.8),(3.9),(3.10), and (3.11) are also satisfied by the expressions of c_1 and c_3 determined in (3.13) and (3.15) respectively. So

$$\begin{aligned}
f(a) = c_1 b + c_3 b^3 =& \sum_{k=1}^{\frac{n}{2}-1} c_{k,1}(a^{-2k} - a^{2k})b \\
&+ \sum_{k=1}^{n} d_{k,0}(a^{-(2k-1)} - a^{2k-1}b^2)b \\
&+ \sum_{k=1}^{\frac{n}{2}-1} \lambda_{k,0}(a^{2k-1} - a^{-(2k+1)})b + \sum_{k=1}^{\frac{n}{2}} \mu_{k,0}(a^{2k-2} - a^{-2k}b^2)b \\
&+ \sum_{k=1}^{\frac{n}{2}} \delta_{k,0}(a^{-2k} - a^{2k-2}b^2)b + \sum_{k=1}^{\frac{n}{2}-1} c_{k,0}(a^{-2k} - a^{2k})b^3 \\
&+ \sum_{k=1}^{\frac{n}{2}-1} \lambda_{k,2}(a^{2k-1} - a^{-(2k+1)})b^3.
\end{aligned}$$

Then, as shown in Case 1, it can be shown that the set

$$\mathcal{B}_e = \{d_{(\bar{a},\bar{b})} \mid (\bar{a},\bar{b}) \in B_{e1} \cup B_{e2} \cup B_{e3}\},$$

where

$$\begin{aligned}
B_{e1} = \big\{&((a^{-2k} - a^{2k})b, 0), \quad ((a^{2k-1} - a^{-(2k+1)})b, (a^{2k} - a^{-2k})), \\
&((a^{-2k} - a^{2k})b^3, 0), \quad ((a^{2k-1} - a^{-(2k+1)})b^3, (a^{2k} - a^{-2k})b^2), \\
&(0, (a^{2k} - a^{-2k})b), \quad (0, (a^{2k} - a^{-2k})b^3) \mid 1 \leqslant k \leqslant \frac{n}{2} - 1\big\},
\end{aligned}$$

$$\begin{aligned}B_{e2} = \big\{&((a^{2k-2} - a^{-2k}b^2)b, (a^{2k-1} - a^{-(2k-1)}b^2)),\\ &((a^{-2k} - a^{2k-2}b^2)b, (a^{-(2k-1)} - a^{2k-1}b^2)),\\ &(0, (a^{2k-1} - a^{-(2k-1)}b^2)b), \quad (0, (a^{-(2k-1)} - a^{2k-1}b^2)b)\\ &\mid 1 \leqslant k \leqslant \frac{n}{2}\big\},\end{aligned}$$

$$B_{e3} = \{((a^{-(2k-1)} - a^{2k-1}b^2)b, 0) \mid 1 \leqslant k \leqslant n\},$$

where $\bar{a} = d(a) = f(a)$ and $\bar{b} = d(b) = f(b)$, is a basis of $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n})$ over $\mathbb{F}$. Since $|\mathcal{B}_e| = 6(n-1)$, therefore, the dimension of $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n})$ over $\mathbb{F}$ is $6(n-1)$ when n is even. Observe that

$$\mathcal{B} = \begin{cases} \mathcal{B}_o & \text{if } n \text{ is odd} \\ \mathcal{B}_e & \text{if } n \text{ is even} \end{cases}.$$

So, part (i) of the theorem is proved.

(ii) $\mathrm{char}(\mathbb{F}) \neq 0$, that is, $\mathrm{char}(\mathbb{F}) = p$. Then (3.1) always holds, that is, c_0 and c_2 are not necessarily 0. We can proceed as in part (i) to show that the conditions (3.2) and (3.3) give $c_1 + c_3 \in \Delta'(\langle a^2 \rangle)$ when n is odd and give equations (3.8), (3.9), (3.10) and (3.11) when n is even. Proceeding likewise as in (i), we will get that

$$c_0 + c_1 b + c_2 b^2 + c_3 b^3 = b^{-1} f(ba) + f(b) a^{-1} b.$$

On solving and equating, we will get the following four equations:

$$\begin{aligned}c_0 = &\sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} c_{k,3}(a^{-(2k-1)} - a^{2k+1}) + \sum_{k=1}^{n} d_{k,1} a^{-(2k-2)}\\ &+ \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \lambda_{k,1}(a^{2k+1} - a^{-(2k-1)}) + \sum_{k=1}^{\lfloor \frac{n+1}{2} \rfloor} \mu_{k,1} a^{2k} + \sum_{k=1}^{\lceil \frac{n-1}{2} \rceil} \delta_{k,1} a^{-(2k-2)};\end{aligned}$$

$$\begin{aligned}c_1 = &\sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} c_{k,1}(a^{-2k} - a^{2k}) + \sum_{k=1}^{n} d_{k,0} a^{-(2k-1)}\\ &+ \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \lambda_{k,0}(a^{2k-1} - a^{-(2k+1)}) + \sum_{k=1}^{\lfloor \frac{n+1}{2} \rfloor} \mu_{k,0} a^{2k-2} + \sum_{k=1}^{\lceil \frac{n-1}{2} \rceil} \delta_{k,0} a^{-2k};\end{aligned}$$

$$c_2 = \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} c_{k,2}(a^{-(2k-1)} - a^{2k+1}) - \sum_{k=1}^{n} d_{k,1}a^{2k} + \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \lambda_{k,3}(a^{2k+1} - a^{-(2k-1)}) - \sum_{k=1}^{\lfloor \frac{n+1}{2} \rfloor} \mu_{k,1}a^{-(2k-2)} - \sum_{k=1}^{\lceil \frac{n-1}{2} \rceil} \delta_{k,1}a^{2k};$$

$$c_3 = \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} c_{k,0}(a^{-2k} - a^{2k}) - \sum_{k=1}^{n} d_{k,0}a^{2k-1} + \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \lambda_{k,2}(a^{2k-1} - a^{-(2k+1)}) - \sum_{k=1}^{\lfloor \frac{n+1}{2} \rfloor} \mu_{k,0}a^{-2k} - \sum_{k=1}^{\lceil \frac{n-1}{2} \rceil} \delta_{k,0}a^{2k-2}.$$

For the above computed values of c_1 and c_3, a careful observation gives that when n is odd, $c_1 + c_3 \in \Delta'(\langle a^2 \rangle)$ and when n is even, then equations (3.8),(3.9),(3.10) and (3.11) hold. So

$$f(a) = c_0 + c_1 b + c_2 b^2 + c_3 b^3,$$

where c_0, c_1, c_2, c_3 are as determined above. Then, as done in part (i), it can be very easily seen that the set $\mathcal{B}'$ given in part (ii) of the statement of the theorem is a basis of $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n})$ over $\mathbb{F}$. Also,

$$|\mathcal{B}| = 8\Big(\Big\lfloor \frac{n-1}{2} \Big\rfloor\Big) + 2\Big(\Big\lfloor \frac{n+1}{2} \Big\rfloor\Big) + 2\Big(\Big\lceil \frac{n-1}{2} \Big\rceil\Big) + 2n.$$

Therefore, the dimension of $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n})$ over $\mathbb{F}$ is $4(2n-1)$ when n is odd and $8(n-1)$ when n is even. Hence, the theorem is proved. □

Corollary 10 *Let* $\mathbb{F}$ *be an algebraic extension of a prime field whose characteristic is either* 0 *or an odd rational prime relatively prime to* n. *Then the dimension of the derivation algebra* $\mathrm{Der}(\mathbb{F}V_{8n})$ *over* $\mathbb{F}$ *is* $6(n-1)$ *if* n *is even and* $3(2n-1)$ *if* n *is odd, and a basis is* $\mathcal{B}$ *given in* Theorem 9 (i).

Proof — Follows from Theorem 2 and Theorem 9 (i). □

Proposition 11 *Let* $\mathbb{F}$ *be a field. Then the dimension of* $\mathrm{Der}_{\mathrm{Inn}}(\mathbb{F}V_{8n})$ *is* $6(n-1)$ *if* n *is even and* $3(2n-1)$ *if* n *is odd.*

(i) *When* n *is even, a basis for* $\mathrm{Der}_{\mathrm{Inn}}(\mathbb{F}V_{8n})$ *over* $\mathbb{F}$ *is*

$$\mathcal{B}_1 = \{d_g \mid g \in \{\{a^{2k},\ a^{2k}b^2,\ a^{4k}b^{-1},\ a^{4k+1}b^{-1},\ a^{4k+2}b^{-1},\ a^{4k+3}b^{-1} \mid 1 \leqslant k \leqslant n/2-1\} \cup \{a^{2k-1} \mid 1 \leqslant k \leqslant n\}$$

$$\cup\{a^{4k}b,\ a^{4k+1}b,\ a^{4k+2}b,\ a^{4k+3}b \mid 1 \leqslant k \leqslant n/2\}\}\}.$$

(ii) *When* n *is odd, a basis for* $\mathrm{Der}_{\mathrm{Inn}}(\mathbb{F}V_{8n})$ *over* $\mathbb{F}$ *is*

$$\begin{aligned}\mathcal{B}_2 = \Big\{ d_g \mid g \in \{&a^{2k},\ a^{2k}b^2 \mid 1 \leqslant k \leqslant (n-1)/2\} \\ &\cup\{a^{2k-1},\ a^{2k}b,\ a^{2k+1}b \mid 1 \leqslant k \leqslant n\} \\ &\cup\{a^{2k}b^{-1},\ a^{2k+1}b^{-1} \mid 1 \leqslant k \leqslant n-1\}\Big\}.\end{aligned}$$

Proof — Follows from Theorem 3 and Lemma 6. □

Corollary 12 *Let* $\mathbb{F}$ *be an algebraic extension of a prime field and* p *be an odd rational prime.*

(i) *If* $\mathrm{char}(\mathbb{F})$ *is either* 0 *or* p *with* $\gcd(n,p) = 1$, *then all derivations of* $\mathbb{F}V_{8n}$ *are inner, that is,* $\mathrm{Der}(\mathbb{F}V_{8n}) = \mathrm{Der}_{\mathrm{Inn}}(\mathbb{F}V_{8n})$. *In other words,* $\mathbb{F}V_{8n}$ *has no non-zero outer derivations.*

(ii) *If* $\mathrm{char}(\mathbb{F}) = p$ *with* $\gcd(n,p) \neq 1$, *then*

$$\mathrm{Der}_{\mathrm{Inn}}(\mathbb{F}V_{8n}) \subsetneq \mathrm{Der}(\mathbb{F}V_{8n}).$$

In other words, $\mathbb{F}V_{8n}$ *has non-zero outer derivations.*

Proof — This follows from Theorem 9, Corollary 10 and Proposition 11. □

We conclude this section with a remark on the restriction of derivations to the simple components in the Wedderburn decomposition of $\mathbb{F}V_{8n}$, in case it is semisimple.

Remark 13 Consider the case when the group algebra $\mathbb{F}V_{8n}$ is semisimple, that is, by Maschke's Theorem, the case when $\mathrm{char}(\mathbb{F})$ does not divide the order of V_{8n}. Therefore, $\mathbb{F}V_{8n}$ is semisimple if and only if either $\mathrm{char}(\mathbb{F}) = 0$ or p with $\gcd(n,p) = 1$. By Theorem 9 (i) and Proposition 11,

$$\mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n}) = \mathrm{Der}_{\mathrm{Inn}}(\mathbb{F}V_{8n}).$$

As a result, in its Wedderburn decomposition, an $\mathbb{F}$-derivation of $\mathbb{F}V_{8n}$ restricts to each simple component of $\mathbb{F}V_{8n}$. More precisely, take $d \in \mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n})$. Then $d = d_\beta$ for some $\beta \in \mathbb{F}V_{8n}$. A simple component of $\mathbb{F}V_{8n}$ looks like $\mathbb{F}V_{8n}e$, where e is a primitive central idempotent of $\mathbb{F}V_{8n}$. Then, for any $\alpha \in \mathbb{F}V_{8n}e$, $\alpha = \gamma e$ for some $\gamma \in \mathbb{F}V_{8n}$.

So

$$d(\alpha) = d_\beta(\alpha) = \alpha\beta - \beta\alpha = (\gamma e)\beta - \beta(\gamma e) = (\gamma\beta - \beta\gamma)e$$
$$= (d_\beta(\gamma))e = d(\gamma)e \in \mathbb{F}V_{8n}e$$

as $d(\gamma) \in \mathbb{F}V_{8n}$. Therefore, $d(\mathbb{F}V_{8n}e) \subseteq \mathbb{F}V_{8n}e$. When $\mathbb{F}$ is an algebraic extension of a prime field, then by Corollary 10,

$$\mathrm{Der}_{\mathbb{F}}(\mathbb{F}V_{8n}) = \mathrm{Der}(\mathbb{F}V_{8n}),$$

that is, every $\mathbb{F}$-derivation of $\mathbb{F}V_{8n}$ is a derivation of $\mathbb{F}V_{8n}$. Therefore, from the above discussion, it follows that when $\mathbb{F}$ is an algebraic extension of a prime field, then any derivation of $\mathbb{F}V_{8n}$ restricts to each simple component of $\mathbb{F}V_{8n}$, that is, $d(\mathbb{F}V_{8n}e) \subseteq \mathbb{F}V_{8n}e$ for all d in $\mathrm{Der}(\mathbb{F}V_{8n})$.

We can prove that the result holds for any semisimple group algebra $\mathbb{F}G$ of a finite group G over a field $\mathbb{F}$. In fact, by Maschke's Theorem, $\mathrm{char}(\mathbb{F})$ does not divide the order of G. By the Wedderburn–Artin Theorem,

$$\mathbb{F}G \simeq \mathbb{F}Ge_1 \oplus \ldots \oplus \mathbb{F}Ge_r$$

with the following conditions:

(i) The above isomorphism is an isomorphism of $\mathbb{F}$-algebras.

(ii) $\{e_1, \ldots, e_r\}$ is a unique collection of primitive central idempotents of $\mathbb{F}G$.

(iii) For each $i \in \{1, \ldots, r\}$, $\mathbb{F}Ge_i$ is a simple ring, and $\mathbb{F}Ge_1, \ldots, \mathbb{F}Ge_r$ are called *simple components* of $\mathbb{F}G$.

(iv) For each $i \in \{1, \ldots, r\}$, $\mathbb{F}Ge_i \simeq M_{n_i}(D_i)$, the full matrix ring over D_i, where D_i is a division algebra containing an isomorphic copy of $\mathbb{F}$ in its center.

Let $d \in \mathrm{Der}(\mathbb{F}G)$ and $i, j \in \{1, \ldots, r\}$ with $j \neq i$. Then

$$d(e_i) = d(e_i^2) = d(e_i)e_i + e_i d(e_i).$$

Multiplying both sides by e_j and using the fact that the idempotents e_i, e_j are central with $e_i e_j = 0$, we get that

$$d(e_i)e_j = d(e_i)(e_i e_j + e_i e_j) = 0.$$

Therefore, for each $j \in \{1, \ldots, r\}$ with $j \neq i$, $d(e_i)e_j = 0$, that is, for each $j \in \{1, \ldots, r\}$, $d(e_i)$ is orthogonal to e_j. Therefore, $d(e_i) \in \mathbb{F}Ge_i$. Now let $\beta \in \mathbb{F}Ge_i$ so that $\beta = \alpha e_i$ for some $\alpha \in \mathbb{F}G$. Then

$$d(\beta) = d(\alpha e_i) = d(\alpha)e_i + \alpha d(e_i).$$

Since $\alpha, d(\alpha) \in \mathbb{F}G$, $e_i, d(e_i) \in \mathbb{F}Ge_i$ and $\mathbb{F}Ge_i$ is a two-sided ideal of $\mathbb{F}G$, therefore, $d(\beta) \in \mathbb{F}Ge_i$. Therefore, $d(\mathbb{F}Ge_i) \subseteq \mathbb{F}Ge_i$. Therefore, all derivations of $\mathbb{F}G$ restrict to all simple components of $\mathbb{F}G$ in the Wedderburn decomposition of $\mathbb{F}G$.

Acknowledgments

The authors thank the referees and the editor for their critical reviews, comments, and suggestions, which have improved the presentation and quality of the paper. The second author was the ConsenSys Blockchain chair professor when the work was being carried out. He thanks ConsenSys AG for that privilege.

REFERENCES

[1] A. Alekseev – A. Arutyunov – S. Silvestrov: "On (σ, τ)-derivations of group algebra as category characters", in Non-Commutative and Non-Associative Algebra and Analysis Structures, *Springer*, Cham (2023), 81–99.

[2] O.D. Artemovych – V.A. Bovdi – M.A. Salim: "Derivations of group rings", *Acta Sci. Math.* (*Szeged*) 86 (2020), 51–72.

[3] A.A. Arutyunov: "Derivation algebra in noncommutative group algebras", *Proc. Steklov Inst. Math.* 308 (2020), 22–34.

[4] A. Arutyunov: "Derivations in group algebras and combinatorial invariants of groups", *Eur. J. Math.* 9 (2023), Paper No. 39, 20pp.

[5] A. Arutyunov – A. Alekseev: "Complex of n-categories and derivations in group algebras", *Topology Appl.* 275 (2020), 107002, 12pp.

[6] A.A. Arutyunov – L.M. Kosolapov: "Derivations of group rings for finite and FC groups", *Finite Fields Appl.* 76 (2021), 101921, 31pp.

[7] A.A. Arutyunov – A.S. Mishchenko – A.I. Shtern: "Derivations of group algebras", *J. Math. Sci.* 248 (2020), 709–718.

[8] M.J. Atteya: "New types of permuting n-derivations with their applications on associative rings", *Symmetry* 12 (2019), Paper No. 46, 48pp.

[9] M. Bresar: "On the composition of (α, β)-derivations of rings and applications to von Neumann algebras", *Acta Sci. Math* 56 (1992), 369–375.

[10] M.A. Chaudhry – Z. Ullah: "On generalized (α, β)-derivations on lattices", *Quaest. Math.* 34 (2011), 417–424.

[11] D. Chaudhuri: "(σ, τ)-Derivations of group rings", *Comm. Algebra* 47 (2019), 3800–3807.

[12] D. Chaudhuri: "The twisted derivation problem for group rings", *Arch. Math.* (*Basel*) 116 (2021), 391–401.

[13] L. Creedon – K. Hughes: "Derivations on group algebras with coding theory applications", *Finite Fields Appl.* 56 (2019), 247–265.

[14] B. Delphine – F. Ulmer: "Linear codes using skew polynomials with automorphisms and derivations", *Des. Codes Cryptogr.* 70 (2014), 405–431.

[15] M. Ferrero – A. Giambruno – C.P. Milies: "A note on derivations of group rings", *Canad. Math. Bull.* 38 (1995), 434–437.

[16] L. Kamali Ardakani – B. Davvaz: "f-Derivations and (f, g)-derivations of MV-algebras", *J. Alg. Syst.* 1 (2013), 11–31.

[17] K.H. Kim: "On (f, g)-derivations of incline algebras", *J. Chungcheong Math. Soc.* 27 (2014), 643–649.

[18] S. Klimek – M. McBride: "Unbounded derivations in algebras associated with monothetic groups", *J. Aust. Math. Soc.* 111 (2021), 345–371.

[19] P. Manju – R.K. Sharma: "Derivations of non-commutative group algebras", *J. Algebra Appl.* (2025); doi:10.1142/S0219498825503712.

[20] G. Muhiuddin – A.M. Al-Roqi: "On (α, β)-derivations in BCI-algebras", *Discrete Dyn. Nat. Soc.* (2012), 403209, 11pp.

[21] A. Mustafa – Ş. Ceran: "Generalized (f, g)-derivations of lattices", *Math. Sci. Appl. E-Notes* 1 (2013), 56–62.

[22] M.A. Raza – N.U. Rehman: "On prime and semiprime rings with generalized derivations and non-commutative Banach algebras", *Proc. Indian Acad. Sci. Math. Sci.* 126 (2016), 389–398.

[23] M.A. Salahshour – A.R. Ashrafi: "Commuting conjugacy class graph of finite CA-groups", *Khayyam J. Math.* 6 (2020), 108–118.

[24] S. Sehrawat – M. Pruthi: "Codes over non-abelian groups", *J. Inf. Optim. Sci.* 40 (2019), 789–804.

[25] M.K. Smith: "Derivations of group algebras of finitely-generated, torsion-free, nilpotent groups", *Houston J. Math* 4 (1978), 277–288.

[26] E. Spiegel: "Derivations of integral group rings", *Comm. Algebra* 22 (1994), 2955–2959.

Praveen Manju (*corresponding author*)
Department of Mathematics
Indian Institute of Technology Delhi
110016 Hauz Khas, New Delhi (India)
e-mail: praveenmanjuiitd@gmail.com

Rajendra Kumar Sharma

Earlier Affiliation
Department of Mathematics
Indian Institute of Technology Delhi
110016 Hauz Khas, New Delhi (India)

Present Affiliation
Department of Mathematics
South Asian University
110068 Maidan Garhi, New Delhi (India)

e-mail: rksharmaiitd@gmail.com