TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 364, Number 8, August 2012, Pages 4155–4168
S 0002-9947(2012)05454-7
Article electronically published on March 21, 2012

SMASH PRODUCTS AND DIFFERENTIAL IDENTITIES

CHEN-LIAN CHUANG AND YUAN-TSUNG TSAI

To Pjek-Hwee Lee on his retirement

ABSTRACT. Let $\mathbf{U}$ be the universal enveloping algebra of a Lie algebra and R a $\mathbf{U}$-module algebra, where $\mathbf{U}$ is considered as a Hopf algebra canonically. We determine the centralizer of R in $R\#\mathbf{U}$ with its associated graded algebra. We then apply this to the Ore extension $R[X;\phi]$, where $\phi : X \to \mathrm{Der}(R)$. With the help of PBW-bases, the following is proved for a prime ring R: Let Q be the symmetric Martindale quotient ring of R. For $f_i, g_i \in Q[X;\phi]$, $\sum_i f_i r g_i = 0$ for all $r \in R$ iff $\sum_i f_i \otimes g_i = 0$, where $\otimes$ is over the centralizer of R in $Q[X;\phi]$. Finally, we deduce from this Kharchenko's theorem on differential identities.

1. INTRODUCTION

By a derivation of an associative ring R, not necessarily with 1, we mean a map $\delta : R \to R$ satisfying

$$\delta(x+y) = \delta(x) + \delta(y), \quad \delta(xy) = \delta(x)y + x\delta(y) \quad \text{for } x, y \in R.$$

Given $a \in R$, define the map $\mathrm{ad}(a) : R \to R$ by $r \in R \mapsto ar - ra$. We check easily that $\mathrm{ad}(a)$ is a derivation of R, called the inner derivation defined by $a \in R$. Let $\mathrm{Der}(R)$ denote the set of derivations of R and $\mathrm{Der}_0(R)$ the set of inner derivations of R. Clearly, $\mathrm{Der}(R)$ forms a Lie ring with respect to $[\delta, d] \stackrel{\text{def.}}{=} \delta d - d\delta$ for $\delta, d \in \mathrm{Der}(R)$. Also clearly, $\mathrm{Der}_0(R)$ forms a Lie ideal of $\mathrm{Der}(R)$ in the sense that $[\mathrm{Der}(R), \mathrm{Der}_0(R)] \subseteq \mathrm{Der}_0(R)$.

Our primary aim is to investigate differential identities of a prime ring R in terms of Ore extensions (to be defined in §3), as initiated in Amitsur [1] for a single derivation and extended in [5] to a set of derivations. For this purpose, we have to compute the centralizer of R in the Ore extension. This was done for Ore extensions with one indeterminate in [1] for simple rings and was extended to prime rings in [9]. The crucial computation of [1] was interpreted in terms of Hasse-Schmidt higher derivations. For Ore extensions with many indeterminates, the computation of the centralizer of R was left open in [5]. Higher derivations don't help much here because of the lack of the division algorithm. Surprisingly, it turns out that this can be done much easier in the more general context of smash products (to be explained in §2) with the associated graded algebras. We apply this to Ore extensions in §3 and then deduce in §4 an interpretation of Kharchenko's theory of differential identities in the context of Ore extensions. It seems very interesting whether results of §4 can be extended to the context of smash products

Received by the editors May 4, 2010 and, in revised form, August 30, 2010.
2010 *Mathematics Subject Classification.* Primary 16S40, 16S32, 16W25, 16S36, 16S30.
Key words and phrases. Derivations, universal enveloping algebras, centralizers, smash products, Ore extensions, differential identities.

considered in §2. Furthermore, can all these be generalized to q-skew derivations or skew derivations ([4, 8])?

2. Smash products

Throughout here, k is a field. An associative (or Lie, Hopf) algebra over k will be called an associative (or Lie, Hopf resp.) k-algebra. By a Lie ring or a Lie algebra $\mathfrak{g}$, we always mean a restricted p Lie ring or algebra if $\operatorname{char} k = p \geq 2$.

Let $\mathfrak{g}$ be a Lie k-algebra. It is well known that the universal enveloping algebra of $\mathfrak{g}$, denoted by $\mathbf{U}$, forms a pointed irreducible cocommutative Hopf algebra with respect to the comultiplication $\Delta(a) = a \otimes 1 + 1 \otimes a$, the counit $\varepsilon(a) = 0$ and the antipode $S(a) \overset{\text{def.}}{=} -a$ for $a \in \mathfrak{g}$. Assume that R is an associative k-algebra. Let $\operatorname{Der}_k(R)$ be the set of k-linear derivations of R and $\operatorname{End}_k(R)$ the set of k-linear maps of R. So $\operatorname{Der}_k(R)$ forms a Lie k-algebra and $\operatorname{End}_k(R)$ forms an associative k-algebra. Let $\phi : \mathfrak{g} \to \operatorname{Der}_k(R)$ be a Lie k-algebra homomorphism. By the universal mapping property, ϕ extends uniquely to a k-algebra homomorphism $\mathbf{U} \to \operatorname{End}_k(R)$, also denoted by ϕ. With respect to ϕ thus extended, the k-algebra R is a $\mathbf{U}$-module algebra and we can form the smash product $R\#\mathbf{U}$. This is the k-space $R \otimes_k \mathbf{U}$, where we write $a \otimes h$ as $a\#h$ for $a \in R$ and $h \in \mathbf{U}$, endowed with multiplication defined by

$$(a\#h)(b\#g) = ab\#hg + a\phi(h)(b)\#g \quad \text{for } a, b \in R \text{ and } h, g \in \mathbf{U}.$$

We refer the reader to [10] and [13] for the details. Our aim here is to describe the centralizer of R in $R \otimes_k \mathbf{U}$. We recall the following:

Definition 1. Let R be a k-algebra with 1 and ${}_RM$ be a left R-module. We call a finite sum $\sum_i a_i m_i$, where $a_i \in R$ and $m_i \in M$, a left R-linear combination of m_i. By a left R-basis of ${}_RM$, we mean a subset B of M such that any $m \in M$ can be uniquely written as a left R-linear combination of elements in B. A right R-basis of a right R-module is defined analogously. By an R-basis of an (R, R)-bimodule ${}_RM_R$, we mean a subset B of M which is both a left R-basis of ${}_RM$ and a right R-basis of M_R.

The well-known Poincaré-Birkhoff-Witt Theorem asserts that regular words in a linearly ordered k-basis of $\mathfrak{g}$ form a k-basis of its universal enveloping k-algebra $\mathbf{U}$ and hence form an R-basis of $R\#\mathbf{U}$. But our main concern is the centralizer of R in $R\#\mathbf{U}$. Let C be the center of R. Clearly, C centralizes R. So the dependence of elements of $\mathfrak{g}$ over C, not merely over the subfield k of C, has to be considered. We recall the notion of regular words in this general context as follows.

Definition 2. Given a set B, elements of the *free* monoid generated by B are called B-words. The identity of the free monoid generated by B, denoted by 1, is called the empty B-word. Given a B-word, write

$$W = b_1 b_2 \cdots b_n,$$

where $b_i \in B$ and where we postulate $W = 1$ for convenience if $n = 0$. We call n the B-length of W and write $\operatorname{lh}_B(W) = n$. Assume further that B is linearly ordered by $<$. By a *regular* B-word, we mean a B-word in the form

$$b_1^{n_1} b_2^{n_2} \cdot \cdots \cdot b_s^{n_s},$$

where the $b_i \in B$ satisfy $b_1 < b_2 < \cdots < b_s$ and, in the case of $\operatorname{char} k = p \geq 2$, where $0 < n_i < p$ for each i. We order regular B-words first by length and then lexicographically for B-words of the same length.

We shall apply the above notions to algebras. To be precise, we state the following.

Definition 3. Let A be an associative k-algebra with 1 and B a subset of A. By a *B-product*, we mean an *expression* in A of the form

$$b_1 \cdot b_2 \cdot b_3 \cdots b_n,$$

where $b_i \in B$ and where $\cdot$ denotes the multiplication of A. For simplicity of terminology and as an abuse of language, whenever there is no confusion, the B-product above will be identified with the B-word $W \overset{\text{def.}}{=} b_1 b_2 \cdots b_n$ in the free monoid generated by B (as a set of symbols). So the above B-product is regular if so is W and so on.

We stress here that the above notions apply *not* to elements of A but to *expressions* of elements of A as products of elements of B. An element of A may be expressed as many B-products with different associated B-words of different B-lengths and we have to know which expression is meant. Regular words occur naturally in the following.

Lemma 1. *Let R be a k-algebra with 1 and $R[Y]$ the k-algebra generated by R and a set Y of commuting indeterminates subjected to $yr = ry$ and $yy' = y'y$ for $r \in R$ and $y, y' \in Y$. Set $R_p[Y] \overset{\text{def.}}{=} R[Y]/I$, where I is the ideal of $R[Y]$ defined by*

$$I \overset{\text{def.}}{=} \begin{cases} 0 & \text{if } \operatorname{char} k = 0, \\ \text{the ideal generated by } y^p \text{ for } y \in Y & \text{if } \operatorname{char} k = p > 0. \end{cases}$$

For any linear order $<$ of Y, regular Y-words form an R-basis of the polynomial ring $R_p[Y]$. More specifically, for each $n \geq 0$, regular Y-words of Y-length n form an R-basis of the R-module of polynomials of degree n in $R_p[Y]$.

Proof. This is obvious by the commutativity $yr = ry$ and $yy' = y'y$ for $r \in R$ and $y, y' \in Y$. □

Theorem 2. *Assume that R is a ring with the center C being a field. Let k be a subfield of C and $\mathfrak{g}$ a Lie k-algebra with the universal enveloping algebra $\mathbf{U}$. Assume that R is a $\mathbf{U}$-module k-algebra. Let B be a C-basis of $C\mathfrak{g}$ as a left C-subspace of the smash product $R\#\mathbf{U}$. For each $h \in B$, set $h' \overset{\text{def.}}{=} h + a_h$, where $a_h \in R$ is arbitrarily chosen. Define $B' \overset{\text{def.}}{=} \{h' : h \in B\}$ and let $<$ be an arbitrary linear order of B'. Then the set of regular B'-words forms an R-basis of $R\#\mathbf{U}$.*

Proof. For $n \geq 0$, let V_n be the set of $f \in R\#\mathbf{U}$ which can be written in a finite sum $f = \sum_i a_i W_i$, where $0 \neq a_i \in R$ and where W_i is a $\mathfrak{g}$-word of length $\leq n$ for each i. Clearly, $V_n V_m \subseteq V_{n+m}$ and

$$V_0 \subseteq V_1 \subseteq V_2 \subseteq \cdots.$$

So the associative k-algebra $R\#\mathbf{U}$ is filtered. Set $V_{-1} \overset{\text{def.}}{=} 0$ for convenience. Define $\overline{V}_n \overset{\text{def.}}{=} V_n/V_{n-1}$ for $n \geq 0$. For $\bar{a} \in \overline{V}_n$ and $\bar{b} \in \overline{V}_m$, where $a \in V_n$ and $b \in V_m$,

define $\bar{a}\bar{b} \overset{\text{def.}}{=} \overline{ab} \in \overline{V}_{n+m}$. This is well-defined because of $V_sV_t \subseteq V_{s+t}$. With this, we form the graded k-algebra

$$\operatorname{gr}(R\#\mathbf{U}) \overset{\text{def.}}{=} \bigoplus_{i\geq 0} \overline{V}_i.$$

We say that $f \in R\#\mathbf{U}$ has $\mathfrak{g}$-degree n and write $\deg_{\mathfrak{g}}(f) = n$ if $f \in V_n - V_{n-1}$. Given $f \in R\#\mathbf{U}$ with $\deg_{\mathfrak{g}}(f) = n$, define

$$\bar{f} \overset{\text{def.}}{=} f + V_{n-1} \in \overline{V}_n \subseteq \operatorname{gr}(R\#\mathbf{U}).$$

Given finitely many $f, f_i \in R\#\mathbf{U}$, if $f = f_1 + f_2 + \cdots$ and if $\deg_{\mathfrak{g}}(f) = \deg_{\mathfrak{g}}(f_1) = \deg_{\mathfrak{g}}(f_2) = \cdots$, then clearly

$$(\bigstar) \qquad \bar{f} = \bar{f}_1 + \bar{f}_2 + \cdots.$$

For $S \subseteq R\#\mathbf{U}$, set $\overline{S} \overset{\text{def.}}{=} \{\bar{f} \in \operatorname{gr}(R\#\mathbf{U}) : f \in S\}$. Let $h \in \mathfrak{g} \mapsto \delta_h \in \operatorname{Der}_k(R)$ be the Lie homomorphism $\mathfrak{g} \to \operatorname{Der}_k(R)$. For any $r \in R$ and $h \in \mathfrak{g}$, $hr - rh = \delta_h(r) \in R$ and hence $\bar{h}\bar{r} = \bar{r}\bar{h}$ in $\operatorname{gr}(R\#\mathbf{U})$. Since $\delta(C) \subseteq C$ for $\delta \in \operatorname{Der}(R)$, $C\mathfrak{g}$ forms a Lie ring. So for $f_1, f_2 \in C\mathfrak{g}$, $f_1f_2 - f_2f_1 \in C\mathfrak{g} \subseteq V_1$ and hence $\bar{f}_1\bar{f}_2 = \bar{f}_2\bar{f}_1$ in $\operatorname{gr}(R\#\mathbf{U})$. Thus $\overline{C\mathfrak{g}}$ is a commuting set in $\operatorname{gr}(R\#\mathbf{U})$. Clearly, $\operatorname{gr}(R\#\mathbf{U})$ is the k-algebra generated by R and the commuting set $\overline{C\mathfrak{g}}$.

Set $p \overset{\text{def.}}{=} \operatorname{char} R \geq 0$. Given a C-basis Y of $\overline{C\mathfrak{g}}$, let $R_p[Y]$ be as defined in Lemma 1. We *claim* that there is a k-algebra homomorphism $\theta : R_p[Y] \to \operatorname{gr}(R\#\mathbf{U})$ such that $\theta(r) = r$ for $r \in R$ and such that $\theta(y) = y \in \overline{V}_1$ for $y \in Y$. This is clear if $\operatorname{char} R = p = 0$, for $R_p[Y] \overset{\text{def.}}{=} R[Y]$ is the freest k-algebra generated by R and the commuting set Y. Assume $\operatorname{char} R = p \geq 2$. Since $\mathfrak{g}$ is a restricted p-Lie algebra by our convention, there is a unary p-operation $h \mapsto h^{[p]}$ for $h \in \mathfrak{g}$ such that in the universal enveloping algebra $\mathbf{U}$ we have

$$\underbrace{h \cdot h \cdot h \cdots h}_{p \text{ times}} = h^p = h^{[p]}.$$

Since $h^{[p]} \in V_1$, we have $\bar{h}^p = 0$ for $h \in \mathfrak{g}$ in the associated graded algebra $\operatorname{gr}(R\#\mathbf{U})$. Given $0 \neq f \in C\mathfrak{g}$, write $f = \alpha_1h_1 + \alpha_2h_2 + \cdots$, where $\alpha_i \in C$ and $h_i \in \mathfrak{g}$. By $(\bigstar)$, $\bar{f} = \bar{\alpha}_1\bar{h}_1 + \bar{\alpha}_2\bar{h}_2 + \cdots$ and hence

$$\bar{f}^p = (\bar{\alpha}_1\bar{h}_1 + \bar{\alpha}_2\bar{h}_2 + \cdots)^p = \bar{\alpha}_1^p\bar{h}_1^p + \bar{\alpha}_2^p\bar{h}_2^p + \cdots = 0.$$

Since $Y \subseteq \overline{C\mathfrak{g}}$, we see that $y^p = 0$ for $y \in Y$ in $\operatorname{gr}(R\#\mathbf{U})$. By the definition in Lemma 1, $R_p[Y]$ is the freest k-algebra generated by R and the commuting set Y subjected to the condition $y^p = 0$ for $y \in Y$. The claim is thus proved.

We show that θ above is the k-algebra isomorphism of $R_p[Y]$ and $\operatorname{gr}(R\#\mathbf{U})$. The map θ is surjective, since $\operatorname{gr}(R\#\mathbf{U})$ is the k-algebra generated by R and the commuting set Y. To show the injectivity of θ, pick arbitrarily a k-basis B of $\mathfrak{g}$ with a linear order $<$. By the Poincaré-Birkhoff-Witt Theorem, regular B-words form a k-basis of $\mathbf{U}$ and hence form an R-basis of $R\#\mathbf{U}$, since $R\#\mathbf{U}$, as a left C-space, is the same as the left C-space $R \otimes_k \mathbf{U}$; also B forms a C-basis of $C\mathfrak{g}$. So regular B-words of B-lengths $\leq n$ form an R-basis of V_n for each $n \geq 0$. Particularly, $\overline{B}$ forms a C-basis of $\overline{C\mathfrak{g}}$. The injectivity of $R_p[\overline{B}] \to \operatorname{gr}(R\#\mathbf{U})$ follows. Given an arbitrary C-basis Y of $\overline{C\mathfrak{g}}$, there exist $\alpha_b^y, \beta_y^b \in C$ for $b \in B$ and $y \in Y$ such that

$$y = \sum_{b\in B} \alpha_b^y \bar{b} \qquad \text{and} \qquad \bar{b} = \sum_{y\in Y} \beta_y^b y.$$

Since both Y and $\overline{B}$ are C-bases of $\overline{C\mathfrak{g}}$, the two expressions above are inverse to each other. The injectivity of $R_p[Y] \to \mathrm{gr}(R\#\mathbf{U})$ follows from that of $R_p[\overline{B}] \to \mathrm{gr}(R\#\mathbf{U})$.

Let B be a given left C-basis of $C\mathfrak{g}$. Clearly, $\overline{B}$ forms a C-basis of $\overline{C\mathfrak{g}}$ and hence $\mathrm{gr}(R\#\mathbf{U}) = R_p[\overline{B}]$. Let $B' \stackrel{\text{def.}}{=} \{h' : h \in B\}$, where, for each $h \in B$, $h' \stackrel{\text{def.}}{=} h + a_h$ for some $a_h \in R$. Given a linear order $<$ of B', we denote the corresponding linear order of B also by $<$. By Lemma 1, regular $\overline{B}$-words of length n form an R-basis for $\overline{V}_n$. For any $h_1, \dots, h_n \in B$, where $n \geq 1$, we have $h_1 \cdots h_n \equiv h'_1 \cdots h'_n$ modulo V_{n-1}. So regular $\overline{B'}$-words of length n also form an R-basis for $\overline{V}_n$. With this, we see inductively that regular B'-words of length $\leq n$ form a left R-basis of nonzero V_n. From this, our assertion follows. □

Theorem 2 provides very good bases, which deserve a special definition below because of frequent uses in the sequel.

Definition 4. Let R, C, k and $\mathfrak{g}$ be as in Theorem 2. Let $\phi : h \in C\mathfrak{g} \mapsto \delta_h \in \mathrm{Der}_k(R)$ be the left C-linear map extending the Lie homomorphism $\mathfrak{g} \to \mathrm{Der}_k(R)$. (So $\phi(C\mathfrak{g}) = C\phi(\mathfrak{g})$.) Set $\mathfrak{g}_0 \stackrel{\text{def.}}{=} \{h \in C\mathfrak{g} : \delta_h \in \mathrm{Der}_0(R)\}$. Let B be a left C-basis of $C\mathfrak{g}$ such that $B_0 \stackrel{\text{def.}}{=} B \cap \mathfrak{g}_0$ forms a left C-basis of $\mathfrak{g}_0$. For each $h \in B_0$, pick $a_h \in R$ arbitrarily such that $\delta_h = \mathrm{ad}(a_h)$. Define $B'_0 \stackrel{\text{def.}}{=} \{h - a_h : h \in B_0\}$ and $B' \stackrel{\text{def.}}{=} B'_0 \cup (B - B_0)$. Let $<$ be a linear order of B' such that

$$(*) \qquad h < g \qquad \text{for } h \in B'_0 \text{ and } g \in B - B_0.$$

We call B' so ordered a *regular Lie basis* of the smash product $R\#\mathbf{U}$.

With regular Lie bases, we are able to compute the centralizer of R in $R\#\mathbf{U}$. For latter applications, we have to characterize subsets T of R such that the centralizer of T in $R\#\mathbf{U}$ is equal to the centralizer of R in $R\#\mathbf{U}$. This seems interesting in itself.

Theorem 3. *Let R, C, k and $\mathfrak{g}$ be as in Theorem 2. Set $S \stackrel{\text{def.}}{=} R\#\mathbf{U}$. For $T \subseteq R$, set $C_S(T) \stackrel{\text{def.}}{=}$ the centralizer of T in S.*

(1) For $T \subseteq R$, $C_S(T) = C_S(R)$ iff for any $\delta \in C\phi(\mathfrak{g}) + \mathrm{Der}_0(R)$, $\delta(T) = 0$ implies $\delta(R) = 0$.

(2) Let B' be a regular Lie basis of S and retain the notation of Definition 4. The set of regular B'_0-words forms a C-basis of the free C-module $C_S(R)$. For any C-basis V of R, the set

$$\mathbb{B} \stackrel{\text{def.}}{=} \{vW : v \in V \text{ and } W \text{ is a regular word in } B - B_0\}$$

forms a $C_S(R)$-basis of the free $C_S(R)$-module $R\#\mathbf{U}$.

(3) Any element of $S \otimes_{C_S(R)} S$ can be uniquely expressed in the form $\sum_i f_i \otimes g_i$, where $f_i \in R\#\mathbf{U}$ and where the $g_i \in \mathbb{B}$ are distinct.

Proof. Given $h \in C\mathfrak{g}$ and $a \in R$, $\delta_h + \mathrm{ad}(a)$ vanishes on a subset T of R iff $h + a \in C_S(T)$. So if $C_S(T) = C_S(R)$, then $\delta(T) = 0$ implies $\delta(R) = 0$ for $\delta \in C\phi(\mathfrak{g}) + \mathrm{Der}_0(R)$. On the other hand, suppose that $\delta(T) = 0$ implies $\delta(R) = 0$ for any $\delta \in C\phi(\mathfrak{g}) + \mathrm{Der}_0(R)$. Clearly, C and B'_0 are contained in $C_S(R)$ and hence in $C_S(T)$. By Theorem 2, regular B'-words form a left R-basis of $R\#\mathbf{U}$. Any

regular B'-word is of the form ξW, where ξ is a regular B_0'-word and W is a regular $(B - B_0)$-word. So any $f \in R\#\mathbf{U}$ can be uniquely expressed in the form

$$f = \sum_i \xi_i f_i,$$

where ξ_i ranges over all distinct regular B_0'-words and where $f_i \in R\#\mathbf{U}$ are left R-linear combinations of regular $(B - B_0)$-words. Suppose that $f \in C_S(T)$. Since all ξ_i centralize R, we have for any $r \in R$,

$$0 = fr - rf = \sum_i \xi_i (f_i r - r f_i).$$

Since subwords of regular $(B - B_0)$-words are also regular $(B - B_0)$-words, each $f_i r - r f_i$ is also a left R-linear combination of regular $(B - B_0)$-words. So each $\xi_i(f_i r - r f_i)$ is a left R-linear combination of regular B'-words starting with ξ_i. Since the ξ_i are distinct for distinct i, so are the B'-words involved in $\xi_i(f_i r - r f_i)$. It follows that $f_i r - r f_i = 0$ for all i and all $r \in T$. That is, $f_i \in C_S(T)$ for all i. All f_i's are left R-linear combinations of regular $(B - B_0)$-words. It thus suffices to show that for any left R-linear combination g of regular $(B - B_0)$-words, if $g \in C_S(T)$, then $g \in C$. So consider such a g and write it as a left R-linear combination of distinct regular $(B - B_0)$-words W_i:

$$g = a_1 W_1 + a_2 W_2 + \cdots, \qquad \text{where } a_i \in R.$$

If W_i has the maximal length among all $W_1, W_2, \ldots$, then for any $r \in T$,

$$0 = gr - rg = (a_i r - r a_i) W_i + \cdots,$$

where the dots denote a left R-linear combination of regular $(B - B_0)$-words distinct from W_i. So $a_i r - r a_i = 0$ for any $r \in T$. That is, the inner derivation $\mathrm{ad}(a_i)$ vanishes on T and hence on R by our assumption of T. That is, $a_i \in C$. Let us assume that W_1 is the $<$-maximum among all W_i. If $W_1 \neq \emptyset$, then write

$$W_1 = b_1^{n_1} b_2^{n_2} \cdots b_s^{n_s},$$

where $b_i \in B - B_0$ satisfy $b_1 < b_2 < \cdots < b_s$ and where $0 < n_i < p$ for each i in the case of $\operatorname{char} k = p \geq 2$. Suppose that

$$W_j = b_1^{n_1 - 1} b_2^{n_2} \cdots b_s^{n_s} \qquad \text{for some } j.$$

Also, assume that $W_2, \ldots, W_m$ enumerate all those W_i of maximal length such that $W_i = d_i W_j = d_i b_1^{n_1 - 1} b_2^{n_2} \cdots b_s^{n_s}$ for some $d_i \in B - B_0 - \{b_1\}$. Recall that $\phi : h \in C\mathfrak{g} \mapsto \delta_h \in \mathrm{Der}_k(R)$ denotes the left C-linear map extending the Lie k-algebra homomorphism $\mathfrak{g} \to \mathrm{Der}_k(R)$. The left coefficient of $b_1^{n_1 - 1} b_2^{n_2} \cdots b_s^{n_s}$ in $gr - rg$ is then given by

$$n_1 a_1 \delta_{b_1}(r) + \sum_{i=2}^{m} a_i \delta_{d_i}(r) + a_j r - r a_j.$$

We have seen that $a_i \in C$ for $i = 0, 1, \ldots, m$. So the above expression defines a derivation in $C\phi(\mathfrak{g}) + \mathrm{Der}_0(R)$. Since g centralizes T, the above expression vanishes for $r \in T$ and hence for $r \in R$ by our assumption of T. So we have

$$n_1 a_1 \delta_{b_1} + \sum_{i=2}^{m} a_i \delta_{d_i} + \mathrm{ad}(a_j) = 0.$$

So $n_1a_1b_1 + \sum_{i=2}^{m} a_id_i$ falls in $C\mathfrak{g}_0$ and hence can be expressed as a C-linear combination of B_0'. But $b_1, d_2, \ldots, d_m \in B - B_0$, implying $n_1a_1 = 0$. Also, n_1 is invertible in R. So $a_1 = 0$, a contradiction. (1) is thus proved. By $(*)$, any regular B'-word can be uniquely written as a product ξW, where ξ is a regular B_0'-word and W is a regular $(B - B_0)$-word. By Theorem 2, these words ξW form a left R-basis of $R\#\mathbf{U}$. Since V is a C-basis of R, the set $v\xi W$, where $v \in V$, ξ is a regular B_0'-word and W is a regular $(B - B_0)$-word, forms a C-basis of $R\#\mathbf{U}$. But $v\xi W = \xi vW$, since ξ centralizes R. So (2) follows. As right $C_S(R)$-modules, $S = \bigoplus_i C_S(R)g_i$, where g_i enumerate $\mathbb{B}$. So

$$S \underset{C_S(R)}{\otimes} S = S \underset{C_S(R)}{\otimes} \Big(\bigoplus_i C_S(R)g_i \Big) = \bigoplus_i S \underset{C_S(R)}{\otimes} g_i.$$

So (3) follows. □

3. Ore extensions

Given a set X of noncommuting indeterminates, finite or infinite, and a map $\phi : X \to \mathrm{Der}(R)$, write $\delta_x \overset{\text{def.}}{=} \phi(x)$ for brevity. Let $R[X;\phi]$ denote the ring of polynomials in indeterminates $x \in X$ and with coefficients in R subjected to the following commutation rule for $a \in R$ and $x \in X$:

$$xa = ax + \delta_x(a), \text{ where } \delta_x = \phi(x) \in \mathrm{Der}(R).$$

We call $R[X;\phi]$ the Ore extension of R by ϕ. (See [3, 15, 14].) We stress here that the indeterminates $x \in X$ do not commute with each other and that the map ϕ may *not* be injective. So distinct $x \in X$ can be associated with the same derivation.

In traditional notation, we enumerate X as a sequence x_i, $i = 0, 1, \ldots$, and let D be the corresponding sequence $\delta_i \overset{\text{def.}}{=} \phi(x_i) = \delta_{x_i} \in \mathrm{Der}(R)$, $i = 0, 1, \ldots$. In this way, the map ϕ is explicitly encoded in the two corresponding sequences X and D. We can thus denote $R[X;\phi]$ by $R[X;D]$. Ore extensions are also called skew polynomial rings, which has become one of the most basic and useful constructions in ring theory. This topic has been extensively studied in various directions for a few decades.

Here are some interesting special instances of $R[X;D]$: If X is a singleton, say $X = \{x\}$, then $R[X;\phi]$ is commonly written as $R[x;\delta]$, where $\delta \overset{\text{def.}}{=} \phi(x) \in \mathrm{Der}(R)$. This is the most extensively investigated Ore extension. If δ happens to be the zero derivation, then $R[x;\delta]$, usually written as $R[x]$ and called the polynomial ring in x over R, is merely the ring R adjoined by the indeterminate x which commutes with R. More generally, if $\phi(x) = 0$ for $x \in X$, then the Ore extension $R[X;\phi]$, usually denoted by $R\langle X\rangle$ and called the free algebra generated by X over R, is simply the ring R adjoined by the indeterminates $x \in X$ which all commute with R but which do *not* commute with each other.

Let R be an associative k-algebra and $\phi : X \to \mathrm{Der}_k(R)$. Let $\mathfrak{g}_X$ be the Lie k-algebra generated by X in $R[X;\phi]$. (So $\mathfrak{g}_X$ is a restricted p-Lie k-algebra if $\mathrm{char}\, R = p \geq 2$ by our convention.) Clearly, $\mathfrak{g}_X$ is the free Lie k-algebra generated by X. By [12] or [11], the universal enveloping algebra of $\mathfrak{g}_X$ is $k\langle X\rangle$, the free associative k-algebra generated by X. This is also contained in $R[X;\phi]$. The map $\phi : X \to \mathrm{Der}_k(R)$ extends to a unique Lie k-algebra homomorphism $\mathfrak{g}_X \to \mathrm{Der}_k(R)$ by the freedom of $\mathfrak{g}_X$ on the generator set X and then to a k-algebra homomorphism $k\langle X\rangle \to \mathrm{End}_k(R)$ by the freedom of $k\langle X\rangle$. With the map thus extended, which

we also denoted by ϕ, R is a $k\langle X\rangle$-module algebra. It was pointed out to us by the referee of [14] that the Ore extension $R[X;\phi]$ can be interpreted as a smash product as the following.

Lemma 4. *In the context above, the Ore extension $R[X;\phi]$ is canonically isomorphic with the smash product $R\#k\langle X\rangle$ via the map $a \mapsto a\#1$ for $a \in R$ and $x \mapsto 1\#x$ for $x \in X$.*

Proof. For $a \in R$ and $x \in X$, write $\delta_x \stackrel{\text{def.}}{=} \phi(x)$ and we have

$$(1\#x)(a\#1) = a\#x + \phi(x)(a)\#1 = a\#x + \delta_x(a)\#1.$$

So $a \mapsto a\#1$ for $a \in R$ and $x \mapsto 1\#x$ for $x \in X$ induces a surjective k-algebra homomorphism $R[X;\phi] \to R\#k\langle X\rangle$. Suppose that $f \in R[X;\phi]$ is in the kernel of the above k-algebra homomorphism. Write $f = \sum_i a_i w_i$, where $a_i \in R$ and where w_i are distinct words in X. Then $0 = \sum_i a_i\#w_i = \sum_i a_i \otimes_k w_i$. The distinct words w_i, as elements of $k\langle X\rangle$, are k-independent. So $\sum_i a_i\#w_i = 0$, which is the same as $\sum_i a_i \otimes_k w_i = 0$, implies each $a_i = 0$, that is, $f = \sum_i a_i w_i = 0$. So the k-algebra homomorphism $R[X;\phi] \to R\#k\langle X\rangle$ defined above is actually a k-algebra isomorphism, as expected. □

Let R be a ring with the center C, which forms a field. Clearly, $\delta(C) \subseteq C$ for any $\delta \in \mathrm{Der}(R)$. Given a map $\phi : X \to \mathrm{Der}(R)$, where X is a set of indeterminates, write $\delta_x \stackrel{\text{def.}}{=} \phi(x)$ for $x \in X$ and define

$$C^{(\phi)} \stackrel{\text{def.}}{=} \{\alpha \in C : \delta_x(\alpha) = 0 \text{ for any } x \in X\}.$$

Clearly, $C^{(\phi)}$ is a subfield of C. Let k be any subfield of $C^{(\phi)}$. The simplest choice of k is the prime subfield of C. Then $\phi(x) \stackrel{\text{def.}}{=} \delta_x \in \mathrm{Der}_k(R)$ for $x \in X$. By Lemma 4, $R[X;\phi]$ is canonically isomorphic to the smash product $R\#k\langle X\rangle$. With this, we are able to apply Theorems 2 and 3 to the Ore extension $R[X;\phi]$. For the convenience of later applications, we recall Definition 4 and Theorems 2 and 3 in the context of Ore extensions as follows.

Definition 5. Let R be a ring with the center C being a field. In the Ore extension $R[X;\phi]$, let $\mathfrak{g}$ be the free Lie algebra generated by X over the prime field of C and let $h \in C\mathfrak{g} \mapsto \delta_h \in \mathrm{Der}(R)$ be the left C-linear Lie map extending the map $\phi : X \to \mathrm{Der}(R)$. Let $\mathfrak{g}_0$ be the C-space of $h \in \mathfrak{g}$ such that $\delta_h \in \mathrm{Der}_0(R)$. Let B be a C-basis of $C\mathfrak{g}$ such that $B_0 \stackrel{\text{def.}}{=} B \cap \mathfrak{g}_0$ forms a C-basis of $\mathfrak{g}_0$. For $h \in B_0$, choose $a_h \in R$ such that $\delta_h = \mathrm{ad}(a_h)$. Define $B_0' \stackrel{\text{def.}}{=} \{h - a_h : h \in B_0\}$ and $B' \stackrel{\text{def.}}{=} B_0' \cup (B - B_0)$. Let $<$ be a linear order of B' such that $h < g$ for $h \in B_0'$ and $g \in B - B_0$. We call B' so ordered a *regular Lie basis* of the Ore extension $R[X;\phi]$.

Theorem 5. *Let R be a ring with the center C being a field. Set $S \stackrel{\text{def.}}{=} R[X;\phi]$. Let B' be a regular Lie basis of S and retain the notation of Definition 5. We have the following:*

(1) *Regular B'-words form an R-basis of $R[X;\phi]$.*

(2) *For $T \subseteq R$, $C_S(T) = C_S(R)$ iff for any $\delta \in C\phi(\mathfrak{g}) + \mathrm{Der}_0(R)$, $\delta(T) = 0$ implies $\delta(R) = 0$.*

(3) *The set of regular B_0'-words forms a C-basis of the free C-module $C_S(R)$. For any C-basis V of R, the set*

$$\mathbb{B} \stackrel{\text{def.}}{=} \{vW : v \in V \text{ and } W \text{ is a regular word in } B - B_0\}$$

forms a $C_S(R)$-basis of the free $C_S(R)$-module S.

(4) *Any element of $S \otimes_{C_S(R)} S$ can be uniquely expressed in the form $\sum_i f_i \otimes g_i$, where $f_i \in S$ and where $g_i \in \mathbb{B}$ are distinct.*

Proof. (1) follows by Theorem 2 and the rest by Theorem 3. □

It is interesting to see the special instance of Theorem 5 for $X = \{x\}$. This has already generalized all the known results in the literature, in which R has to be simple [1] or prime [9]. Ours is true for any ring R with the center C being a field.

Corollary 6. *Consider the Ore extension $S \stackrel{\text{def.}}{=} R[x;\delta]$, where $\delta \in \operatorname{Der}(R)$ and where R is a ring with the center C being a field. Set $C^{(\delta)} \stackrel{\text{def.}}{=} \{\alpha \in C : \delta(\alpha) = 0\}$. Let Z_S denote the center of S.*

(1) $\operatorname{char} R = 0$*: If δ is inner, say $\delta = \operatorname{ad}(a)$, where $a \in R$, then $C_S(R) = Z_S = C[\xi]$, where $\xi \stackrel{\text{def.}}{=} x - a$. Otherwise, $C_S(R) = C$ and $Z_S = C^{(\delta)}$.*

(2) $\operatorname{char} R = p \geq 2$*: Assume that there exist $\alpha_i \in C^{(\delta)}$ and $a \in R$ such that*

$$\delta^{p^s} + \alpha_1 \delta^{p^{s-1}} + \cdots + \alpha_s \delta = \operatorname{ad}(a). \tag{$\dagger$}$$

Let $s \geq 0$ above be the minimal such integer. Then $C_S(R) = C[\xi]$, where $\xi \stackrel{\text{def.}}{=} x^{p^s} + \alpha_1 x^{p^{s-1}} + \cdots + \alpha_s x - a$. If $\delta(a) \in \delta(C)$, say $\delta(a) = \delta(\alpha)$, where $\alpha \in C$, then $Z_S = C^{(\delta)}[\xi + \alpha]$. If $\delta(a) \notin \delta(C)$, then $Z_S = C^{(\delta)}[\xi^p]$. If δ does not *satisfy any identities of the form ($\dagger$), then $C_S(R) = C$ and $Z_S = C^{(\delta)}$.*

Proof. We retain the notation of Theorem 5. Let k be the prime field of C. For the case $\operatorname{char} R = 0$, the Lie ring $\mathfrak{g}$ generated by kx is kx itself. If $\delta = \operatorname{ad}(a)$ for some $a \in R$, then $\mathfrak{g}_0 = \mathfrak{g} = Cx$ and $C_S(R) = C[\xi]$, where $\xi \stackrel{\text{def.}}{=} x - a$, follows from Theorem 5 by letting $B_0' \stackrel{\text{def.}}{=} \{\xi\}$. Since $C_S(R) \supseteq Z_S \supseteq C[\xi]$, we have $C[\xi] = Z_S$. If δ is outer, then $\mathfrak{g}_0 = 0$ and $C_S(R) = C$ follows from Theorem 5 by letting $B_0' \stackrel{\text{def.}}{=} \emptyset$. For the case $\operatorname{char} R = p \geq 2$, the Lie ring $\mathfrak{g}$ generated by kx is $\bigoplus_{0 \leq j} kx^{p^j}$, and $C\mathfrak{g} = \bigoplus_{0 \leq j} Cx^{p^j}$, the left C-space spanned by $\{x^{p^j} : j \geq 0\}$. Suppose that δ satisfies ($\dagger$) with s being the minimum. Set $y \stackrel{\text{def.}}{=} x^{p^s} + \alpha_1 x^{p^{s-1}} + \cdots + \alpha_s x$. Clearly,

$$\mathfrak{g} = \bigoplus_{0 \leq j} Cx^{p^j} = \bigoplus_{0 \leq j < s} Cx^{p^j} \oplus \bigoplus_{0 \leq t} Cy^{p^t}.$$

By the minimality of s, $\mathfrak{g}_0 = \bigoplus_{0 \leq t} Cy^{p^t}$. So $\mathfrak{g}_0$ has the left C-basis $B_0 \stackrel{\text{def.}}{=} \{y^{p^t} : t \geq 0\}$. Clearly, $\delta_{y^{p^t}} = \operatorname{ad}(a^{p^t})$. Set $B_0' \stackrel{\text{def.}}{=} \{y^{p^t} - a^{p^t} : t \geq 0\}$ and $\xi \stackrel{\text{def.}}{=} y - a$. Since $ya = ay$, we have $y^{p^t} - a^{p^t} = \xi^{p^t}$. So $B_0' = \{\xi^{p^t} : t \geq 0\}$. Order B_0' linearly by setting $\xi < \xi^p < \xi^{p^2} < \cdots$. Regular B_0' words consist of ξ^n, $n \geq 0$. So $C_S(R) = C[\xi]$ follows by Theorem 5. Since S is generated by R and x, we have $Z_S = \{f \in C_S(R) : [f, x] = 0\}$. For $\alpha \in C$, $\delta\alpha = \alpha\delta + \delta(\alpha)$. With this, we multiply

(†) by δ from the left-hand sides, from the right-hand sides, and then take their difference. This yields

$$\delta(\alpha_1)\delta^{p^{s-1}} + \cdots + \delta(\alpha_s)\delta = \mathrm{ad}(\delta(a)).$$

This implies $\delta(\alpha_i) = 0$ and $\delta(a) \in C$ by the minimality of s. With this,

$$[\xi, x] = [y - a, x] = \delta(\alpha_1)x^{p^{s-1}} + \cdots + \delta(\alpha_s)x - \delta(a) = -\delta(a).$$

Assume $\delta(a) \in \delta(C)$, say $\delta(a) = \delta(\alpha)$, where $\alpha \in C$. Then $[\xi + \alpha, x] = -\delta(a) + \delta(\alpha) = 0$, implying $\xi + \alpha \in Z_S$. Since $C_S(R) = C[\xi] = C[\xi + \alpha]$, $Z_S = C^{(\delta)}[\xi + \alpha]$. Assume $\delta(a) \notin \delta(C)$. Since $\delta(a) \in C$, we have $[\xi^p, x] = p\xi^{p-1}\delta(a) = 0$. Any $f \in C_S(R)$ can be written uniquely in the form

$$f = a_0(\xi) + a_1(\xi)\xi^p + a_2(\xi)\xi^{p^2} + \cdots,$$

where each $a_i(\xi) \in C[\xi]$ has ξ-degree $< p$. So $f \in Z_S$ iff $0 = [f, x] = [a_0(\xi), x] + [a_1(\xi), x]\xi^p + [a_2(\xi), x]\xi^{p^2} + \cdots$, iff $[a_i(\xi), x] = 0$ for each i. Write $a_i(\xi) = \sum_{j=0}^{t} \beta_j \xi^j$, where $0 \le j \le t < p$, $\beta_j \in C$ and $\beta_t \neq 0$. We have

$$\begin{aligned}
[a_i(\xi), x] &= \sum_{j=0}^{t} [\beta_j, x]\xi^j + \sum_{j=1}^{t} \beta_j [\xi^j, x] \\
&= -\sum_{j=0}^{t} \delta(\beta_j)\xi^j - \sum_{j=1}^{t} j\delta(a)\beta_j \xi^{j-1} \\
&= -\sum_{j=0}^{t-1} (\delta(\beta_j) + (j+1)\delta(a)\beta_{j+1})\xi^j - (\delta(\beta_t))\xi^t.
\end{aligned}$$

Suppose $[a_i(\xi), x] = 0$. Then $\delta(\beta_t) = 0$ and $\delta(\beta_{t-1}) + t\delta(a)\beta_t = 0$. If $t > 0$, then $\delta(a) = \frac{-\delta(\beta_{t-1})}{t\beta_t} = -\delta(\frac{\beta_{t-1}}{t\beta_t}) \in \delta(C)$, contradicting our assumption. So $t = 0$ and $a_i(\xi) = \beta_0 \in C^{(\delta)}$. We have thus shown that $f \in Z_S$ implies $f \in C^{(\delta)}[\xi^p]$. Clearly, $f \in C^{(\delta)}[\xi^p]$ implies $f \in Z_S$. So $Z_S = C^{(\delta)}[\xi^p]$ follows. □

4. Differential identities

A differential identity of R is an equality

$$\sum_i \sum_j a_{ij} w_i(r) b_{ij} = 0 \qquad \forall r \in R,$$

where $a_{ij}, b_{ij} \in R$ and where w_i are compositions of derivations of R. In the Ore extension $R[X; \phi]$, write $\phi(x) = \delta_x$ for $x \in X$. For $r \in R$,

$$\begin{aligned}
\delta_x(r) = [x, r] &\overset{\text{def.}}{=} xr - rx, \\
\delta_y\delta_x(r) &= [y, [x, r]], \\
&\cdots\cdots
\end{aligned}$$

In this way, a differential identity involving derivations in $\phi(X)$ can be put in the form

$$\sum_i f_i r g_i = 0 \qquad \forall r \in R,$$

where $f_i, g_i \in R[X; \phi]$. We will prove the following.

Theorem 7. *Let R be a prime ring and Q its symmetric Martindale quotient ring. Set $S \overset{\text{def.}}{=} Q[X;\phi]$ and*

$$C_S(R) \overset{\text{def.}}{=} \{f \in S : fr = rf \text{ for } r \in R\}.$$

Given $f_i, g_i \in S$, $\sum_i f_i r g_i = 0$ for all $r \in R$ iff $\sum_i f_i \underset{C_S(R)}{\otimes} g_i = 0$.

We recall some notation from [6] and [7]. Let Q^{op} denote the opposite ring of Q and let $\mathbb{Z}$ be the ring of integers. The tensor product $Q \otimes_{\mathbb{Z}} Q^{\text{op}}$ consists of elements in the form $\sum_i r_i \otimes r_i'$, where $r_i \in Q$ and $r_i' \in Q^{\text{op}}$. For $f \in S$ and $\beta = \sum_i r_i \otimes r_i' \in Q \otimes_{\mathbb{Z}} Q^{\text{op}}$, we define

$$f \cdot \beta \overset{\text{def.}}{=} \sum_i r_i' f r_i.$$

Let L denote the subring of $Q \otimes_{\mathbb{Z}} Q^{\text{op}}$ generated by the elements of the form $r \otimes r'$ for all $r, r' \in R \cup \{1\}$. Thus we can regard S as a right L-module. For a subset $Y \subseteq S$, we define

$$Y^{\perp} \overset{\text{def.}}{=} \{\beta \in L \mid f \cdot \beta = 0 \text{ for all } f \in Y\}.$$

Note that $Y^{\perp}$ is an (R,R)-submodule of L. On the other hand, for $U \subseteq L$, we define

$$U^{\perp} \overset{\text{def.}}{=} \{f \in S \mid f \cdot \beta = 0 \text{ for all } \beta \in U\}.$$

We need the following.

Lemma 8 (Lemma 4 [5])**.** *Let C denote the extended centroid of R. Given finitely many $a_1, \ldots, a_n \in Q$, we have*

$$(Ca_1 + \cdots + Ca_n)^{\perp\perp} = a_1 C_S(R) + \cdots + a_n C_S(R).$$

We are ready for

Proof of Theorem 7. The implication $\Leftarrow$ is obvious. For the implication $\Rightarrow$, we apply Theorem 5. It is well known that any derivation of R can be uniquely extended to Q. So any derivation of Q vanishing on R must also vanish on Q. So $C_S(R) = C_S(Q)$ by Theorem 5. Let C denote the extended centroid of R, which is defined to be the center of Q. Fix a C-basis V of Q. By Theorem 5, the set of regular B'-words forms a right Q-basis of S, the set of regular B_0'-words forms a C-basis of $C_S(R)$ and the set

$$\mathbb{B} \overset{\text{def.}}{=} \{vU : v \in V \text{ and } U \text{ is a regular word in } B - B_0\}$$

forms a basis of the free $C_S(R)$-module S. Let $g_1, g_2, \ldots$ enumerate elements of $\mathbb{B}$. By (4) of Theorem 5, we have for any $f_i \in S$,

$$\sum_i f_i \underset{C_S(R)}{\otimes} g_i = 0 \;\Leftrightarrow\; \text{all } f_i = 0.$$

Assume on the contrary that there exist $0 \neq f_i \in Q[X;\phi]$, and $g_i \in \mathbb{B}$ such that

$$(\ddagger) \qquad \sum_i f_i r g_i = 0 \qquad \text{for all } r \in R.$$

Fix arbitrarily a linear order $\preceq$ of X-words such that

$$\text{short word} \prec \text{long word}.$$

The $\preceq$-leading word of $0 \neq f \in S$ is the $\preceq$-maximal word occurring nontrivially in f. By the $\preceq$-leading word of (‡), we mean the $\preceq$-maximum of $\preceq$-leading words of nonzero f_i's. We may further choose (‡) so that that its $\preceq$-leading word W is minimal possible. For each i, write

$$f_i = a_i W + \cdots .$$

For $\beta \in \bigcap_i a_i^{\perp}$, each $f_i \cdot \beta$ has $\preceq$-leading word $< W$. We easily see $\sum_i (f_i \cdot \beta) r g_i = 0$ for all $r \in R$. By the $\preceq$-minimality of (‡), we have $f_i \cdot \beta = 0$. So $\beta \in \bigcap_i a_i^{\perp}$ implies $f_i \cdot \beta = 0$. By Lemma 8, $f_i \in \sum_j a_j C_S(R)$. Let ξ_j enumerate regular B_0'-words. We may thus write

$$f_i = \sum_j b_{ij} \xi_j, \qquad \text{where } b_{ij} \in Q.$$

With this, rewrite (‡) as

$$0 = \sum_i \sum_j b_{ij} \xi_j r g_i = \sum_i \sum_j b_{ij} r \xi_j g_i \qquad \text{for all } r \in R.$$

Let $v_1, v_2, \ldots$ enumerate V and $U_1, U_2, \ldots$ enumerate regular B'-words. Each $g_i \in \mathbb{B}$ can be written uniquely as $g_i = v_s U_t$. We re-index the corresponding b_{ij} as b_{stj} if $g_i = v_s U_t$. So

$$0 = \sum_{s,t} \sum_j b_{stj} r \xi_j v_s U_t = \sum_{s,t,j} b_{stj} r v_s \xi_j U_t \qquad \text{for all } r \in R.$$

Distinct ordered pairs (j,t) correspond to distinct regular B'-words $\xi_j U_t$ and these regular B'-words form a right R-basis of S. So for a fixed ordered pair (j,t),

$$0 = \sum_s b_{stj} r v_s.$$

But $V = \{v_1, v_2, \ldots\}$ forms a C-basis of Q. By the well-known Martindale's lemma, $b_{stj} = 0$. This is true for all s, t, j. So all $b_{ij} = 0$ and hence $f_i = \sum_j b_{ij} \xi_j = 0$ for all i, contradicting the assumption. □

It is interesting to deduce Kharchenko's Theorem from the above.

Theorem 9 (Lemma 2 [6])**.** *Let R be a prime ring, Q its symmetric Martindale quotient ring and C its extended centroid. Suppose that $\delta_i \in \mathrm{Der}(Q)$, $i = 1, 2, \ldots$, are mutually outer in the sense that given any finite sum $\sum_i \alpha_i \delta_i \in \mathrm{Der}_0(Q)$, where $\alpha_i \in C$, then all $\alpha_i = 0$ follows. Let $<$ linearly order these δ_i. Let w_j enumerate regular words in these δ_i. Given $a_{ij}, b_{ij} \in Q$, if*

$$\sum_{i,j \geq 0} a_{ij} w_j(r) b_{ij} = 0 \qquad \textit{for all } r \in R,$$

then $\sum_i a_{ij} \underset{C}{\otimes} b_{ij} = 0$ for each j.

Proof. Pick a set $X = \{x_1, x_2, \ldots\}$ of indeterminates with the cardinality equal to that of these δ_i. Define $\phi : X \to \mathrm{Der}(Q)$ such that $\phi(x_i) \overset{\text{def.}}{=} \delta_i$. Extend ϕ to X-words by setting

$$\phi(x_{i_1} x_{i_2} \cdots) \overset{\text{def.}}{=} \phi(x_{i_1}) \phi(x_{i_2}) \cdots ,$$

where $x_{i_1}, x_{i_2}, \ldots \in X$. Conversely, given a product (or word) w of derivations in $\mathrm{Der}(Q)$, let $\phi^{-1}(w)$ be the X-word W such that $\phi(W) = w$. Let k be the prime subfield of C and $\mathfrak{g}$ the free Lie algebra generated by X over k. Define

$$\mathfrak{g}_0 = \{h \in C\mathfrak{g} : \phi(h) \in \mathrm{Der}_0(Q)\}.$$

Fix a C-basis B_0 of $\mathfrak{g}_0$. The set $X \cup B_0$ is C-independent by the mutual outerness of $\delta_i \overset{\text{def.}}{=} \phi(x_i)$ and hence can be extended to a left C-basis B of $C\mathfrak{g}$. For $h \in B_0$, pick $a_h \in Q$ such that $\phi(h) = \mathrm{ad}(a_h)$. Set $B_0' \overset{\text{def.}}{=} \{h - a_h\}$. Order X by setting $x_i < x_j$ if $\delta_i < \delta_j$. Extend this order of X to B' such that $h < g$ for $h \in B_0'$ and $g \in B - B_0$. Given a derivation word $w = \cdots \delta_{s_2}\delta_{s_1}$, where $\delta_{s_i} \in \mathrm{Der}(Q)$, write

$$w(r) = [\cdots\cdots[x_{s_2}, [x_{s_1}, r]]\cdots] = \sum_l f_l r g_l,$$

where f_l, g_l are subwords of the word $\phi^{-1}(w) = \cdots x_{s_2}x_{s_1}$. So if w is a regular word in derivations, then f_l, g_l are regular X-words (and hence regular $(B - B_0)$-words, since $X \subseteq B - B_0$). Given $a_{ij}, b_{ij} \in Q$, suppose that

$$\sum_{i,j} a_{ij} w_j(r) b_{ij} = 0 \qquad \text{for all } r \in R.$$

In the way explained above, write this in the form $\sum_l f_l r g_l = 0$, where $f_l, g_l \in S$ involve only regular X-subwords of $\phi^{-1}(w_j)$. By Theorem 7, $\sum_l f_l \otimes g_l = 0$, where $\otimes$ is taken over $C_S(R)$. Since $f_l, g_l \in S$ involve only regular X-subwords of $\phi^{-1}(w_j)$, $\sum_l f_l \otimes g_l$ is a sum of terms of the form

$$aW \otimes bW',$$

where $a, b \in Q$ and where W, W' are regular X-subwords of some $\phi^{-1}(w_j)$. We may assume that w_0 has the maximal length n among all w_i. In $\sum_l f_l \otimes g_l$, the sum of terms involving $W_0 \overset{\text{def.}}{=} \phi^{-1}(w_0)$ is clearly

$$\sum_i a_{i0} W_0 \otimes b_{i0} + (-1)^n \sum_i a_{i0} \otimes b_{i0} W_0.$$

By (4) of Theorem 5, $\sum_i a_{i0} \otimes_C b_{i0} = 0$. On the other hand, $\sum_i a_{i0} \otimes_C b_{i0} = 0$ implies $\sum_i a_{i0} w_0(r) b_{i0} = 0$ for $r \in R$. So we have

$$\sum_{i,j>0} a_{ij} w_j(r) b_{ij} = 0 \qquad \text{for all } r \in R.$$

Apply the same argument to this and continue in this manner. It follows that $\sum_i a_{ij} \otimes_C b_{ij} = 0$ for all j. □

References

[1] S. A. Amitsur, *Derivations in simple rings*, Proc. London Math. Soc. (3) **7** (1957), 87–112. MR0088480 (19:525d)

[2] K. I. Beidar, W. S. Martindale, III, A. V. Mikhalev, "Rings with generalized identities", Monographs and Textbooks in Pure and Applied Mathematics **196**, Marcel Dekker, Inc., New York, 1996. MR1368853 (97g:16035)

[3] V. D. Burkov, *On differentially prime rings*, (Russian) Uspekhi Mat. Nauk **35**(5) (1980), 219–220. (Engl. Transl. *Russian Math. Surveys* 35(5):253–254.) MR595145 (82f:16002)

[4] C.-L. Chuang and Y.-T. Tsai, *Higher derivations of Ore extensions by q-skew derivations*, Journal of Pure and Applied Algebra, **214**(10) (2010), 1778-1786. MR2608105

[5] C.-L. Chuang, T.-K. Lee, C.-K. Liu and Y.-T. Tsai, *Higher Derivations of Ore Extensions*, Israel J. Math **175** (2010), 157–178. MR2607542

[6] V. K. Kharchenko, *Differential identities of prime rings*, (Russian) Algebra i Logika **17**(2) (1978), 220–238. (Engl. Transl., Algebra and Logic **17**(2) (1978), 154–168.) MR541758 (81f:16025)

[7] V. K. Kharchenko, *Differential identities of semiprime rings*, (Russian) Algebra i Logika **18**(1) (1979), 86–119. (Engl. Transl., Algebra and Logic **18**(1) (1979), 58–80.) MR566776 (81f:16052)

[8] A. Leroy and J. Matczuk, *The extended centroid and X-inner automorphisms of Ore extensions*, J. Algebra **145**(1) (1992), 143–177. MR1144664 (93b:16053)

[9] J. Matczuk, *Extended centroids of skew polynomial rings*, Math. J. Okayama Univ. **30** (1988), 13–20. MR976726 (89m:16006)

[10] S. Montgomery, "Hopf algebras and their actions on rings", Regional conference series in mathematics; no. 82, American Mathematical Society, Providence, Rhode Island, 1992. MR1243637 (94i:16019)

[11] C. Reutenauer, "Free Lie algebras", London Mathematical Society monographs; new ser. 7, Oxford: Clarendon Press; New York, Oxford University Press, 1993. MR1231799 (94j:17002)

[12] J.-P. Serre, "Lie algebras and Lie groups: 1964 lectures given at Harvard University", (1992), 2nd ed., Lecture Notes in Mathematics, 1500, Springer-Verlag: Berlin. MR1176100 (93h:17001)

[13] M. E. Sweedler, "Hopf Algebras", Mathematics Lecture Notes Series, 1969, W. A. Benjamin, Inc., New York, 1996. MR0252485 (40:5705)

[14] Y.-T. Tsai and C.-L. Chuang, *Quotient Rings of Ore Extensions with More Than One Indeterminate*, Commun. Algebra **36**(10), (2008), 3608–3615. MR2458396 (2009k:16054)

[15] Y.-T. Tsai, T.-Y. Wu, and C.-L. Chuang, *Jacobson radicals of Ore extensions of derivation type*, Commun. Algebra **35**(3) (2007), 975–982. MR2305244 (2007m:16045)

Department of Mathematics, National Taiwan University, Taipei 106, Taiwan
E-mail address: chuang@math.ntu.edu.tw

Department of Applied Mathematics, Tatung University, Taipei 104, Taiwan
E-mail address: yttsai@ttu.edu.tw