行政院國家科學委員會專題研究計畫　成果報告

常值具多項式恆等式之代數斜導算(3/3)

計畫類別： 個別型計畫
計畫編號： NSC91-2115-M-002-002-
執行期間： 91 年 08 月 01 日至 93 年 07 月 31 日
執行單位： 國立臺灣大學數學系暨研究所

計畫主持人： 李秋坤

報告類型： 完整報告
報告附件： 出席國際會議研究心得報告及發表論文
處理方式： 本計畫可公開查詢

中　華　民　國 93 年 12 月 10 日

NILPOTENT DERIVATIONS

Chen-Lian Chuang and Tsiu-Kwen Lee

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

Abstract. Motivated by Grzeszczuk's paper [9], we give a detailed analysis of nilpotent derivations of semiprime rings. With this, many known results can be either generalized or deduced.

[1]

† 2000 *Mathematics Subject Classification.* 16W20, 16W25, 16W55.

‡ *Key words and phrases.* Nilpotent derivation, (semi-)prime ring, annihilating nilpotency.

Members of Mathematics Division, National Center for Theoretical Sciences at Taipei.∎

§0. Introduction

Throughout, R is always a semiprime ring and Q its symmetric Martindale quotient ring. The center C of Q is called the extended centroid of R. By a derivation of R we mean a map $\delta\colon R \to R$ satisfying

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

For $b \in R$, the map $\mathrm{ad}(b)\colon x \in R \mapsto [x,b] = xb - bx$ defines a derivation of R. A derivation of this form is called inner. More generally, a derivation δ of R is called X-inner if it is the restriction of an inner derivation of Q, that is, if there exists $b \in Q$ such that $x^\delta = [x,b]$ for $x \in R$. An ideal I of R satisfying $I^\delta \subseteq I$ is called a δ-ideal of R. This paper is motivated by Grzeszczuk's paper [9] and the object of our investigation is the following:

Definition 1. ([9]) A derivation δ is called nilpotent if $\delta^n = 0$ for some $n \geq 0$. The least such n is called the nilpotency of δ, denoted by $n_\delta(R)$. The least integer m such that, for each nonzero δ-ideal I of R there exists $0 \neq c \in I$ with $R^{\delta^m} c = 0$, is called the annihilating nilpotency of δ and is denoted by $m_\delta(R)$.

[1]

For a nilpotent derivation δ, any ideal $I \neq 0$ of R contains a δ-ideal $J \neq 0$: We merely set $J \overset{\text{def.}}{=} \sum_{i=0}^{n_\delta(R)-1} (I^n)^{\delta^i}$, where $n \geq n_\delta(R)$. Therefore, $m_\delta(R)$ is also the least integer m such that, for each nonzero ideal I of R, there exists $0 \neq c \in I$ such that $R^{\delta^m} c = 0$. When R is a prime ring, $m_\delta(R)$ is then the least integer m such that $R^{\delta^m} c = 0$ for some nonzero $c \in R$. The annihilating nilpotency of δ is first investigated in [9]; we give it this name for brevity. Nilpotent derivations enjoy many interesting properties and have been studied extensively [3, 5, 6, 9, 15]. When R has a prime characteristic $p \geq 2$, most results impose restrictions on p. Our aim here is to remove these restrictions. Let us briefly illustrate our results: For a prime ring R of $\operatorname{char} R = p \geq 2$, [10, Corollary 3] asserts that a C-algebraic derivation δ of R must satisfy an identity in the following form with s as small as possible:

$$x^{\delta^{p^s}} + \beta_1 x^{\delta^{p^{s-1}}} + \cdots + \beta_s x^\delta = xb - bx,$$

where $\beta_i \in C$ and where $b \in Q$ is C-algebraic. Algebraic properties of δ should be characterized by this identity and by the minimum polynomial of b over C, both of which assume very simple forms for nilpotent δ (Theorems 2.2 and 2.3 below). We justify this point of view by calculating the nilpotency and the annihilating nilpotency of δ in terms of the number p^s and the degree of b over C (Theorems 2.4 and 2.5 below). We then extend these to the semiprime case, which merely says that Q can be decomposed into a finite direct sum $\oplus_i Q_i$ such that the nilpotent derivation restricted to each $Q_i \cap R$ behaves in the same way as in the prime case (Theorems 3.1, 3.2 and 3.3 below). As applications, we give an interesting connection between nilpotency and the annihilating nilpotency (Theorems 3.4 and 3.5 below), which generalizes [3, 5, 9]. Finally, we deduce a result of [9] as a corollary.

We organize this article as follows: In §1 we recall some notions and facts, mainly formulated for semiprime rings, which are either well-known or implicit in the literature. In §2 we consider the prime case which shows the main results of this paper. In §3 we extend our results to semiprime case.

§1. Preliminaries

The section is devoted to some notions and facts about semiprime rings (Theorems 1.1–1.7). They are used only in §3 and can be skipped if the reader is interested only in the prime case. Our ring R is always *semiprime*. It is well-known that a derivation of R can be uniquely extended to a derivation of Q. So all derivations will be assumed to be defined on Q. By a differential polynomial, we mean a generalized polynomial

φ with coefficients in Q and with variables acted by derivations of R. If φ vanishes on R then we call φ a differential identity. The following is actually implicit in [11]. There is a proof [13] in the spirit of the theory of orthogonal completion [2]. We sketch below a short proof following the line of [4]:

Theorem 1.1. *A differential identity φ of R also vanishes on Q.*

Proof. We transform φ into its reduced form φ' by the basic identities on [11, p. 58]. By [11, Theorem 2], φ' is a consequence of a generalized polynomial identity φ'' of R in a specific way. By [1, Theorem 6.4.1], φ'' also vanishes on Q and hence so does φ'. The basic identities also hold for Q by the uniqueness of extension of derivations from R to Q. Our assertion follows from transforming φ' back into φ.

This implies that a nilpotent derivation of R can be extended to a unique nilpotent derivation of Q of the same nilpotency and of the same annihilating nilpotency.

It is shown in [1] that the commutative ring C is a von Neumann regular in the sense that for any $\alpha \in C$, there exists $\beta \in C$ such that $\alpha = \alpha^2\beta$. It is shown in [1] that central idempotents of Q form a complete Boolean algebra B. For any subset T of Q, we define $\mathrm{E}[T]$ to be the smallest central idempotent such that $\mathrm{E}[T]t = t$ for all $t \in T$. (See [1, Lemma 3.1.1]). If $T = \{a\}$, where $a \in Q$, we denote $E[T]$ by $\mathrm{E}[a]$ for brevity. For a derivation δ of Q we write $\mathrm{E}[\delta]$ to stand for $\mathrm{E}[Q^\delta]$. We need the following from [11]:

Theorem 1.2. *For any maximal ideal $\mathcal{A}$ of B, the set $\mathcal{A}Q$ forms a minimal prime ideal of Q. Conversely, any minimal prime ideal of Q admits this form.*

We remark that the intersection of all minimal prime ideals is zero. For a semiprime ring R, C may *not* be a field and we must be careful in extending our notions: We call $a_i \in Q$ $(1 \leq i \leq n)$ C-independent if all $a_i \neq 0$ and for any $\alpha_i \in C$, $\sum_{i=1}^n \alpha_i a_i = 0$ implies that all $\alpha_i a_i = 0$. Analogously, derivations δ_i $(1 \leq i \leq n)$ of R are said to be mutually outer if all $\delta_i \neq 0$ and if for any $b \in Q$ and $\alpha_i \in C$, the identity $\sum_{i=1}^n \alpha_i x^{\delta_i} = xb - bx$ for all $x \in R$ implies $\alpha_1 x^{\delta_1} = \cdots = \alpha_n x^{\delta_n} = 0$ for all $x \in R$. (This is called strongly independent in [11] but we follow [12].) The following is also implicit in [11]. For brevity, we refer its proof to pp. 65–68 of [11].

Theorem 1.3. *Let P be a minimal prime ideal of Q. For $a \in Q$, let $\overline{a}$ denote the natural image of a in $\overline{Q} \overset{\text{def.}}{=} Q/P$. For a derivation δ of Q, let $\overline{\delta}$ denote the derivation of $\overline{Q}$ induced canonically by δ.*

(1) The extended centroid of $\overline{Q}$ is the natural image $\overline{C}$ of C in $\overline{Q}$.

(2) If $a_1, a_2, \dots$ are C-independent, then nonzero $\overline{a}_i$'s are $\overline{C}$-independent.

(3) If derivations $\delta_1, \delta_2, \dots$ of Q are mutually outer, then so are nonzero $\overline{\delta}_i$'s.

Additive endomorphisms of the abelian group $(Q,+)$ form a ring $\mathrm{End}(Q,+)$. Derivations preserve the addition and hence are elements of $\mathrm{End}(Q,+)$. Let $b \in Q$ and δ, a derivation. We compute: for $x \in Q$, $x^{\mathrm{ad}(b)\delta} = [x,b]^\delta = [x^\delta, b] + [x, b^\delta] = (x^\delta)^{\mathrm{ad}(b)} + x^{\mathrm{ad}(b^\delta)} = x^{\delta\,\mathrm{ad}(b) + \mathrm{ad}(b^\delta)}$. We hence have the equality $\mathrm{ad}(b)\delta = \delta\,\mathrm{ad}(b) + \mathrm{ad}(b^\delta)$ in $\mathrm{End}(Q,+)$. We also interpret $\alpha \in C$ as the map $\alpha\colon x \in Q \mapsto x\alpha \in Q$ and, in this sense, α is an additive endomorphism of $(Q,+)$. For $\delta\alpha$ in this order, we have $\delta\alpha\colon x \in Q \mapsto \alpha x^\delta \in Q$. But the map $\alpha\delta$ sends $x \in R$ to $x^{\alpha\delta} \overset{\text{def.}}{=} (x\alpha)^\delta = x^\delta\alpha + x\alpha^\delta = x^{\delta\alpha} + x\alpha^\delta$. So we have the equality $\alpha\delta = \delta\alpha + \alpha^\delta$ in $\mathrm{End}(Q,+)$.

An element $b \in Q$ is said to be integral over C or C-integral if $b^n + \alpha_1 b^{n-1} + \cdots + \alpha_{n-1}b + \alpha_n = 0$ for some integer $n \geq 1$ and $\alpha_i \in C$. The minimal such n is called the integral degree of b. A derivation δ of R is said to be C-integral if there exist $\alpha_1, \dots, \alpha_{n-1} \in C$ such that

$$\delta^n + \delta^{n-1}\alpha_1 + \cdots + \delta\alpha_{n-1} = 0.$$

The least such n is called the integral degree of δ. We have the following

Theorem 1.4. *For $b \in Q$, the derivation* $\mathrm{ad}(b)$ *is C-integral if and only if b is C-integral.*

Proof. Suppose first that b is C-integral. We define the left multiplication ℓ_b and the right multiplication r_b by

$$\ell_b : x \in Q \mapsto bx, \qquad r_b : x \in Q \mapsto xb.$$

Then $\ell_b, r_b \in \mathrm{End}(Q,+)$. Since $\ell_b r_b = r_b \ell_b$ and b is C-integral, we see that the subalgebra over C generated by 1, ℓ_b and r_b is commutative and is a finitely generated module over C. Thus every element in this subalgebra is C-integral. In particular, the element $\mathrm{ad}(b) \overset{\text{def.}}{=} \ell_b - r_b$ is C-integral, as asserted.

Suppose next that $\mathrm{ad}(b)$ is C-integral of degree n. Consider the set

$$\Sigma = \{e \in B \mid (b^n + \sum_{i=1}^{n} \alpha_i b^{n-i})e = 0 \text{ for some } \alpha_i \in C\}.$$

We must show $1 \in \Sigma$. For $g \in B$, if $g \leq e$ for some $e \in \Sigma$, then obviously $g \in \Sigma$. If $e, f \in \Sigma$ are orthogonal, then obviously $e + f \in \Sigma$. This shows that Σ is an ideal of

B. Assume on the contrary that $1 \notin \Sigma$. We then extend Σ to a maximal ideal $\mathcal{A}$ of B. By (1) of Theorem 1.3, the extended centroid of $Q/\mathcal{A}Q$ is the natural image $\overline{C}$ of C. In $Q/\mathcal{A}Q$, $\mathrm{ad}(\bar{b})$ is also $\overline{C}$-integral and has the integral degree $\leq n$. Expanding this integral relation of degree $\leq n$ into a linear GPI and then applying [14, Theorem 2], we conclude that the elements $\bar{1}, \bar{b}, \cdots, \bar{b}^n$ are $\overline{C}$-dependent. So there exist $\alpha_i \in C$ such that $b^n + \sum_{i=1}^n \alpha_i b^{n-i} \in \mathcal{A}Q$. That is, $(b^n + \sum_{i=1}^n \alpha_i b^{n-i})(1-e) = 0$ for some $e \in \mathcal{A}$. This says $1 - e \in \Sigma \subseteq \mathcal{A}$. But $e \in \mathcal{A}$. So $1 = e + (1-e) \in \mathcal{A}$, a contradiction.

Let $b \in Q$ be C-integral. By the minimum polynomial of $b \in Q$ over C, we mean an identity relation $b^n + \alpha_1 b^{n-1} + \cdots + \alpha_{n-1} b + \alpha_n = 0$, where $\alpha_i \in C$ and where $1, b, \ldots, b^{n-1}$ are C-independent. Minimum polynomials of $b \in Q$, if they exist, are unique in the following sense: If $b^n + \alpha_1 b^{n-1} + \cdots + \alpha_{n-1} b + \alpha_n = 0$ and $b^m + \beta_1 b^{m-1} + \cdots + \beta_{m-1} b + \beta_m = 0$ are both minimum polynomials of b over C, then $n = m$ and $\alpha_i b^{n-i} = \beta_i b^{n-i}$ for $i = 1, \ldots, n$. It is *not* true that any C-integral $b \in Q$ has a minimum polynomial. We need the following more precise description:

Theorem 1.5. *Let $b \in Q$ be a C-integral element of degree n. Then there exist finitely many integers t_i with $1 \leq t_i \leq n$ and orthogonal $g_i \in B$ $(i = 1, \ldots, k)$ with $\sum_{i=1}^k g_i = 1$ such that the following hold:*

(1) bg_i has the minimal polynomial of degree t_i.

(2) $\mathrm{E}[b^j g_i] = g_i$ for $j = 0, 1, \cdots, t_i - 1$.

Proof. We define D_t to be the set of $e \in B$ such that $\mathrm{E}[b^i] \geq e$ for $0 \leq i < t$ and such that $b^i e$ $(0 \leq i < t)$ are C-independent. If $0 \neq f \in B$ and $f \leq e$ for some $e \in D_t$, then obviously $f \in D_t$. Let $e_t \overset{\text{def.}}{=} \bigvee D_t$. Note $e_t = 0$ if and only if $D_t = \emptyset$. We *claim* that if $e_t \neq 0$, then $e_t \in D_t$: Obviously, $E[b^i] \geq e_t$ and particularly $b^i e_t \neq 0$ for $0 \leq i < t$. Suppose $\sum_{i=0}^{t-1} \alpha_i b^i e_t = 0$ for some $\alpha_i \in C$. Multiplying the equality by any given $e \in D_t$ and using $ee_t = e$, we see that $\sum_{i=0}^{t-1} \alpha_i b^i e = 0$. These $b^i e$ are C-independent, since $e \in D_t$. So all $\alpha_i b^i e = 0$. This is true for all $e \in D_t$ and hence for $e_t \overset{\text{def.}}{=} \bigvee D_t$. So $\alpha_i b^i e_t = 0$. This shows the C-independence of $b^i e_t$ $(0 \leq i < t)$. So $e_t \in D_t$, as claimed.

Let n be the C-integral degree of b. If $t > n$, then for any $e \in D_t$, $e, eb, \ldots, eb^n$ are not C-independent. So $D_t = \emptyset$ for $t > n$. Set $D_0 \overset{\text{def.}}{=} B$ and $e_0 \overset{\text{def.}}{=} 1$. Since $D_0 \supseteq D_1 \supseteq \cdots \supseteq D_{n+1} = \emptyset$, we have $e_0 \geq e_1 \geq \cdots \geq e_n \geq e_{n+1} = 0$. Set $\hat{e}_t \overset{\text{def.}}{=} e_t - e_{t+1}$ for $0 \leq t \leq n$. Define $\tilde{D}_t$ to be the set consisting of central idempotents $e \leq \hat{e}_t$ such that $(b^t + \sum_{i=1}^t \alpha_i b^{t-i})e = 0$ for some $\alpha_i \in C$. If $f \in B$ and $f \leq e$ for some $e \in \tilde{D}_t$, then obviously $f \in \tilde{D}_t$. Set $\tilde{e}_t \overset{\text{def.}}{=} \bigvee \tilde{D}_t$. Write $\tilde{e}_t = \bigvee_{\nu \in I} f_\nu$, where

$\{f_\nu \mid \nu \in I\}$ is an orthogonal subset of $\tilde{D}_t$. For each $\nu \in I$, we have

$$b^t f_\nu + \alpha_{\nu 1} b^{t-1} f_\nu + \cdots + \alpha_{\nu t} = 0$$

for some $\alpha_{\nu i} \in C$. By the orthogonal completeness of C, for each i with $1 \leq i \leq t$ there exists $\alpha_i \in C$ such that $\alpha_i f_\nu = \alpha_{\nu i} f_\nu$ for all $\nu \in I$ and $\alpha_i(1 - \tilde{e}_t) = 0$. Applying the orthogonal completeness of Q, we obtain that

$$b^t \tilde{e}_t + \alpha_1 b^{t-1} \tilde{e}_t + \cdots + \alpha_t = 0.$$

Therefore, $\tilde{e}_t \in \tilde{D}_t$ follows. Of course, we have $\tilde{e}_t \leq \hat{e}_t$.

We claim next that $\tilde{e}_t = \hat{e}_t$. Otherwise, $f \overset{\text{def.}}{=} \hat{e}_t - \tilde{e}_t \neq 0$. Notice that

$$0 \neq f = \hat{e}_t - \tilde{e}_t = \hat{e}_t(1 - \tilde{e}_t) = e_t(1 - e_{t+1})(1 - \tilde{e}_t).$$

If $f \in D_{t+1}$, then $f \leq e_{t+1}$ and so $f = 0$, a contradiction. Therefore, $f \in D_t \setminus D_{t+1}$. Notice that $\mathrm{E}[b^i] \geq e_t \geq f$ for $0 \leq i \leq t-1$.

If $g \overset{\text{def.}}{=} f(1 - \mathrm{E}[b^t]) \neq 0$, then $gb^t = 0$. Since $g \leq \hat{e}_t$, this implies that $g \in \tilde{D}_t$ and so $g \leq \tilde{e}_t$. But then $g = g\tilde{e}_t = gf\tilde{e}_t = 0$, a contradiction. Therefore, we have $\mathrm{E}[b^t] \geq f$ and, particularly, $b^i f \neq 0$ for $0 \leq i \leq t$. Since $f \notin D_{t+1}$, $b^i f$ $(0 \leq i \leq t)$ cannot be C-independent. Thus there exist $\alpha_i \in C$ such that

$$\alpha_0 b^t f + \alpha_1 b^{t-1} f + \cdots + \alpha_{t-1} bf + \alpha_t f = 0$$

and such that $\alpha_i b^{t-i} f \neq 0$ for some $i \leq t$. We have $\alpha_0 b^t f \neq 0$, for otherwise the elements $b^{t-1}f, \ldots, bf, f$ would not be C-independent, contradicting the fact that $f \in D_t$. By abelian regularity of C ([1, Theorem 2.3.9]), there exists $\beta \in C$ such that $(f\alpha_0)^2\beta = f\alpha_0$. Since $e \overset{\text{def.}}{=} f\alpha_0\beta \in B$ and $0 < e \leq f$, we multiply the above equality by βe and obtain $eb^t \in \sum_{i=1}^{t} Ceb^{t-i}$. This implies that $e \in \tilde{D}_t$ and so $e \leq \tilde{e}_t$. But $e \leq f \overset{\text{def.}}{=} \hat{e}_t - \tilde{e}_t$, a contradiction. So $f = 0$ follows, that is, $\tilde{e}_t = \hat{e}_t$.

So b satisfies an identity $b^t\hat{e}_t + \sum_{i=1}^{t} \alpha_i b^{t-i}\hat{e}_t = 0$, where $\alpha_i \in C$. This is the minimum polynomial of $b\hat{e}_t$, since the elements $b^i\hat{e}_t$, where $0 \leq i < t$, are C-independent by the fact that $\hat{e}_t \in D_t$. Note that $\mathrm{E}[b^i\hat{e}_t] = \hat{e}_t$ for $0 \leq i < t$. We set $g_t = \hat{e}_t$ for $t = 1, 2, \cdots, n$. Then the central idempotents g_i, where $1 \leq i \leq n$, are pairwise orthogonal and $\sum_{i=1}^{n} g_i = 1$. This completes our proof.

For the case $\mathrm{char}\, R = 0$, it is proved in [11] that every C-integral derivation of R is X-inner. For the case $\mathrm{char}\, R = p \geq 2$, the corresponding result is [10, Corollary 3], which is for prime rings only. We need the following more detailed information:

Theorem 1.6. *Assume* $\operatorname{char} R = 0$. *If* δ *is a* C*-integral derivation of* R*, then there exist a* C*-integral element* $b \in Q$*, integers* $t_i \geq 1$ *and orthogonal* $e_i \in B$ $(i = 1, \dots, k)$ *with* $\sum_{i=1}^{k} e_i = 1$ *such that the following holds:*

(1) $\delta = \operatorname{ad}(b)$.

(2) be_i *has the minimal polynomial of degree* t_i.

(3) $\mathrm{E}[b^j e_i] = e_i$ *for* $j = 0, 1, \cdots, t_i - 1$.

Proof. By assumption, δ is C-integral. Since $\operatorname{char} R = 0$, δ is X-inner by [11]. Write $\delta = \operatorname{ad}(b)$ for some $b \in Q$. In view of Theorem 1.4, b is C-integral. Now, we conclude by applying Theorem 1.5 to our b. This proves the theorem.

Theorem 1.7. *Assume* $\operatorname{char} R = p \geq 2$. *If* δ *is a* C*-integral derivation of* R *with degree* n*, then there exist integers* $s_i \geq 0$, t_i *with* $1 \leq t_i \leq n$ *and orthogonal* $e_i \in B$ $(i = 1, \dots, k)$ *with* $\sum_{i=1}^{k} e_i = 1$ *such that the following holds for* $\delta_i \overset{\text{def.}}{=} \delta e_i$*:*

(1) $\delta_i^{p^j}$ $(0 \leq j < s_i)$ *are mutually outer and* $\mathrm{E}[\delta_i^{p^j}] = e_i$ *for* $0 \leq j < s_i$.

(2) $\delta_i^{p^{s_i}} = \sum_{j=0}^{s_i - 1} \delta_i^{p^j} \alpha_j + \operatorname{ad}(b_i)$ *holds for some* $\alpha_j \in e_i C$ *and* $b_i \in e_i Q$.

(3) b_i *has the minimum polynomial of degree* t_i *and* $\mathrm{E}[b_i^j] = e_i$ *for* $0 \leq j < t_i$.

Proof. For $s \geq 0$, we define B_s to be the set of $e \in B$ such that $\delta^{p^j} e$ $(0 \leq j < s)$ are mutually outer and such that $\mathrm{E}[\delta^{p^j}] \geq e$ for $0 \leq j < s$. Obviously, if $0 \neq f \in B$ and $f \leq e$ for some $e \in B_s$, then $f \in B_s$. Set $e_s \overset{\text{def.}}{=} \bigvee B_s$. Note that $e_s = 0$ if and only if $B_s = \emptyset$.

Claim 1. If $e_s \neq 0$, then $e_s \in B_s$: Pick orthogonal central idempotents $f_\nu \in B_s$ with $\bigvee_\nu f_\nu = e_s$. For $0 \leq j < s$, we have $\mathrm{E}[\delta^{p^j}] \geq f_\nu$ for all f_ν and hence $\mathrm{E}[\delta^{p^j}] \geq \bigvee f_\nu = e_s$. Suppose that $\sum_{j=0}^{s-1} \delta^{p^j} e_s \alpha_j - \operatorname{ad}(b) = 0$ holds for some $\alpha_j \in C$ and $b \in Q$. Multiplying the equality by f_ν, we have

$$\sum_{j=0}^{s-1} \delta^{p^j} f_\nu \alpha_j - \operatorname{ad}(b f_\nu) = \Big(\sum_{j=0}^{s-1} \delta^{p^j} e_s \alpha_j - \operatorname{ad}(b) \Big) f_\nu = 0.$$

Since $f_\nu \in B_s$, the derivations $\delta^{p^j} f_\nu$, where $0 \leq j < s$, are mutually outer and hence all $\delta^{p^j} f_\nu \alpha_j = 0$. This is true for all f_ν. Hence, $\delta^{p^j} e_s \alpha_j = \delta^{p^j} (\bigvee f_\nu) \alpha_j = 0$ for all $0 \leq j < s$. So $\delta^{p^j} e_s$ $(0 \leq j < s)$ are mutually outer. This proves the claim.

By the C-integrality of δ, we have a relation $\delta^n + \sum_{i=1}^{n-1} \delta^{n-i} \alpha_i = 0$, where $\alpha_i \in C$. Let $e \in B_s$, where $p^s > n$. If $\delta^{p^i} e$ $(0 \leq i < s)$ are mutually outer, then $\delta^i e$ $(0 \leq i \leq n)$ are regular words in mutually outer derivations $\delta e, \delta^p e, \dots, \delta^{p^{s-1}} e$ ordered in this order. By [11, Theorem 2], we have the identity $e(z_n + \sum_{i=1}^{n-1} \alpha_i z_{n-i}) = 0$ of Q, where z_i are distinct indeterminates. This is absurd. So $B_s = \emptyset$.

Set $B_0 \overset{\text{def.}}{=} B$ and $e_0 \overset{\text{def.}}{=} 1$. Then $B_0 \supseteq B_1 \supseteq B_2 \supseteq \cdots$ and hence $e_0 \geq e_1 \geq e_2 \geq \cdots$. Set $\hat{e}_s \overset{\text{def.}}{=} e_s - e_{s+1}$ for $0 \leq p^s \leq n$. For $0 \leq p^s \leq n$, let $\tilde{B}_s$ be the set of central idempotents $e \leq \hat{e}_s$ such that $\delta^{p^s} e + \sum_{i=0}^{s-1} \delta^{p^i} e\alpha_i - \mathrm{ad}(b) = 0$ for some $\alpha_i \in C$ and $b \in Q$. For $f \in B$, if $f \leq e$ for some $e \in \tilde{B}_s$, then obviously $f \in \tilde{B}_s$. Set $\tilde{e}_s \overset{\text{def.}}{=} \bigvee \tilde{B}_s$. Applying the same argument as that in Claim 1, we see $\tilde{e}_s \in \tilde{B}_s$. Notice that $\mathrm{E}[\delta^{p^i}] \geq e_s$ for $0 \leq i < s$.

Claim 2. $\tilde{e}_s = \hat{e}_s$: Otherwise, $f \overset{\text{def.}}{=} \hat{e}_s - \tilde{e}_s \neq 0$. Note that $f = \hat{e}_s(1 - \tilde{e}_s) = e_s(1 - e_{s+1})(1 - \tilde{e}_s)$. Therefore, $f \notin B_{s+1}$. Suppose for the moment that $g \overset{\text{def.}}{=} f(1 - \mathrm{E}[\delta^{p^s}]) \neq 0$. Then $\delta^{\delta^{p^s}} g = 0$, implying that $g \in \tilde{B}_s$. and so $g \leq \tilde{e}_s$. Then $g = gf\tilde{e}_s = 0$, a contradiction. Therefore, we have $g = 0$ and so $\mathrm{E}[\delta^{p^s}] \geq f$.

Since $f \notin B_{s+1}$, $\delta^{p^i} f$ $(0 \leq i \leq s)$ are *not* mutually outer. Since $E[\delta^{p^s}] \geq f$, we have $\delta^{p^i} f = 0$ for $0 \leq i \leq s$. So for some $\alpha_i \in C$ and $b \in Q$, $\sum_{i=0}^{s} \delta^{p^i} f\alpha_i - \mathrm{ad}(b) = 0$ and yet some $\delta^{p^i} f\alpha_i \neq 0$. Since $f \in B_s$, therefore $\delta^{p^i} f$ $(0 \leq i < s)$ are mutually outer. We must have $\delta^{p^s} f\alpha_s \neq 0$. By abelian regularity of C [1, Theorem 2.3.9], there exists $\beta \in C$ such that $(f\alpha_s)^2\beta = f\alpha_s$. Since $e \overset{\text{def.}}{=} f\alpha_s\beta \in B$ and $0 < e \leq f$, we have

$$\delta^{p^s} e + \sum_{i=0}^{s-1} \delta^{p^i} e\alpha_i\beta - \mathrm{ad}(be\beta) = \big(\sum_{i=0}^{s} \delta^{p^i} f\alpha_i - \mathrm{ad}(b)\big)e\beta = 0.$$

This says $e \in \tilde{B}_s$ and so $0 < e \leq \bigvee \tilde{B}_s \overset{\text{def.}}{=} \tilde{e}_s$. But $e \leq f \overset{\text{def.}}{=} \hat{e}_s - \tilde{e}_s$, a contradiction.

It suffices to show each $\hat{e}_s Q$ has the desired property. Replacing Q by $\hat{e}_s Q$ and δ by $\delta\hat{e}_s$, we may assume, with Claims 1 and 2, that $\mathrm{E}[\delta^{p^i}] = 1$ for $0 \leq i < s$, that δ^{p^i} $(0 \leq i < s)$ are mutually outer and that

$$\delta^{p^s} = \sum_{j=0}^{s-1} \delta^{p^j} \alpha_j + \mathrm{ad}(b)$$

for some $\alpha_i \in C$ and $b \in Q$. Multiply the above equality by δ from the left and the right hand sides respectively, and then take their difference. We see that

$$\sum_{j=0}^{s-1} \delta^{p^j} \alpha_j^\delta + \mathrm{ad}(b^\delta) = 0.$$

In view of [11, Theorem 2], we have $\alpha_j^\delta = 0$ for all j and $b^\delta \in C$. Therefore, the C-integrality of δ implies that $\mathrm{ad}(b)$ is C-integral. By Theorem 1.4, b is C-integral. We conclude by applying Theorem 1.5 to our b. This proves the theorem.

§2. Prime Case

Throughout this section, R is prime and C is hence a field. The case of $\operatorname{char} R = 0$ is well-known. But we include it here and sketch a proof for easy reference.

Theorem 2.1. *Let R be a prime ring of* $\operatorname{char} R = 0$ *and δ, a nilpotent derivation of R. Then $\delta = \operatorname{ad}(b)$ for a nilpotent element $b \in Q$ with nilpotency, say, l. Moreover, $m_\delta(R) = l$ and $n_\delta(R) = 2l - 1$.*

Proof. By [10, Corollary 2], $\delta = \operatorname{ad}(b)$ for some $b \in Q$. It follows from Theorem 1.1 that $\operatorname{ad}(b)$ is also a nilpotent derivation of Q with the same nilpotency. By [15, Theorem 2], b may be chosen to be a nilpotent element of the nilpotency, say l, and then $n_\delta(R) = 2l - 1$. Let $c \neq 0$ be such that $R^{\delta^m} c = 0$, where $m = m_\delta(R)$. For all $x \in R$,

$$(-1)^m x^{\delta^m} c = b^m xc - \binom{m}{1} b^{m-1} xbc + \cdots + (-1)^m \binom{m}{m} xb^m c = 0.$$

If $m < l$, then the elements $1, b, \ldots, b^m$ are C-independent and, by [14, Theorem 2], we have $c = 0$, absurd. So $m \geq l$. But $x^{\delta^l} b^{l-1} = 0$ and $b^{l-1} \neq 0$. So $m = l$ by the minimality of m.

The case of $\operatorname{char} R = p \geq 2$ is analogous to Theorem 2.1 but is more complicated.

Theorem 2.2 *Assume that R is a prime ring of* $\operatorname{char} R = p \geq 2$ *and δ, a nilpotent derivation of R. Then there exists an integer $s \geq 0$ such that $\delta^{p^s} = \operatorname{ad}(b)$ for some $b \in Q$ and such that the derivations δ^{p^i} are mutually outer for $i = 0, \ldots, s-1$.*

Proof. By [10, Corollary 3], there exists an integer $s \geq 0$ such that the derivations δ^{p^i}, where $0 \leq i < s$, are mutually outer and such that $\delta^{p^s} = \sum_{i=0}^{s-1} \delta^{p^i} \beta_i + \operatorname{ad}(b)$ for some $\beta_i \in C$ and $b \in Q$. We must show that all $\beta_i = 0$. Assume on the contrary that $\beta_t \neq 0$ for some $0 \leq t < s$. Let t be the least such integer and rewrite

$$\delta^{p^s} = \sum_{i=t}^{s-1} \delta^{p^i} \beta_i + \operatorname{ad}(b). \tag{1}$$

Claim: For any $n \geq 0$, there exist $\alpha_i \in C$ $(0 \leq i < s-1)$, not all vanishing, and $a \in Q$ such that

$$\delta^{p^{s+n}} = \sum_{i=t}^{s-1} \delta^{p^i} \alpha_i + \operatorname{ad}(a). \tag{2}$$

Granted the claim, we take n so large that $\delta^{p^{s+n}} = 0$. Then $0 = \delta^{s^{p+n}} = \sum_{i=t}^{s-1} \delta^{p^i}\alpha_i + \mathrm{ad}(a)$, where $\alpha_i \in C$ are *not* all vanishing. This contradicts the mutual outerness of δ^{p^i} $(0 \leq i < s)$ and proves our assertion.

The claim is proved by induction on n: If $n = 0$, then the expression (1), in which $\beta_t \neq 0$, is already in the expected form. As the induction hypothesis, assume that the claim holds for $n \geq 0$. Multiply (2) by δ from the right hand side:

$$\delta^{p^{s+n}+1} = \sum_{i=t}^{s-1} \delta^{p^i+1}\alpha_i + \sum_{i=t}^{s-1} \delta^{p^i}\alpha_i^\delta + \delta\,\mathrm{ad}(a) + \mathrm{ad}(a^\delta).$$

But(2) multiplied by δ from the left hand side gives $\delta^{p^{s+n}+1} = \sum_{i=t}^{s-1} \delta^{p^i+1}\alpha_i + \delta\,\mathrm{ad}(a)$. The difference between these two expressions of $\delta^{1+p^{s+n}}$ gives the identity $\sum_{i=t}^{s-1} \delta^{p^i}\alpha_i^\delta + \mathrm{ad}(a^\delta) = 0$. The mutual outerness of δ^{p^i} $(0 \leq i < s)$ implies $\alpha_i^\delta = 0$ $(t \leq i < s)$ and hence $\mathrm{ad}(a^\delta) = 0$ also. So $\alpha_i\delta = \delta\alpha_i + \alpha_i^\delta = \delta\alpha_i$ and $\mathrm{ad}(a)\delta = \delta\,\mathrm{ad}(a) + \mathrm{ad}(a^\delta) = \delta\,\mathrm{ad}(a)$. That is, all α_i and $\mathrm{ad}(a)$ commute with δ. Let u be the greatest integer with $\alpha_u \neq 0$ in (2) and rewrite (2) as $\delta^{p^{s+n}} = \sum_{i=t}^{u} \delta^{p^i}\alpha_i + \mathrm{ad}(a)$. Raise both sides of this equality to the p-th power using the commutativity of $\mathrm{ad}(a)$ and α_i:

$$\delta^{p^{s+n+1}} = \sum_{i=t}^{u} \delta^{p^{i+1}}\alpha_i^p + \mathrm{ad}(a^p). \tag{3}$$

If $u + 1 < s$, then (3) is in the claimed form since the coefficient of $\delta^{p^{u+1}}$ is $\alpha_u^p \neq 0$. If $u + 1 = s$, we replace δ^{p^s} of (3) by the right hand side of (1) and obtain

$$\delta^{p^{s+n+1}} = \delta^{p^{s-1}}(\cdot) + \cdots + \delta^{p^{t+1}}(\cdot) + \delta^{p^t}(\beta_t\alpha_u^p) + \mathrm{ad}(\alpha_u^p b + a^p),$$

where the coefficient of δ^{p^t} is $\beta_t\alpha_u^p \neq 0$, as claimed.

In Theorem 2.1 above, $\mathrm{ad}(b)$ is nilpotent, since δ is also nilpotent. We now characterize nilpotent $\mathrm{ad}(b)$ in terms of the minimum polynomial of b:

Theorem 2.3. *Let R be a prime ring of* $\mathrm{char}\,R = p \geq 2$ *and let $b \in Q$ define a nilpotent derivation* $\mathrm{ad}(b)$ *of R. Then the minimum polynomial of b over C admits the form $(b^{p^t} - \alpha)^l = 0$, where $\alpha \in C$, $t \geq 0$, $l \geq 1$ are integers and $(p, l) = 1$.*

Proof. Let $n \geq 0$ be the nilpotency of $\mathrm{ad}(b)$ on R. The identity $x^{\mathrm{ad}(b)^n} = 0$ of R also holds for $x \in Q$ by [1, Theorem 6.4.1]. Let $\overline{C}$ be the algebraic closure of C. The tensor product $\overline{Q} \overset{\text{def.}}{=} Q \underset{C}{\otimes} \overline{C}$ is a prime ring with the extended centroid $\overline{C}$ by [7, Theorem 3.5].

The map $r \in Q \mapsto r \otimes 1 \in \overline{Q}$ gives a ring embedding. The linear identity $x^{\mathrm{ad}(b)^n} = 0$ also extends linearly to $x \in \overline{Q}$. The nilpotency of $\mathrm{ad}(b)$ acting on $\overline{Q}$ is thus also n. Consider the polynomial ring $\overline{C}[\lambda]$ in the commuting indeterminate λ. Let $\mu(\lambda)$ be the minimum polynomial of b over $\overline{C}$. We *claim* that $\mu(\lambda) \in C[\lambda]$. Let ν be the degree of $\mu(\lambda)$ and write $\mu(\lambda) = \lambda^\nu + \alpha_1 \lambda^{\nu-1} + \cdots + \alpha_\nu$, where $\alpha_1, \cdots, \alpha_\nu \in \overline{C}$. We must show all $\alpha_i \in C$. Note that C is a subfield of $\overline{C}$. Pick a C-basis $\beta_0 \stackrel{\mathrm{def.}}{=} 1, \beta_1, \beta_2, \ldots$ of the C-space $\overline{C}$ and express each α_i as a C-linear combination of the basis $\beta_j \in \overline{C}$: $\alpha_i = \gamma_{i0} 1 + \gamma_{i1}\beta_1 + \gamma_{i2}\beta_2 + \cdots$, where $\gamma_j^i \in C$. Substitute these expressions of α_i into the minimum polynomial of b over $\overline{C}$ and collect terms according to β_i:

$$\begin{aligned} 0 &= b^\nu + \alpha_1 b^{\nu-1} + \cdots + \alpha_\nu \\ &= b^\nu + (\gamma_{10} + \gamma_{11}\beta_1 + \cdots) b^{\nu-1} + \cdots + (\gamma_{\nu 0} + \gamma_{\nu 1}\beta_1 + \cdots) \\ &= (b^\nu + \gamma_{10} b^{\nu-1} + \cdots + \gamma_{\nu 0}) + (\cdot)\beta_1 + (\cdot)\beta_2 + \cdots . \end{aligned}$$

In this expression, the left coefficients of $\beta_0 \stackrel{\mathrm{def.}}{=} 1, \beta_1, \beta_2, \ldots$ are all in Q, since $b \in Q$ and $\gamma_j^i \in C$. By the defining property of the tensor product $Q \underset{C}{\otimes} \overline{C}$, these coefficients of β_i must all be vanishing, since $\beta_0 = 1, \beta_1, \beta_2, \ldots$ are C-independent. Particularly, the coefficient of $\beta_0 \stackrel{\mathrm{def.}}{=} 1$ gives the equality $b^\nu + \gamma_{10} b^{\nu-1} + \cdots + \gamma_{\nu 0} = 0$. So b satisfies the polynomial $\lambda^\nu + \gamma_{10}\lambda^{\nu-1} + \cdots + \gamma_{\nu 0} \in C[\lambda]$. This polynomial also has the minimal degree ν of $\mu(\lambda)$ and hence must be equal to $\mu(\lambda)$. So $\mu(\lambda) \in C[\lambda]$ as claimed.

We pick a root $\lambda_0 \in \overline{C}$ of $\mu(\lambda)$. Then $\mathrm{ad}(b) = \mathrm{ad}(b - \lambda_0)$. For $x \in \overline{Q}$, we have

$$x^{\mathrm{ad}(b-\lambda_0)^n} = x(b-\lambda_0)^n + \sum_{i=1}^{n} (-1)^i \binom{n}{i} (b-\lambda_0)^i x (b-\lambda_0)^{n-i} = 0.$$

Set $\mu_0(\lambda) \stackrel{\mathrm{def.}}{=} \mu(\lambda)/(\lambda - \lambda_0)$. Multiplying the above by $\mu_0(b)$ from the left and using $\mu_0(b)(b - \lambda_0) = \mu(b) = 0$, we obtain $0 = \mu_0(b) x (b-\lambda_0)^n$ for $x \in \overline{Q}$. Since $\mu_0(b) \neq 0$, $(b - \lambda_0)^n = 0$ by the primeness of $\overline{Q}$ [7]. So $\mu(\lambda)$ divides $(\lambda - \lambda_0)^n$. We hence have $\mu(\lambda) = (\lambda - \lambda_0)^\nu$ for some ν. Write $\nu = p^t l$ with $(l, p) = 1$ and compute:

$$\begin{aligned} \mu(\lambda) =& (\lambda - \lambda_0)^\nu = (\lambda - \lambda_0)^{p^t l} = (\lambda^{p^t} - \lambda_0^{p^t})^l \\ =& \lambda^{p^t l} - \binom{l}{1} \lambda^{p^t (l-1)} \lambda_0^{p^t} + \cdots . \end{aligned}$$

Since $\mu(\lambda) \in C[\lambda]$, $\binom{l}{1}\lambda_0^{p^t} \in C$. But $l \in C$ is invertible, since $(l, p) = 1$. So $\lambda_0^{p^t} \in C$. Set $\alpha \stackrel{\mathrm{def.}}{=} \lambda_0^{p^t} \in C$. We have $\mu(\lambda) = (\lambda^{p^t} - \lambda_0^{p^t})^l = (\lambda^{p^t} - \alpha)^l$, as asserted.

By the p-power expansion of an integer $n \geq 0$, we mean an expression of the form $n = \sum_{s \geq 0} n_s p^s = n_0 + n_1 p + n_2 p^2 + \dots$, where $0 \leq n_s < p$ for each s.

Theorem 2.4. *Assume that R is a prime ring of* $\operatorname{char} R = p \geq 2$*, and δ a nilpotent derivation of R. Let $\delta^{p^s} = \operatorname{ad}(b)$ be as described in Theorem 2.2 and let $(b^{p^t} - \alpha)^l = 0$ be as described in Theorem 2.3. Then $m_\delta(R) = lp^{s+t}$.*

Proof. Let $m = m_\delta(R)$ be the annihilating nilpotency of δ and let $m = \sum_{i \geq 0} m_i p^i$ be the p-power expansion of m. We have

$$\begin{aligned}\delta^m &= \big(\delta^{m_0 + m_1 p + \cdots + m_{s-1} p^{s-1}}\big)\big(\delta^{m_s p^s + m_{s+1} p^{s+1} + \cdots}\big) \\ &= \big(\delta^{m_0} (\delta^p)^{m_1} \cdots (\delta^{p^{s-1}})^{m_{s-1}}\big)\big(\delta^{p^s}\big)^{m_s + m_{s+1} p + \cdots} \\ &= \Delta \operatorname{ad}(b)^n,\end{aligned}$$

where we have set $\Delta \overset{\text{def.}}{=} \delta^{m_0} (\delta^p)^{m_1} \cdots (\delta^{p^{s-1}})^{m_{s-1}}$ and $n \overset{\text{def.}}{=} m_s + m_{s+1} p + \cdots$. Note that Δ is a regular derivation word in the mutually outer derivations $\delta, \dots, \delta^{p^{s-1}}$ linearly ordered by $\delta < \delta^p < \cdots < \delta^{p^{s-1}}$. Suppose that $R^{\delta^m} c = 0$ with $c \neq 0$. We apply [11, Theorem 2] to the identity $0 = x^{\delta^m} c = (x^\Delta)^{\operatorname{ad}(b)^n} c$ and obtain the identity $x^{\operatorname{ad}(b)^n} c = 0$ for R. But $0 = x^{\operatorname{ad}(b)^n} c = x^{\delta^{p^s n}} c$. So $m = p^s n$ by the minimality of m. We then have

$$\begin{aligned}0 =& x^{\delta^m} c = x^{(\delta^{p^s})^n} c = x^{\operatorname{ad}(b)^n} c \\ =& (-1)^n \Big(b^n x - \binom{n}{1} b^{n-1} x b + \binom{n}{2} b^{n-2} x b^2 - \cdots\Big) c.\end{aligned}$$

Note that lp^t is the algebraic degree of b over C. If $n < p^t l$, then left coefficients $1, b, \dots, b^n$ of the above are C-independent and right coefficients must be all vanishing by [14, Theorem 2], contradicting $c \neq 0$. So $n \geq p^t l$. But $\operatorname{ad}(b)^{p^t l} = \operatorname{ad}(b^{p^t})^l = \operatorname{ad}(b^{p^t} - \alpha)^l = \operatorname{ad}(\tilde{b})^l$, where $\tilde{b} \overset{\text{def.}}{=} b^{p^t} - \alpha$ has nilpotency l. We have the expansion

$$x^{\operatorname{ad}(b)^{p^t l}} = x^{\operatorname{ad}(\tilde{b})^l} = \sum_{i=0}^{l} (-1)^i \binom{n}{i} \tilde{b}^i x \tilde{b}^{l-i} = \sum_{i=1}^{l-1} (-1)^i \binom{n}{i} \tilde{b}^i x \tilde{b}^{l-i}.$$

We see that $x^{\operatorname{ad}(b)^{p^t l}} \tilde{b}^{l-1} = 0$ using $\tilde{b}^l = 0$. So $n = p^t l$ and $m = p^s p^t l = p^{s+t} l$, as asserted.

We are now ready to describe completely the nilpotency of a nilpotent derivation.

Theorem 2.5. *Assume that R is a prime ring of* $\operatorname{char} R = p \geq 2$*, and δ a nilpotent derivation of R. Let $\delta^{p^s} = \operatorname{ad}(b)$ be as described in Theorem 2.2 and let $(b^{p^t} - \alpha)^l = 0$ be as described in Theorem 2.3. Let $l = \sum_{i \geq 0} l_i p^i$ be the p-power expansion of l.*

(1) If $2l_0 - 1 < p$ *and* $2l_i < p$ *for all* $i > 0$*, then*

$$n_\delta(R) = \big((2l_0 - 1) + \sum_{i>0} 2l_i p^i\big)p^{s+t} = (2l - 1)p^{s+t}.$$

(2) If $2l_0 - 1 \geq p$ *or if* $2l_i \geq p$ *for some* $i > 0$*, then*

$$n_\delta(R) = \big((2l_u + 1)p^u + \sum_{i>u} 2l_i p^i\big)p^{s+t},$$

where $u \geq 0$ *is the least integer such that* $2l_u + 1 < p$ *and* $2l_i < p$ *for all* $i > u$*.*

We need to tell whether $\binom{n}{i} \equiv 0 \pmod p$ or not. This is solved neatly by Lucas in his *Theorie des Nombres* (pp. 417–420) and his solution is reproduced in [8]:

Lemma 2.6. *(*Lucas*) Given a prime* $p \geq 2$*, let* $n = \sum_{s\geq 0} n_s p^s$ *and* $i = \sum_{s\geq 0} i_s p^s$ *be the* p*-power expansions of integers* $n, i \geq 0$ *respectively. Then* $\binom{n}{i} \equiv \prod_{s\geq 0} \binom{n_s}{i_s}$ *(mod* p*), where we postulate* $\binom{k}{0} = 1$ *for* $k \geq 0$ *and* $\binom{k}{j} = 0$ *for* $j > k \geq 0$*.*

We recall two notations in number theory: For a real number $r \geq 0$, let $[r]$ be the greatest integer n such that $n \leq r$ and let $\{r\}$ be the smallest integer n such that $n \geq r$. Obviously, $\{\frac{n}{2}\} + \big[\frac{n}{2}\big] = n$ for any integer $n \geq 0$. With this we compute the *central* nonvanishing binomial coefficients (mod p):

Lemma 2.7. *Given a prime* $p \geq 2$*, let* n *be a given nonnegative integer with the* p*-power expansion* $n = \sum_{s\geq 0} n_s p^s$*. Let* v *be the least nonnegative integer such that* n_s *is even for* $s > v$*. Define*

$$\ell(n) \stackrel{\text{def.}}{=} \{\frac{n_v}{2}\}p^v + \sum_{s>v} \frac{n_s}{2} p^s \quad \textit{and} \quad \ell'(n) \stackrel{\text{def.}}{=} n - \ell(n).$$

Then $\ell'(n) \leq \ell(n)$ *and* $\binom{n}{i} \equiv 0$ *(mod* p*) for* $\ell'(n) < i < \ell(n)$ *but* $\binom{n}{\ell(n)} \not\equiv 0$ *(mod* p*).*

Proof. Write $\ell(n), \ell'(n)$ as ℓ, ℓ' for brevity. In view of the equality $\{\frac{n_v}{2}\} + [\frac{n_v}{2}] = n_v$, the p-power expansion of ℓ' is given by

$$\ell' = \sum_{s<v} n_s p^s + \big[\frac{n_v}{2}\big]p^v + \sum_{s>v} \frac{n_s}{2} p^s.$$

If $\{\frac{n_v}{2}\} > [\frac{n_v}{2}]$, then $\ell > \ell'$. If $\{\frac{n_v}{2}\} = [\frac{n_v}{2}]$, then n_v is even. This happens only when $v = 0$ by the definition of v. In this case, $\ell = \frac{n_0}{2} + \sum_{s>0} \frac{n_s}{2} p^s = \ell'$. So always $\ell \geq \ell'$, as asserted.

Since $0 \le \{\frac{n_v}{2}\} \le n_v < p$, $\binom{n_v}{\{n_s/2\}} \not\equiv 0 \pmod p$. For $s > v$, n_s is even by the definition of v and, since $0 \le n_s/2 \le n_s < p$, we also have $\binom{n_s}{n_s/2} \not\equiv 0 \pmod p$. By Lemma 2.6, we have $\binom{n}{\ell} \equiv \binom{n_v}{\{n_v/2\}} \prod_{s>v} \binom{n_s}{n_s/2} \not\equiv 0 \pmod p$, as asserted.

Given $\ell' < i < \ell$, let $i = \sum_{s\ge 0} i_s p^s$ be its p-power expansion. For brevity, let ℓ_s, ℓ'_s denote the coefficients of p^s in the p-power expansions of ℓ, ℓ' respectively. Since $\ell' < i$, there exists $\overline{s}$ such that $i_{\overline{s}} > \ell'_{\overline{s}}$ and $i_s = \ell'_s$ for all $s > \overline{s}$. If $\overline{s} > v$, then also $i > \ell$, since $\ell'_s \overset{\text{def.}}{=} n_s/2 \overset{\text{def.}}{=} \ell_s$ for $s > v$. This contradicts the assumption $\ell' < i < \ell$. If $\overline{s} = v$, then $i_v > \ell'_v \overset{\text{def.}}{=} [n_v/2]$ and hence $i_v \ge \{n_v/2\} \overset{\text{def.}}{=} \ell_v$. This implies $i \ge \ell$, since $i_s = \ell'_s = n_s/2 = \ell_s$ for $s > v$. Again, this contradicts the assumption $\ell' < i < \ell$. So we must have $\overline{s} < v$. But then $i_{\overline{s}} > \ell'_{\overline{s}} \overset{\text{def.}}{=} n_{\overline{s}}$ and, by our convention on binomial coefficients, $\binom{n_{\overline{s}}}{i_{\overline{s}}} \overset{\text{def.}}{=} 0$. By Lemma 2.6, we have $\binom{n}{i} \equiv \binom{n_0}{i_0}\binom{n_1}{i_1}\cdots\binom{n_{\overline{s}}}{i_{\overline{s}}}\cdots \equiv 0 \pmod p$, as asserted.

Lemma 2.8. *Let R be a prime ring of* $\operatorname{char} R = p \ge 2$. *Let $b \in Q$ be nilpotent and have the nilpotency m. Then for integer $n \ge 0$, $\operatorname{ad}(b)^n = 0$ if and only if $\ell(n) \ge m$, where $\ell(n)$ is as defined in Lemma 2.7.*

Proof. Write $\ell(n)$ as ℓ for short. Set $\ell' = n - \ell$. We have the expansion

$$x^{\operatorname{ad}(b)^n} = \sum_{i=0}^{n} (-1)^i \binom{n}{i} b^i x b^{n-i}. \tag{4}$$

For necessity ($\Leftarrow$), assume that $\ell \ge m$. Consider a typical term $\binom{n}{i} b^i x b^{n-i}$, where $0 \le i \le n$. If $\ell' < i < \ell$ then $\binom{n}{i} \equiv 0 \bmod p$ by Lemma 2.7. If $i \ge \ell$ then $b^i = 0$, since $i \ge \ell \ge m$. If $i \le \ell'$ then $b^{n-i} = 0$, since $n - i \ge n - \ell' = \ell \ge m$. So $\binom{n}{i} b^i x b^{n-i} = 0$ always and $\operatorname{ad}(b)^n = 0$ follows. For sufficiency ($\Rightarrow$), assume that $x^{\operatorname{ad}(b)^n} = 0$ for all $x \in R$. Since $b^i = 0$ for $i \ge m$, the sum of the terms with $i < m$ in (4) gives a linear identity with right coefficients $1, b, \ldots, b^{m-1}$, which are C-independent. By [14, Theorem 2], their corresponding left coefficients must vanish. That is, $\binom{n}{i} b^{n-i} = 0$ for $0 \le i < m$. So, if $\ell < m$ then $\binom{n}{\ell} b^{n-\ell} = 0$. But $\binom{n}{\ell} \ne 0$ by Lemma 2.7 and $b^{n-\ell} \ne 0$, since $m > \ell \ge \ell' \overset{\text{def.}}{=} n - \ell$. This is a contradiction.

Proof of Theorem 2.5. Let $n = n_\delta(R)$ be the nilpotency of δ. Write $n = p^s q + r$, where q, r are nonnegative integers and $0 \le r < p^s$. With $\delta^{p^s} = \operatorname{ad}(b)$, we write

$$0 = x^{\delta^n} = x^{\delta^{p^s q + r}} = (x^{\delta^r})^{(\delta^{p^s})^q} = (x^{\delta^r})^{\operatorname{ad}(b)^q},$$

which is a linear generalized identity in x^{δ^r}. Let r have the p-power expansion $r_0 + r_1 p + \ldots + r_{s-1} p^{s-1}$. Then

$$\delta^r = (\delta)^{r_0} (\delta^p)^{r_1} \cdots (\delta^{p^{s-1}})^{r_{s-1}}$$

is a regular word in the mutually outer derivations $\delta, \delta^p, \dots, \delta^{p^{s-1}}$ linearly ordered by $\delta < \delta^p < \cdots < \delta^{p^{s-1}}$. We apply [11, Theorem 2] to the differential identity $(x^{\delta^r})^{\mathrm{ad}(b)^q}$ and obtain the identity $z^{\mathrm{ad}(b)^q} = 0$ for R. But $0 = z^{\mathrm{ad}(b)^q} = z^{\delta^{p^s q}}$. By the minimality of the nilpotency n, we have $n = p^s q$. So $0 = \delta^n = \delta^{p^s q} = \mathrm{ad}(b)^q$. It suffices to find q, which is obviously the nilpotency q of $\mathrm{ad}(b)$. Replacing δ by $\mathrm{ad}(b)$, we may assume $s = 0$ to start with. Set $\overline{Q} \stackrel{\text{def.}}{=} Q \underset{C}{\otimes} \overline{C}$, where $\overline{C}$ is the algebraic closure of C. As explained in the proof of Theorem 2.3, $\mathrm{ad}(b)$ has the same nilpotency on $\overline{Q}$ as on R and the minimal polynomial of b over $\overline{C}$ is also $(b^{p^t} - \alpha)^l = 0$. Replacing R by $\overline{Q}$, we may assume that the extended centroid C is algebraically closed. The minimum polynomial of b over C is thus of the form $(b - \alpha^{1/p^t})^{p^t l} = 0$. But b and $b - \alpha^{1/p^t}$ define the same inner derivation. Replacing b by $b - \alpha^{1/p^t}$, we may further assume that b is nilpotent and has the nilpotency lp^t.

Firstly, assume that $2l_0 - 1 < p$ and $2l_i < p$ for all $i > 0$. Set

$$\nu \stackrel{\text{def.}}{=} (2l_0 - 1)p^t + \sum_{i>0} 2l_i p^{i+t} = \big((2l_0 - 1) + \sum_{i>0} 2l_i p^i\big)p^t = (2l - 1)p^t.$$

We compute

$$\ell(\nu) = l_0 p^t + \sum_{i>0} l_i p^{i+t} = (l_0 + \sum_{i>0} l_i p^i)p^t = lp^t.$$

Since lp^t is the nilpotency of b, we have $\mathrm{ad}(b)^\nu = 0$ by Lemma 2.8. Note that $l_0 \geq 1$, since $(l, p) = 1$. The p-power expansion of $\nu - 1$ is thus given by

$$\nu - 1 = \sum_{0 \leq j < t} (p - 1)p^j + (2l_0 - 2)p^t + \sum_{i>0} 2l_i p^{i+t}.$$

If p is odd, then $p - 1$ is even and

$$\ell(\nu - 1) = \sum_{0 \leq j < t} \frac{(p-1)}{2} p^j + (l_0 - 1)p^t + \sum_{i>0} l_i p^{i+t} < lp^t.$$

By Lemma 2.8, $\mathrm{ad}(b)^{\nu-1} \neq 0$. If $p = 2$, then $l_i = 0$ for $i \geq 1$ and $\nu = 2^t$. Thus $\ell(\nu - 1)$ is equal to 0 or 2^{t-1} depending on whether $t = 0$ or $t > 0$. But $\ell(\nu - 1) < l2^t$ in either case. By Lemma 2.8, $\mathrm{ad}(b)^{\nu-1} \neq 0$. So the nilpotency of $\mathrm{ad}(b)$ is ν, as asserted.

Now, we assume that $2l_0 - 1 \geq p$ or $2l_i \geq p$ for some $i > 0$. Let $u \geq 0$ be the least integer such that $2l_u + 1 < p$ and $2l_i < p$ for all $i > u$. Set

$$\nu \stackrel{\text{def.}}{=} (2l_u + 1)p^{u+t} + \sum_{i>u} 2l_i p^{i+t} = \big((2l_u + 1)p^u + \sum_{i>u} 2l_i p^i\big)p^t.$$

We compute

$$\ell(\nu) = (l_u + 1)p^{u+t} + \sum_{i>u} l_i p^{i+t} = \big((l_u + 1)p^u + \sum_{i>u} l_i p^i\big)p^t > lp^t.$$

So $\mathrm{ad}(b)^\nu = 0$ by Lemma 2.8. The p-power expansion of $\nu - 1$ is given by

$$\nu - 1 = \sum_{0\le j<u+t} (p-1)p^j + 2l_u p^{u+t} + \sum_{i>u} 2l_i p^{i+t}.$$

If p is odd, then $p-1$ is even and

$$\ell(\nu - 1) = \sum_{0\le j<u+t} \frac{(p-1)}{2} p^j + l_u p^{u+t} + \sum_{i>u} l_i p^{i+t}.$$

By our case assumption, either $2l_0 - 1 \ge p$ or $2l_i \ge p$ for some $i > 0$. Let $\overline{j}$ be the greatest j such that $2l_j \ge p$. Note that $\overline{j} < u$ by the definition of u. For $\overline{j} < j < u$, we have $2l_j < p$ by the maximality of $\overline{j}$ and $2l_j + 1 \ge p$ by the minimality of u. That is, $l_j = \frac{p-1}{2}$ for $\overline{j} < j < u$. Also, $l_{\overline{j}} \ge \frac{p}{2} > \frac{p-1}{2}$ by the definition of $\overline{j}$. So $\ell(\nu-1) < lp^t$ and hence $\mathrm{ad}(b)^{\nu-1} \ne 0$ by Lemma 2.8. For $p = 2$, the condition that $2l_u + 1 < p$ and $2l_i < p$ for all $i > u$ implies $l_i = 0$ for $i \ge u$ and u is hence the least such integer. So $\nu = 2^{u+t}$ and $l_{u-1} = 1$ by the minimality of u. So $\ell(\nu-1) = 2^{u+t-1}$. Since $(l, p) = 1$, $l_0 = 1$ and the condition $2l_0 - 1 < p = 2$ surely holds. By our case assumption, $2l_j \ge p = 2$ for some $j > 0$. So $u - 1 > 0$, implying $l > 2^{u-1}$ and hence $\ell(\nu-1) < l2^t$. By Lemma 2.8, $\mathrm{ad}(b)^{\nu-1} \ne 0$. So the nilpotency of $\mathrm{ad}(b)$ is ν, as asserted.

§3. Semiprime Case

Our aim here is to extend the results in §2 to semiprime rings. So our R is a semiprime ring with extended centroid C and with symmetric Martindale quotient ring Q throughout. Inspired by the m, n-homogeneity of [9], we give a name for those rings on which nilpotent derivations under consideration behave in the same way as in the prime case:

Definition 2. Let R be a semiprime ring of characteristic 0 or a prime $p \ge 2$. Let δ be a nilpotent derivation of R. We call R δ-homogeneous if one of the following two conditions holds:

(1) If $\mathrm{char}\, R = 0$, then there exists $b \in Q$ satisfying the following: (i) $\delta = \mathrm{ad}(b)$. (ii) The minimum polynomial of this b over C admits the form $b^l = 0$ for some integer $l \ge 0$. (iii) $\mathrm{E}[b^n] = 1$ for $n = 1, 2, \cdots, l-1$.

(2) If $\operatorname{char} R = p \geq 2$, then there exist $b \in Q$ and an integer $s \geq 0$ satisfying the following: (i) $\delta^{p^s} = \operatorname{ad}(b)$. (ii) The derivations $\delta, \delta^p, ..., \delta^{p^{s-1}}$ are mutually outer. (iii) The minimum polynomial of this b over C admits the form $(b^{p^t} - \alpha)^l = 0$, where $\alpha \in C$, $t \geq 0$, $l \geq 1$ are integers and $(p, l) = 1$. (iv) $\mathrm{E}[\delta^{p^i}] = 1$ for $i = 0, 1, \cdots, s-1$ and $\mathrm{E}[b^n] = 1$ for $n = 1, 2, \cdots, p^t l - 1$.

This definition is justified by the following two theorems:

Theorem 3.1. *Let R be a semiprime δ-homogeneous ring of* $\operatorname{char} R = 0$*, where δ is a nilpotent derivation of R. Let δ, l be as described in (1) of Definition 2. Then $m_\delta(R) = l$ and $n_\delta(R) = 2l - 1$.*

The proof of Theorem 3.1 is similar to that of Theorem 3.2 below but is much simpler. We omit it for brevity.

Theorem 3.2. *Let R be a semiprime δ-homogeneous ring of prime characteristic $p \geq 2$, where δ is a nilpotent derivation of R. Let δ and s, t, l be as described in (2) of Definition 2. Then $m_\delta(R) = p^{s+t} l$ and n_δ is given as follows: Let $l = \sum_{i \geq 0} l_i p^i$ be the p-power expansion of l.*

(1) If $2l_0 - 1 < p$ and $2l_i < p$ for all $i > 0$, then

$$n_\delta(R) = \big((2l_0 - 1) + \sum_{i>0} 2l_i p^i\big) p^{s+t} = (2l - 1) p^{s+t}.$$

(2) If $2l_0 - 1 \geq p$ or if $2l_i \geq p$ for some $i > 0$, then

$$n_\delta(R) = ((2l_u + 1) p^u + \sum_{i>u} 2l_i p^i) p^{s+t},$$

where $u \geq 0$ is the least integer such that $2l_u + 1 < p$ and such that $2l_i < p$ for all $i > u$.

Proof. Set $m = p^{s+t} l$. We also let $n = (2l - 1) p^{s+t}$ for Case (1) and let $n = ((2l_u + 1) p^u + \sum_{i>u} 2l_i p^i) p^{s+t}$ for Case (2). We extend δ to Q. By Theorem 1.1, the nilpotency and the annihilating nilpotency of δ remain the same for δ thus extended, and the identity $\delta^{p^s} = \operatorname{ad}(b)$ also holds for Q. Obviously, the p^i-th powers δ^{p^i}, where $0 \leq i < s$, of δ thus extended remain mutually outer. We may thus replace R by Q. Let P be a fixed but arbitrary minimal prime ideal of Q. By Theorem 1.2, we have $P^\delta \subseteq P$. Consider $\overline{Q} \overset{\text{def.}}{=} Q/P$. Let $\overline{b}$ be the natural image of b in $\overline{Q}$, and $\overline{\delta}$ the derivation of $\overline{Q}$ induced by δ. Obviously, $\overline{\delta}^{p^s} = \operatorname{ad}(\overline{b})$. By Theorem 1.3, the minimum polynomial of $\overline{b}$ over $\overline{C}$ is $(\overline{b}^{p^t} - \overline{\alpha})^l = 0$ and $\overline{\delta}^{p^i}$ $(0 \leq i < s)$ remain mutually outer.

By Theorems 2.4 and 2.5 applied to $\overline{Q}$, we see that $m_{\overline{\delta}}(Q/P) = m$ and $n_{\overline{\delta}}(Q/P) = n$. This implies immediately that $n_\delta(R) = n$.

Let $m' = m_\delta(R)$. There exists $0 \neq c \in R$ such that $R^{\delta^{m'}} c = 0$ and so $Q^{\delta^{m'}} c = 0$. Choose a minimal prime ideal P of Q such that $c \notin P$. Then $\overline{Q}^{\overline{\delta}^{m'}} \overline{c} = 0$, where $\overline{Q} \stackrel{\text{def.}}{=} Q/P$ and $\overline{c} \neq 0$. Thus $m' \geq m_{\overline{\delta}}(\overline{Q}) = m$. On the other hand, let I be a nonzero ideal of R. Choose a minimal prime ideal P of Q such that $I \not\subseteq P$. Then $\overline{I} \neq 0$. Since $m_{\overline{\delta}}(\overline{Q}) = m$, there exists $0 \neq \overline{c} \in \overline{I}$, that is, there exists $c \in I \setminus P$, such that $\overline{Q}^{\overline{\delta}^m} \overline{c} = 0$. That is, $Q^{\delta^m} c \subseteq P$. But $Q^{\delta^m} c$ is orthogonally complete. There exists a central idempotent $e \notin P$ such that $Q^{\delta^m} ce = 0$ by [1, Proposition 3.1.11]. Choose a dense ideal J of R such that $ceJ \cup eJ \subseteq R$. Since $ce \neq 0$, we choose a nonzero element $c' \in ceJ$. Then $c' \in I$ and $Q^{\delta^m} c' = 0$. In particular, $R^{\delta^m} c' = 0$ follows. Thus $m \geq m'$ and so $m = m'$. This proves our assertion on m.

We need some more notions to state our main theorem: Central idempotents are always constants of derivations. If e is a central idempotent of Q, then eQ is the symmetric Martindale quotient ring of the semiprime ring $eQ \cap R$ by [1, Proposition 2.3.14]. For any derivation δ of R, we have $(eQ \cap R)^\delta \subseteq eQ \cap R$. That is, the restriction of δ to $eQ \cap R$ gives rise to a derivation of $eQ \cap R$. A family of central idempotents $e_1, e_2, \dots$ is called orthogonal if $e_i e_j = 0$ for $i \neq j$. Orthogonal central idempotents $e_1, \dots, e_k$ with $e_1 + \cdots + e_k = 1$ give rise to the direct sum decomposition $Q = \oplus_{i=1}^k e_i Q$. In this case, the ideal $\oplus_{i=1}^k (e_i Q \cap R)$ is essential in R. Any direct sum decomposition of Q arises in this way. We are now ready to state our main result in semiprime rings:

Theorem 3.3. *Let R be a semiprime ring of characteristic 0 or a prime p and δ, a nilpotent derivation of R. Then there exist finitely many orthogonal central idempotents $e_1, \dots, e_k$ in Q with $e_1 + \cdots + e_k = 1$ such that each $e_i Q \cap R$ is δ_i-homogeneous, where δ_i is the restriction of δ to $e_i Q \cap R$.*

Proof. Let $e_1, \dots, e_k$ be central idempotents given in Theorems 1.4 and 1.7, respectively, according to $\operatorname{char} R = 0$ or a prime p. Let δ_i be the restriction of δ to $e_i Q$. It suffices to show the δ_i-homogeneity of $e_i Q$. Let us consider the case $\operatorname{char} R = p \geq 2$ only. The case $\operatorname{char} R = 0$ is similar and simpler. Replacing R, δ by $R \cap e_i Q$, δ_i respectively, we may assume the following:

(i) δ^{p^i} $(0 \leq i < s)$ are mutually outer and $\mathrm{E}[\delta^{p^i}] = 1$ for $0 \leq i < s$.

(ii) δ satisfies the identity $\delta^{p^s} + \delta^{p^{s-1}} \alpha_1 + \cdots + \delta \alpha_s = \operatorname{ad}(b)$, where $\alpha_i \in C$ and

where $b \in Q$.

(iii) $\mathrm{E}[b^i] = 1$ for $1 \le i < m$ and b has the minimum polynomial over C:

$$b^m + \beta_{m-1}b^{m-1} + \cdots + \beta_0 = 0, \qquad \beta_i \in C.$$

Consider $\overline{Q} \overset{\text{def.}}{=} Q/P$, where P is a fixed but arbitrary minimal prime ideal of Q. Let $\overline{\alpha}_i$, $\overline{b}$, $\overline{\beta}_j$ be the natural images of α_i, b, β_j in $\overline{Q}$ respectively, and $\overline{\delta}$ the derivation of $\overline{Q}$ induced by δ. (We have $P^\delta \subseteq P$ by Theorem 1.2.) Obviously, we have the identities $\overline{\delta}^{p^s} + \overline{\delta}^{p^{s-1}}\overline{\alpha}_1 + \cdots + \overline{\delta}\overline{\alpha}_s = \mathrm{ad}(\overline{b})$ and $\overline{b}^m + \overline{\beta}_{m-1}\overline{b}^{m-1} + \cdots + \overline{\beta}_0 = 0$. By (2) and (3) of Theorem 1.3, the derivations $\overline{\delta}^{p^i}$, where $0 \le i < s$, are mutually outer and the elements $1, \overline{b}, \ldots, \overline{b}^{m-1}$ are $\overline{C}$-independent. Write $m = p^t l$ with $(l, p) = 1$. Applying Theorems 2.2 and 2.3 respectively to the nilpotent derivations $\overline{\delta}$ and $\mathrm{ad}(b)$ of the prime ring $\overline{Q}$, we have all $\overline{\alpha}_i = 0$ and $(\overline{b}^{p^t} - \overline{\alpha})^l = 0$, where $\alpha \overset{\text{def.}}{=} -\beta_{p^t(l-1)}/l$. This is true for any minimal prime ideal P of Q. It follows that all $\alpha_i = 0$ and $(b^{p^t} - \alpha)^l = 0$. So $\delta^{p^s} = \mathrm{ad}(b)$ and b has the minimum polynomial $(b^{p^t} - \alpha)^l = 0$, as asserted.

It is proved in [3] that, for a semiprime ring of prime characteristic $p \ge 2$, the nilpotency of a derivation has the p-power expansion in the form $n = n_\nu p^\nu + \sum_{i>\nu} n_i p^i$, where n_ν is odd and all n_i $(i > \nu)$ are even. We sharpen this as follows:

Theorem 3.4. *Let R be a semiprime ring of prime characteristic $p \ge 2$, and δ a nilpotent derivation with $m_\delta(R) = lp^v$, where $(l, p) = 1$. Then $n_\delta(R)$ is the greatest integer $\nu \le (2l-1)p^v$ with the p-power expansion in the form $\nu = \nu_k p^k + \sum_{i>k} \nu_i p^i$, where ν_k is odd and all ν_i $(i > k)$ are even.*

Proof. By Theorem 3.3, Q is a direct sum of finitely many rings Q_i, $1 \le i \le q$ such that each $Q_i \cap R$ is δ_i-homogeneous, where δ_i is the restriction of δ to $Q_i \cap R$. Observe that $m_\delta(R) = m_\delta(Q) = \max\{m_{\delta_i}(Q_i) \mid 1 \le i \le k\}$, $n_\delta(R) = n_\delta(Q) = \max\{n_{\delta_i}(Q_i) \mid 1 \le i \le k\}$, $m_{\delta_i}(R \cap Q_i) = m_{\delta_i}(Q_i)$ and $n_{\delta_i}(R \cap Q_i) = n_{\delta_i}(Q_i)$. Thus we may assume that R is δ-homogeneous. We see easily that l here is the l in Theorem 3.2 and v here is equal to $s + t$, where s, t are as given in Theorem 3.2. Write l in the p-power expansion $l = \sum_{i \ge 0} l_i p^i$. The nilpotency n given in Theorem 3.2 has the form ν described here. If (1) of Theorem 3.2 holds, then the nilpotency is just $(2l-1)p^v$ and there is nothing to prove. So suppose (2) of Theorem 3.2 holds. Then $n_\delta(R) = ((2l_u + 1)p^u + \sum_{i>u} 2l_i p^i)p^{s+t}$, where $u \ge 0$ is the least integer such that $2l_u + 1 < p$ and such that $2l_i < p$ for all $i > u$. Write n_δ in its p-power expansion $n_\delta(R) = \sum_{i \ge 0} n_i p^i$. Then $n_{u+v} = 2l_u + 1$ and $n_i = 2l_i$ if $i > u + v$. Let ν have

the form described here and assume $\nu > n_\delta(R)$. It suffices to show $\nu > (2l-1)p^v$: Let $\overline{j}$ be the greatest j such that $\nu_j > n_j$ and $\nu_i = n_i$ for $i > j$. If $\overline{j} < u+v$, then $u+v > k$ and so ν_{u+v} is even. But $n_{u+v} = 2l_u+1$ is odd, contradicting $\nu_{u+v} = n_{u+v}$. If $\overline{j} \geq u+v$, then

$$\begin{aligned}\nu &> \sum_{j=0}^{u-1}(p-1)p^{j+v} + (2l_u+1)p^{u+v} + \sum_{i>u} 2l_i p^{i+v} \\ &= \big(-1 + 2(l_u+1)p^u + \sum_{i>u} 2l_i p^i\big)p^v > (2l-1)p^v,\end{aligned}$$

where the last inequality follows from $(l_u+1)p^u + \sum_{i>u} l_i p^i > l$. This finishes our proof.

For a semiprime ring R of $\operatorname{char} R = 2$, Chung and Luh [6] proved that the nilpotency of a nilpotent derivation must be a power of 2. We also have a sharper version for this:

Theorem 3.5. *Let R be a semiprime ring of characteristic 2, and δ a nilpotent derivation of R with $m_\delta(R) = l2^v$, where $(l,2) = 1$. Then $n_\delta(R)$ is the unique 2-power integer between $l2^v$ and $(2l-1)2^v$.*

Proof. By Theorem 3.4, $n_\delta(R)$ is the greatest integer $\leq (2l-1)p^v$. Therefore, it suffices to prove that $n_\delta(R)$ is the least 2-power $\geq m_\delta(R) = l2^v$. As in the proof of Theorem 3.4, we may assume that R is δ-homogeneous. In the notation of Theorem 3.2, we observe that $2l_i < p = 2$ implies $l_i = 0$. If (1) of Theorem 3.2 holds, then $l_i = 0$ for $i > 0$ and hence $l = l_0 = 1$. The nilpotency is thus $(2l-1)2^{s+t} = 2^{s+t} = m_\delta(R)$, as asserted. If (2) of Theorem 3.2 holds, then u is the greatest integer with $l_{u-1} \neq 0$ and the nilpotency of δ is 2^{u+s+t}. By the case assumption of (2), we also have $2l_j \geq p = 2$ for some $j > 0$. So $u-1 > 0$ and the nilpotency 2^{u+s+t} is thus the least 2-power $\geq l2^{s+t}$.

As an application of Theorem 3.3, we deduce [9, Theorem 5] in a slightly generalized form:

Theorem 3.6. (Grzeszczuk [9]) *Let R be a semiprime ring and δ, a nilpotent derivation of R. Suppose that, for any δ-ideal $J \neq 0$ of R, if the characteristic of J is a prime $p \geq 2$, then p does not divide $m_\delta(J)$ or $n_\delta(J)$. Then $\delta = \operatorname{ad}(b)$ for some $b \in Q$ with $b^{m_\delta(R)} = 0$ and, moreover, $bI + Ib \subseteq I$ for an essential ideal I of R.*

Proof. For a prime $p \geq 2$, let e_p be the central idempotent of Q defined by the ideal Q_p of Q generated by all additive p-torsion elements in Q. That is, $Q_p = e_p Q$. We then

set $e_0 = 1 - \bigvee_p e_p$. Then e_0Q has characteristic zero. Replacing R by either $e_0Q \cap R$ or $e_pQ \cap R$, we may assume that R is a semiprime ring of characteristic either 0 or a prime p. By Theorem 3.3, there exist finitely many orthogonal central idempotents $e_1, \ldots, e_k$ in Q with $e_1 + \cdots + e_k = 1$ such that each $e_iQ \cap R$ is δ_i-homogeneous, where δ_i is the restriction of δ to $e_iQ \cap R$. Note that e_iQ is the symmetric Martindale quotient ring of $e_iQ \cap R$ by [1, Proposition 2.3.14]. It suffices to prove our assertions for each δ_i. Replacing R by $e_iQ \cap R$, we may assume that R is δ-homogeneous as described in Definition 2. For the case $\operatorname{char} R = 0$, let b, l be as described there. By Theorem 3.1, $m_\delta(R) = l$ and $n_\delta(R) = 2l - 1$. So $b^{m_\delta(R)} = 0$. For the case $\operatorname{char} R = p \geq 2$, let s, t, b, l, α be as described there. By Theorem 3.2, $m_\delta(R) = lp^{s+t}$ and $n_\delta(R)$ is as described there. Since p does not divide $m_\delta(R)$ or $n_\delta(R)$, we see that $s + t = 0$. So b satisfies $(b - \alpha)^l = 0$. Noting that $\operatorname{ad}(b) = \operatorname{ad}(b - \alpha)$ and replacing b by $b - \alpha$, we also have $b^l = b^{m_\delta(R)} = 0$. Now, we aim to find an essential ideal I such that $bI + Ib \subseteq I$: We let

$$I \stackrel{\text{def.}}{=} \{y \in R \mid b^i y \in R \text{ for all } i \geq 1\}.$$

Let $y \in I$. By induction on j, we show $b^i y b^j \in R$ for all $i, j \geq 0$: This is trivial if $j = 0$. For $j \geq 1$,

$$b^i y b^j = [b^i y b^{j-1}, b] + b^{i+1} y b^{j-1} \in R^\delta + R = R.$$

This implies $I = \{y \in R \mid y b^j \in R \text{ for all } j \geq 1\}$. So I is a two-sided ideal of R. Since $b \in Q$, there is an essential ideal J such that $b^i J \subseteq R$ for $1 \leq i < l$ and hence for all $i \geq 0$, since $b^l = 0$. This shows that I is essential, as asserted.

Acknowledgements The authors are thankful to the referee for her/his useful suggestions and comments. This research was supported by National Science Council of Taiwan.

References

[1] K.I. Beidar, W.S. Martindale 3rd and A.V. Mikhalev, "Rings with Generalized Identities", Marcel Dekker, Inc., New York–Basel–Hong Kong, 1996.

[2] K.I. Beidar and A.V. Mikhalëv, *Orthogonal completeness and algebraic system*, Uspekhi Mat. Nauk **40** (1985) 6, 79-115. English translation: Russian Math. Surveys, **40** (1985) 6, 51-95.

[3] L.O. Chung, Y. Kobayashi and J. Luh, *Remark on nilpotency of derivations*, Proc. Japan Acad. Ser. A **60**(1984), 329-330.

[4] C.-L. Chuang, *On compositions of derivations of prime rings*, Proc. Amer. Math. Soc. **108** (1990), 647-652.

[5] L.O. Chung and J. Luh, *Nilpotency of derivations*, Canad. Math. Bull. **26** (1983), 341-346.

[6] L.O. Chung and J. Luh, *Nilpotency of derivations. II*, Proc. Amer. Math. Soc. **91**(3) (1984), 357–358.

[7] T.S. Erickson, W.S. Martindale 3rd and J.M. Osborn, *Prime nonassociative algebras*, Pacific J. Math. **60** (1975), 49-53.

[8] N.J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly **54** (1947), 589-592.

[9] P. Grzeszczuk, *On nilpotent derivations of semiprime rings*, J. Algebra **149** (1992), 313-321.

[10] V.K. Kharchenko, *Differential identities of prime rings*, Algebra i Logika **17** (1978) 2, 220-238. English translation: Algebra and Logic, **17** (1978) 2, 154-168.

[11] V.K. Kharchenko, *Differential identities of semiprime rings*, Algebra i Logika **18** (1979) 1, 86-119. English translation: Algebra and Logic, **18** (1979) 1, 58-80.

[12] V.K. Kharchenko and A.Z. Popov, *Skew derivations of prime rings*, Comm. Algebra **20** (1992) 11, 3321-3345.

[13] T.-K. Lee, *Semiprime rings with differential identities*, Bull. Inst. Math. Acad. Sinica **20** (1992), 27-38.

[14] W.S. Martindale, 3rd, *Prime rings satisfying a generalized polynomial identity*, J. Algebra **12** (1969), 576-584.

[15] W.S. Martindale, 3rd and C. R. Miers, *On the iterates of derivations of prime rings*, Pacific J. Math. **104** (1983) 1, 179-190.

IDENTITIES WITH A SINGLE SKEW DERIVATION

Chen–Lian Chuang and Tsiu–Kwen Lee

Department of Mathematics
National Taiwan University
Taipei 106, TAIWAN
E–mail: chuang@math.ntu.edu.tw
E–mail: tklee@math.ntu.edu.tw

Abstract. Let R be a prime ring with extended centroid C and δ, a continuous skew derivation of R. We define the notion of K–polynomials which, in the case that δ is an ordinary derivation, reduces to polynomials of the form $x^{\delta^{p^n}}+\alpha_1 x^{\delta^{p^{n-1}}}+\cdots+\alpha_{n-1}x^{\delta}$,

where $\alpha_i \in C$. It is shown that all generalized identities with δ are consequences of GPIs of R and an identity in the form $\psi(x) = x^{\sigma^m} b - bx$, where $\psi(x)$ is a K–polynomial of minimal possible order m.

† 2000 *Mathematics Subject Classification.* 16W20, 16W25, 16W55.

‡ *Key words and phrases.* Automorphism, prime ring, skew derivation, GPI, K–polynomial.

1. Results

An associative ring R is called *prime* if for any $a, b \in R$, $aRb = 0$ implies $a = 0$ or $b = 0$. Throughout here, R will always be an associative prime ring. Let Q and $R_{\mathcal{F}}$ stand for respectively the symmetric and the left Martindale quotient rings of R. (See [2] for definitions.) The center C of Q is the same as that of $R_{\mathcal{F}}$ and is called the extended centroid of R. A map $\delta\colon R \to R$ is called *additive* if $(x+y)^\delta = x^\delta + y^\delta$ for $x, y \in R$. By a derivation of R, we mean an additive map $\delta\colon R \to R$ satisfying $(xy)^\delta = x^\delta y + xy^\delta$ for $x, y \in R$. Given $b \in R$, the map $\mathrm{ad}_b\colon x \in R \mapsto xb - bx$ obviously defines a derivation, called the inner derivation defined by b. We call a derivation *outer*, if it is not of this form. To analyze derivations of R, as shown in Kharchenko's theory [7, 8], we have to work in the larger ring Q. We introduce a topology on Q, which we may call the *ideal* topology, by endowing $x \in Q$ with the neighborhood system consisting of x plus a nonzero two-sided ideal of R. Let $g\colon Q \to Q$ be an additive map. We call g a continuous map of R if it is a continuous map with respect to the ideal topology. It is easy to check that a derivation δ of Q is continuous if and only if $I^\delta \subseteq R$ for some nonzero ideal I of R. Inner derivations of Q are obviously continuous. Any derivation of R can be uniquely extended to a continuous derivation of R. A continuous derivation of R is called X–inner or X–outer according as it is equal to an inner derivation of Q or not. A continuous derivation δ of R is said to be C–algebraic modulo inner derivations if there exist $b \in Q$ and $\beta_1, \cdots, \beta_{n-1} \in C$ such that

$$x^{\delta^n} + \beta_1 x^{\delta^{n-1}} + \beta_2 x^{\delta^{n-2}} + \cdots + \beta_{n-1} x^\delta = xb - bx$$

for all $x \in R$. We call n the δ–order or simply the order of the above algebraic dependence. Let σ be an automorphism of Q. We call σ a *bi–continuous* automorphism of R if both σ and σ^{-1} are continuous. Equivalently, there exist nonzero ideals I and J of R such that $J \subseteq I^\sigma \subseteq R$. Any automorphism of R can be uniquely extended to an automorphism of Q and gives rise to a bi–continuous automorphism of Q. Let $\mathcal{A}(R)$ be the set of bi–continuous automorphisms of R. It is shown in [9] that $\mathcal{A}(R)$ forms a group. We say that $g_1, g_2, \ldots \in \mathcal{A}(R)$ are mutually outer if $g_i^{-1} g_j$ is *not* X-inner for $i \neq j$. All generalized polynomials considered in the paper have coefficients in $R_{\mathcal{F}}$. Kharchenko's powerful theory of differential identities [7, 8] yields the following thorough analysis of GPIs with a single continuous derivation:

Theorem. (Kharchenko) *Let R be a prime ring and δ, an X–outer continuous derivation of R. If δ is not C–algebraic modulo inner derivations, then any GPI of the form $\varphi(x_i^{\delta^j g_k})$, where $g_k \in \mathcal{A}(R)$ are mutually outer, yields the GPI $\varphi(z_{ijk})$, where z_{ijk} are distinct indeterminates. If δ is C–algebraic modulo inner derivations, then (1)* $\mathrm{char}\, R = p \geq 2$*, (2) the algebraic dependence of minimal δ–order assumes*

the form

$$x^{\delta^{p^m}} + \alpha_1 x^{\delta^{p^{m-1}}} + \cdots + \alpha_{m-1} x^{\delta} = xb - bx$$

for some $\alpha_1, \ldots, \alpha_{m-1} \in C$*, and (3) any GPI of the form* $\varphi(x_i^{\delta^j g_k})_{j<p^m}$*, where* $g_k \in \mathcal{A}(R)$ *are mutually outer, yields the GPI* $\varphi(z_{ijk})_{j<p^m}$*, where* z_{ijk} *are distinct indeterminates.*

This theorem is actually a combined consequence of several theorems, all variously formulated for various purposes. For the sake of completeness, we provide a proof below. Let us recall some notions: A set S of continuous derivations of R is called outer independent if for any $\delta_1, \ldots, \delta_n$, any $\alpha_1, \ldots, \alpha_n \in C$ and any $b \in Q$, the condition $\alpha_1 x^{\delta_1} + \cdots + \alpha_n x^{\delta_n} = xb - bx$ for all $x \in R$ implies $\alpha_1 = \cdots = \alpha_n = 0$. We say the set S is ordered if S is endowed with a *linear* order $<$. By a regular word in an ordered independent set S of X–outer continuous derivations, we mean an expression of the form:

$$\delta_1^{s_1} \delta_2^{s_2} \cdots \delta_n^{s_n},$$

where (i) $\delta_i \in S$ are such that $\delta_1 < \delta_2 < \cdots < \delta_n$ and where (ii) each $s_i < \operatorname{char} R$ in case of $\operatorname{char} R = p \geq 2$.

Proof of the Theorem: We first show that all δ^i occurring in φ are regular words in an ordered outer independent set: If $\operatorname{char} R = 0$, then all δ^n are regular words in the ordered outer independent singleton set $\{\delta\}$. Assume $\operatorname{char} R = p \geq 2$. If $\delta, \delta^p, \delta^{p^2}, \ldots$ are outer independent, then we order them by $\delta < \delta^p < \delta^{p^2} < \cdots$. Any $k \geq 0$ can be written as $k = k_0 + k_1 p + k_2 p^2 + \cdots$, where each $0 \leq k_i < p$. So $\delta^k = \delta^{k_0} (\delta^p)^{k_1} (\delta^{p^2})^{k_2} \cdots$ is a regular word in this ordered outer independent set. If $\delta, \delta^p, \delta^{p^2}, \ldots$ are dependent modulo inner derivations, let n be the largest such that $\delta, \delta^p, \ldots, \delta^{p^{n-1}}$ are independent modulo inner derivations. We order $\delta, \ldots, \delta^{p^{n-1}}$ by $\delta < \cdots < \delta^{p^{n-1}}$. For $0 \leq k < p^n = m$, we write $k = k_0 + k_1 p + \cdots + k_{n-1} p^{n-1}$, where each $0 \leq k_i < p$. So $\delta^k = \delta^{k_0} (\delta^p)^{k_1} \cdots (\delta^{p^{n-1}})^{k_{n-1}}$ is a regular word in the ordered outer independent set $\{\delta, \ldots, \delta^{p^{n-1}}\}$. We recall two more notions: An automorphism h of Q is called Frobenius if, in the case of $\operatorname{char} R = 0$, $\alpha^h = \alpha$ for $\alpha \in C$ and if, in the case of $\operatorname{char} R = p \geq 2$, $\alpha^h = \alpha^{p^n}$ for $\alpha \in C$, where n is an fixed integer, which may be zero, positive or negative. Automorphisms $h_1, h_2, \ldots$ are said to be *strongly independent* if $h_i h_j^{-1}$ is not Frobenius for $i \neq j$. We then show that the mutually outer automorphisms g_k are strongly independent: Assume on the contrary that $h \overset{\text{def.}}{=} g_i g_j^{-1}$ is Frobenius for some $i \neq j$. If $\operatorname{char} R = p \geq 2$ and there exists $n \neq 0$ such that $\alpha^h = \alpha^{p^n}$ for all $\alpha \in C$, then $C = C^p$ and hence $C^\delta = (C^p)^\delta = 0$.

If φ is trivial, then there is nothing to prove. Thus we may assume that φ is nontrivial. In view of Corollary p.371 [3], R is a GPI–ring and so δ is X–inner by a result in p.68 [8]. This contradicts our assumption. If $\alpha^h = \alpha$ for all $\alpha \in C$, then h is X–inner by a result in p.140 [6]. This is absurd again, since $g_1, g_2, \ldots$ are mutually outer. So g_k occurring in φ are indeed strongly independent. The desired assertion of our Theorem now follows immediately from Theorem 2 of [4] (cited as Main Theorem in the abstract).

Our aim here is to generalize this theorem to skew derivations, which we define now: Let σ, τ be automorphisms of a ring R. By a (σ, τ)–derivation of R, we mean an additive map $\delta\colon R \to R$ satisfying $(xy)^\delta = x^\sigma y^\delta + x^\delta y^\tau$ for $x, y \in R$. Given $b \in R$, the map $\delta\colon x \in R \mapsto x^\sigma b - bx^\tau$ obviously defines a (σ, τ)–derivation, called the inner (σ, τ)–derivation defined by b. A (σ, τ)–derivation not of this form is called *outer*. If τ is the identity automorphism $\tau\colon x \mapsto x$, then (σ, τ)–derivations are particularly called σ–derivations. For brevity, σ–derivations are generally called skew derivations.

Just as in Kharchenko's theory, we can*not* simply sit in R but instead, we have to work in the symmetric Martindale quotient ring Q. Following Kharchenko and Popov [8], we define, for $\sigma, \tau \in \mathcal{A}(R)$,

$$\mathcal{L}_{\sigma,\tau}(R) \overset{\text{def.}}{=} \text{the set of continuous } (\sigma, \tau)\text{–derivations of } R,$$

$$\mathcal{L}_{\sigma}(R) \overset{\text{def.}}{=} \text{the set of continuous } \sigma\text{–derivations of } R,$$

$$\mathcal{L}(R) \overset{\text{def.}}{=} \bigcup_{\sigma \in \mathcal{A}(R)} \mathcal{L}_\sigma(R).$$

For brevity, we may simply call elements of $\mathcal{L}(R)$ continuous skew derivations of R. Just like ordinary derivations, any (σ, τ)–derivation of R, together with its automorphisms σ, τ, can be uniquely extended to an element in $\mathcal{L}_{\sigma,\tau}(R)$ with $\sigma, \tau \in \mathcal{A}(R)$. This can be easily verified. All skew derivations considered here will be continuous.

The notion of algebraicity with coefficients in C turns out to be too restrictive for skew derivations, as shown in the following:

Example 1. Assume that $\operatorname{char} R = p \geq 2$. Let d be an outer ordinary derivation which is C–algebraic modulo inner derivations. By Kharchenko's Theorem cited above, the algebraic dependence relation of minimal δ–order assumes the form

$$x^{d^{p^n}} + \alpha_1 x^{d^{p^n-1}} + \cdots + \alpha_n x^d = xb - bx$$

where $\alpha_i \in C$ and $b \in Q$. Given a unit $u \in Q$, the map $\delta\colon x \mapsto ux^d$ defines a σ–derivation, where σ is the inner automorphism defined by u, i.e., $x^\sigma = uxu^{-1}$. A direct computation shows that

$$x^{\delta^k} = u^k x^{d^k} + \text{terms of the form } ax^{d^i}, \text{ where } a \in Q \text{ and } 1 \leq i < k.$$

Using this, we see that δ satisfies an identity of the form

$$x^{\delta^{p^n}} + t_1 x^{\delta^{p^n-1}} + \cdots + t_{p^n-1} x^\delta = u^{p^n}(xb - bx),$$

where $t_1, \ldots, t_{p^n-1} \in Q$. Note that the map $x \mapsto u^{p^n}(xb - bx)$ defines an X–inner σ^{p^n}–derivation. Conversely, by substituting ux^d for x^δ, an identity for δ will yield an identity of the same order for d, which by Kharchenko's theory, must be of order $\geq p^n$. So the above identity for δ is of minimal δ–order and is unique. Obviously, some t_i may *not* be in C and also some δ^i occurring in the above expression may *not* be of the form δ^{p^s}. In spite of these, the above identity for δ is most important, for it

is most closely related to the minimal identity for d, which gives the most important information of d and hence of δ also.

The more general notion introduced by Leroy [12] in the following is suitable for our purpose here:

Definition: We say that $\delta \in \mathcal{L}_\sigma(R)$ is left $R_{\mathcal{F}}$–algebraic modulo inner skew derivations if there exist $g \in \mathcal{A}(R)$ and $b_0 \neq 0, \ldots, b_{n-1}, b \in R_{\mathcal{F}}$ such that for all $x \in R$,

$$b_0 x^{\delta^n} + b_1 x^{\delta^{n-1}} + b_2 x^{\delta^{n-2}} + \cdots + b_{n-1} x^{\delta} = x^g b - bx.$$

The algebraicity with coefficients in C surely implies the left algebraicity with coefficients in $R_{\mathcal{F}}$. The two notions are equivalent for ordinary derivations by Kharchenko's Theorem just cited. However, this is not true in general as shown in the following example:

Example 2. (Koryukin [11]) Let δ be a continuous σ–derivation such that $\sigma\delta + \delta\sigma$ is the inner (σ^2, σ)–derivation defined by $-a \in Q$: $x^{\sigma\delta+\delta\sigma} = x^{\sigma^2}(-a) - (-a)x^\sigma$ for $x \in R$. Koryukin observed that the map $\psi(x) \stackrel{\text{def.}}{=} x^{\delta^2} - ax^\delta$ defines a σ^2–derivation. With this, he constructed an δ satisfying $x^{\delta^2} - ax^\delta = 0$: Let C be a field and let R be the free C–algebra with free generators a_i, where i ranges over all integers except -1. Then R coincides with its symmetric Martindale quotient ring and C is the extended centroid of R (see [1]). Set $a \stackrel{\text{def.}}{=} a_0$ and $a_{-1} \stackrel{\text{def.}}{=} 0$. The C–linear map $\sigma\colon a_j \mapsto a - a_{j+1}$ has the inverse $\sigma^{-1}\colon a_j \mapsto a_{-2} - a_{j-1}$ and hence extends to an automorphism of R. Let δ be the σ–derivation defined by the map $\delta\colon a_j \mapsto a_{j+1}a_j$. Then $x^{\sigma\delta+\delta\sigma} = x^{\sigma^2}(-a) - (-a)x^\sigma$ for $x \in R$. We verify easily that $x^{\delta^2} - ax^\delta = 0$ for $x = a_j$. Since these a_j generate R and the map $\psi\colon x \mapsto x^{\delta^2} - ax^\delta$ is a σ^2–derivation, we have $x^{\delta^2} - ax^\delta = 0$ for all $x \in R$. Inductively, for $n \geq 1$, $x^{\delta^n} = a^{n-1}x^\delta$ for all $x \in R$. Thus δ is not C–algebraic, since the C–algebraicity of δ implies the C–algebraicity of a. Moreover, an easy computation can prove that δ is X–outer.

Our results are based on a generalization of Koryukin's identity. To simplify our notation, we introduce the following: Given $t \in Q$, we let $r(t)$, $\ell(t)$ denote respectively the right and the left multiplication by t:

$$r(t)\colon x \in Q \mapsto xt \qquad \text{and} \qquad \ell(t)\colon x \in Q \mapsto tx.$$

Let $\delta \in \mathcal{L}_\sigma(R)$ and let $D_{s,t}$, where $s, t \geq 0$, denote the sum of all distinct products with s δ's and t σ's. For instance, $D_{1,1} = \delta\sigma + \sigma\delta$ and $D_{2,1} = \delta^2\sigma + \delta\sigma\delta + \sigma\delta^2$, etc.. A direct computation proves that

$$(xy)^{\delta^n} = \sum_{i=0}^{n} x^{D_{i,n-i}} y^{\delta^{n-i}}$$

for $x, y \in R$.

Lemma 1. *Let $\delta \in \mathcal{L}_\sigma(R)$. Given $0 \leq n \leq m$, if there exist $t_1, \ldots, t_{n-1} \in Q$ such that*

$$\psi_k \stackrel{\text{def.}}{=} D_{k,m-k} + \sum_{j=1}^{k-1} D_{k-j,m-k}\ell(t_j) = \sigma^m r(t_k) - \sigma^{m-k}\ell(t_k)$$

for $k = 1, \ldots, n-1$, then the map

$$\psi_n \stackrel{\text{def.}}{=} D_{n,m-n} + \sum_{j=1}^{n-1} D_{n-j,m-n}\ell(t_j)$$

defines a (σ^m, σ^{m-n})–derivation from Q into Q.

We adopt Sweedler's notation [15] to simplify our presentation: Given additive maps $\epsilon, \epsilon_i, \epsilon'_i$ of Q into Q, we write

$$\Delta(\epsilon) = \sum_i \epsilon_i \otimes \epsilon'_i,$$

where the tensor product $\otimes$ is taken over the ring of integers, to denote that

$$(xy)^\epsilon = \sum_i x^{\epsilon_i} y^{\epsilon'_i}$$

for all $x \in Q$. For example, if $t \in Q$, $\sigma \in \mathcal{A}(R)$ and $\delta \in \mathcal{L}_\sigma(R)$, then

$$\begin{aligned}
&\Delta(r(t)) = 1 \otimes r(t),\\
&\Delta(\ell(t)) = \ell(t) \otimes 1,\\
&\Delta(\sigma) = \sigma \otimes \sigma,\\
&\Delta(\delta) = \sigma \otimes \delta + \delta \otimes 1.
\end{aligned}$$

Clearly, we have $\Delta(\epsilon\epsilon') = \Delta(\epsilon)\Delta(\epsilon')$ for additive maps ϵ, ϵ' of Q. Using this, we have

$$\Delta(\delta^n) = \sum_{i=0}^{n} D_{i,n-i} \otimes \delta^{n-i}$$

for $\delta \in \mathcal{L}_\sigma(R)$. More generally, we have

$$\Delta(D_{s,t}) = \sum_{i=0}^{s} D_{s-i,t+i} \otimes D_{i,t}.$$

These can be easily verified. Finally, we observe an equality: $r(t) \otimes 1 = 1 \otimes \ell(t)$. We are ready for:

Proof of Lemma 1: Set $t_0 \stackrel{\text{def.}}{=} 1$. We can thus write $\psi_k = \sum_{j=0}^{k-1} D_{k-j,m-k}\ell(t_j)$ for $k = 1, \ldots, n$. Since $D_{0,m-k} = \sigma^{m-k}$, we have, for $k = 1, \ldots, n-1$,

$$\begin{aligned}
&\sum_{j=0}^{k} D_{k-j,m-k}\ell(t_j)\\
=&\sum_{j=0}^{k-1} D_{k-j,m-k}\ell(t_j) + D_{0,m-k}\ell(t_k) = \psi_k + \sigma^{m-k}\ell(t_k) = \sigma^m r(t_k).
\end{aligned}$$

With these, we compute

$$\begin{aligned}
\Delta(\psi_n) &= \Delta\Big(\sum_{j=0}^{n-1} D_{n-j,m-n}\ell(t_j)\Big) \\
&= \sum_{j=0}^{n-1} \Delta\big(D_{n-j,m-n}\ell(t_j)\big) \\
&= \sum_{j=0}^{n-1} \Big(\sum_{s=0}^{n-j} D_{n-j-s,m-n+s}\ell(t_j)) \otimes D_{s,m-n}\Big) \\
&= \sum_{j=0}^{n-1}\sum_{k=j}^{n} D_{k-j,m-k}\ell(t_j) \otimes D_{n-k,m-n} \qquad \text{(by setting } k \stackrel{\text{def.}}{=} n-s\text{)} \\
&= \sum_{k=0}^{n-1}\sum_{j=0}^{k} D_{k-j,m-k}\ell(t_j) \otimes D_{n-k,m-n} + \sum_{j=0}^{n-1} D_{n-j,m-n}\ell(t_j) \otimes D_{0,m-n} \\
&\qquad \text{(by switching summations and singling out summands with } k=n\text{)} \\
&= \sum_{k=0}^{n-1} \sigma^m r(t_k) \otimes D_{n-k,m-n} + \psi_n \otimes \sigma^{m-n} \\
&= \sigma^m \otimes \sum_{k=0}^{n-1} D_{n-k,m-n}\ell(t_k) + \psi_n \otimes \sigma^{m-n} \\
&= \sigma^m \otimes \psi_n + \psi_n \otimes \sigma^{m-n}.
\end{aligned}$$

This proves that ψ_n is a (σ^m, σ^{m-n})–derivation, as asserted.

When $n = m$ in Lemma 1 above, the GP ψ_m involves only the skew derivation δ and no automorphism σ, that is, no $D_{s,t}$ with $t > 0$ occur in ψ_n. Such GPs are of crucial importance to us. It is convenient to give a specific name for them:

Definition: Let $\delta \in \mathcal{L}_\sigma(R)$. By a Koryukin polynomial of δ or K–polynomial for short, we mean an expression of the form:

$$\psi(x) = x^{\delta^m} + \sum_{j=1}^{m-1} t_j x^{\delta^{m-j}},$$

where $t_1, \ldots, t_{m-1} \in Q$, $m \geq 1$, satisfy

$$D_{k,m-k} + \sum_{j=1}^{k-1} D_{k-j,m-k}\ell(t_j) = \sigma^m r(t_k) - \sigma^{m-k}\ell(t_k)$$

for $k = 1, \ldots, m-1$. By Lemma 1, $\psi(x)$ defines a σ^m–derivation μ of Q. We call the expression $\psi(x) - x^\mu$ a Koryukin identity or K–identity for short. We call

m the δ–order or simply the order of the K–polynomial ψ and of the K–identity $\psi(x) - x^{\mu}$. In particular, x^{δ} is the K–polynomial of δ of δ–order 1. We remark that our K–polynomials are closely related to right semi-invariant polynomials introduced in [13]. We explore their connections elsewhere.

We are now ready to state our main

Theorem 1. *Let R be a prime ring and δ, an X–outer continuous σ–derivation of R. If δ is not left $R_{\mathcal{F}}$–algebraic modulo inner skew derivations, then any GPI of the form $\varphi(x_i^{\delta^j g_k})$, where $g_k \in \mathcal{A}(R)$ are mutually outer, yields the GPI $\varphi(z_{ijk})$, where z_{ijk} are distinct indeterminates. If δ is left $R_{\mathcal{F}}$–algebraic modulo inner skew derivations, then (i) such algebraic dependence of minimal δ–order assumes the form*

$$\psi(x) = x^{\sigma^m} b - bx,$$

where $b \in Q$ and $\psi(x)$ is a K–polynomial of δ–order $m \geq 1$ and (ii) any GPI of the form $\varphi(x_i^{\delta^j g_k})_{j<m}$, where $g_j \in \mathcal{A}(R)$ are mutually outer, yields the GPI $\varphi(z_{ijk})_{j<m}$, where z_{ijk} are distinct indeterminates.

This was originally obtained by the result in [5]. But our proof presented here is independent of [5]. Before proceeding, it is instructive to examine our Theorem 1 for the familiar ordinary derivations:

Example 3. We need a simple number theoretic result: Let p be a prime ≥ 2. For integer $k \geq 1$, if $(p, k) = 1$, then $\binom{p^n k}{p^n} \equiv_p k$. To see this, we write

$$\binom{p^n k}{p^n} = \frac{p^n k(p^n k - 1)(p^n k - 2) \cdots (p^n k - i) \cdots (p^n k - p^n + 1)}{1 \cdot 2 \cdots i \cdots p^n}.$$

For $1 \leq i < p^n$, if $i = p^s i_0$, where $(p, i_0) = 1$, then $s < n$ and

$$\frac{(p^n k - i)}{i} = \frac{(p^n k - p^s i_0)}{p^s i_0} = \frac{p^{n-s} k - i_0}{i_0} \equiv_p \frac{-i_0}{i_0} = -1.$$

So $\binom{p^n k}{p^n} \equiv_p (-1)^{p^n - 1} k \equiv_p k$ follows.

From this, we deduce immediately that if $\binom{l}{i} \equiv_p 0$ for all $0 < i < l$, then l must be a power of p. Now, let δ be a continuous ordinary derivation and let

$$\psi(x) = x^{\delta^m} + \sum_{j=1}^{m-1} t_j x^{\delta^{m-j}},$$

be the K–polynomial of the minimal δ–order which defines an X–inner derivation. Setting $t_0 \stackrel{\text{def.}}{=} 1$, we have, for each $0 < k < m$, the equality

$$\sum_{j=0}^{k-1} t_j x^{D_{k-j,m-k}} = x^{D_{k,m-k}} + \sum_{j=1}^{k-1} t_j x^{D_{k-j,m-k}} = x t_k - t_k x$$

for $x \in Q$. Since σ is the identity automorphism, we have $D_{s,t} = \binom{s+t}{s}\delta^s$. So the equalities above are actually polynomial expressions in δ. By the minimality of m, these equalities must be trivial in the sense that for each $0 \leq j \leq k-1$, either $t_j = 0$ or $D_{k-j,m-k} = 0$. Since $t_0 \overset{\text{def.}}{=} 1$ is nonzero, the characteristic of R must be a prime $p \geq 2$. Also, if $t_j \neq 0$, then $\binom{m-j}{k-j} \equiv_p 0$ for all $j < k < m$ and $m-j$ is hence a power of p. We have thus shown that $m-j$ is a p–power if $t_j \neq 0$. Also, since $xt_k - t_k x = \sum_{j=0}^{k-1} t_j x^{D_{k-j,m-k}} = 0$ for $x \in Q$, it follows that $t_k \in C$. We may rewrite

$$\psi(x) = x^{\delta^{p^n}} + \alpha_1 x^{\delta^{p^{n-1}}} + \cdots + \alpha_n x^{\delta},$$

where $m = p^n$ and $\alpha_1, \ldots, \alpha_n \in C$. By the minimality of $m = p^n$, n is the minimal integer such that δ^{p^n} is a C–linear combination of $\delta, \delta^p, \ldots, \delta^{p^{n-1}}$ modulo inner derivations. So our Theorem 1 does coincide with Kharchenko's Theorem.

Consider an identity of the more general form $\phi(x_i^{\delta^j g_k})$, which may *not* be of the form described in Theorem 1. We transform it into the form of Theorem 1 as follows: Firstly, if δ is left $R_{\mathcal{F}}$–algebraic modulo inner skew derivations, we let m be the minimal order of such algebraic dependence and let

$$\psi(x) = x^{\delta^m} + t_1 x^{\delta^{m-1}} + \cdots + t_{m-1} x^{\delta},$$

where $t_1, \ldots, t_{m-1} \in Q$, be the K–polynomial of δ–order m such that for some $b \in Q$, $\psi(x) = x^{\sigma^m} b - bx$ for $x \in Q$. For $n > m$, the equality

$$\psi(x^{\delta^{n-m}}) = x^{\delta^n} + t_1 x^{\delta^{n-1}} + \cdots + t_{m-1} x^{\delta^{n-m+1}} = x^{\delta^{n-m}\sigma^m} b - b x^{\delta^{n-m}}$$

gives an expression of x^{δ^n} in terms of $x^{\delta^i g}$, where $i < n$ and $g \in \mathcal{A}(R)$. With this, we may reduce the power of δ consecutively and finally obtain an expression $\phi'(x_i^{\delta^j g_k})_{j<m}$, where only δ^j, $j < m$, occur nontrivially. If δ is *not* left $R_{\mathcal{F}}$–algebraic modulo X–inner skew derivations, then we simply set $\phi'(x_i^{\delta^j g_k})$ to be $\phi(x_i^{\delta^j g_k})$. Secondly, for $g, h \in \mathcal{A}(R)$, if $g^{-1}h$ is X–inner, say $x^{g^{-1}h} = uxu^{-1}$, then by replacing x by x^g, we have $x^h = ux^g u^{-1}$. With these, we can make all automorphisms involved mutually outer and thus transform $\phi'(x_i^{\delta^j g_k})$ into the form described in Theorem 1. We may call the expression thus obtained a *reduced* form of $\phi(x_i^{\delta^j g_k})$. Let us call the identity $\phi(x_i^{\delta^j g_k})$ trivial or nontrivial according as its reduced expression is trivial or not respectively. Thus we have:

Corollary 1 *If a prime ring R satisfies a nontrivial identity of the form $\phi(x_i^{\delta^j g_k})$, where $\delta \in \mathcal{L}(R)$ and $g_k \in \mathcal{A}(R)$, then R is a GPI–ring.*

Corollary 2 *All identities of the form $\phi(x_i^{\delta^j g_k})$, where $\delta \in \mathcal{L}(R)$ and $g_k \in \mathcal{A}(R)$ are consequences of GPIs of R, the K–identity of minimal order in the form $\psi(x) = x^{\sigma^m} b - bx$ and identities of the form $x^h = ux^g u^{-1}$, where $g, h \in \mathcal{A}(R)$ and $u \in Q$ is a unit.*

For convenience of applications, we also include the following:

Theorem 2 *Given $\delta \in \mathcal{L}_\sigma(R)$, if a GP of the form $\varphi(x_i^{\delta^j g_k})$, where $g_k \in \mathcal{A}(R)$, vanishes on a nonzero two–sided ideal of R, then it also vanishes on $R_\mathcal{F}$.*

As an immediate application, if $\sum_{j=0}^m q_j x^{\delta^j} = 0$, where $q_0, \cdots, q_m \in R_\mathcal{F}$, for all $x \in R$, then $q_0 = 0$. This follows by substituting $x = 1$, since the equation also holds on $R_\mathcal{F}$ by Theorem 2. This is proved by Leroy (Proposition 1 [12]) with the additional assumption that δ and σ commute.

2. Proofs of Theorems

We examine a nice property of K–polynomials:

Lemma 2. *Let $\psi(x)$ be a K–polynomial of δ–order m. Then any K–polynomial of order m, different from $\psi(x)$, assumes the form $\psi(x) + u\theta(x)$, where $\theta(x)$ is a K–polynomial of δ–order ℓ, $\ell < m$, such that $\sigma^{m-\ell}$ is an X–inner automorphism defined by the unit $u \in Q$. Conversely, for any such $\theta(x)$, $\psi(x) + u\theta(x)$ indeed defines a K–polynomial of δ–order m.*

Proof. Assume that $\phi(x)$, different from $\psi(x)$, is another K–polynomial also of δ–order m. Let us write

$$\psi(x) = x^{\delta^m} + \sum_{j=1}^{m-1} a_j x^{\delta^{m-j}} \qquad \text{and} \qquad \phi(x) = x^{\delta^m} + \sum_{j=1}^{m-1} b_j x^{\delta^{m-j}}.$$

The definition of K–polynomials gives the equalities

$$x^{D_{i,m-i}} + \sum_{j=1}^{i-1} a_j x^{D_{i-j,m-i}} = x^{\sigma^m} a_i - a_i x^{\sigma^{m-i}},$$
$$x^{D_{i,m-i}} + \sum_{j=1}^{i-1} b_j x^{D_{i-j,m-i}} = x^{\sigma^m} b_i - b_i x^{\sigma^{m-i}}$$

for $i = 1, \ldots, m-1$. Take the difference of their defining conditions for $D_{s,t}$. We have

$$(*) \qquad \sum_{j=1}^{i-1} (b_j - a_j) x^{D_{i-j,m-i}} = x^{\sigma^m}(b_i - a_i) - (b_i - a_i) x^{\sigma^{m-i}}$$

for $1 \le i \le m-1$. Since ϕ is different from ψ, we let n be the least i such that $b_i - a_i \neq 0$. For $i = 1, \ldots, n-1$, the equality above is thus trivial. For $i = n$, the left side of the equality above is 0 and the right side gives

$$x^{\sigma^m}(b_n - a_n) - (b_n - a_n) x^{\sigma^{m-n}} = 0$$

for $x \in Q$. Hence $u \stackrel{\text{def.}}{=} b_n - a_n$ is a unit and defines the inner automorphism σ^n. For $i \geq n$, we set $c_{i-n} \stackrel{\text{def.}}{=} u^{-1}(b_i - a_i)$. Dropping terms with $b_i - a_i = 0$ for $i < n$, we rewrite the equality $(*)$ for $i > n$ in terms of c_{i-n}:

$$\sum_{j=n}^{i-1} uc_{j-n}x^{D_{i-j,m-i}} = x^{\sigma^m}uc_{i-n} - uc_{i-n}x^{\sigma^{m-i}}$$

for $i = n+1, \ldots, m-1$. Set $s \stackrel{\text{def.}}{=} i-n$, $k \stackrel{\text{def.}}{=} j-n$, $\ell \stackrel{\text{def.}}{=} m-n$ and use $uxu^{-1} = x^{\sigma^n}$. It follws that

$$\sum_{k=0}^{s-1} c_k x^{D_{s-k,m-n-s}} = x^{\sigma^{m-n}}c_s - c_s x^{\sigma^{m-n-s}}$$

for $s = 1, \ldots, m-n-1$. That is,

$$\sum_{k=0}^{s-1} c_k x^{D_{s-k,\ell-s}} = x^{\sigma^\ell}c_s - c_s x^{\sigma^{\ell-s}}$$

for $s = 1, \ldots, \ell - 1$. By Lemma 1, these equalities show that

$$\theta(x) \stackrel{\text{def.}}{=} \sum_{k=0}^{\ell-1} c_k x^{\delta^{\ell-k}} = x^{\delta^\ell} + \sum_{k=1}^{\ell-1} c_k x^{\delta^{\ell-k}}$$

is a K–polynomial. Moreover, we have $\phi(x) = \psi(x) + u\theta(x)$. The second assertion follows by reversing the argument. This proves the lemma.

Lemma 3. *Let $\delta \in \mathcal{L}_{\sigma,\tau}(R)$. For $a \neq 0, b, t \in R_{\mathcal{F}}$, if $ax^\delta + bx^\tau = ax^\sigma t$ holds for all x in a nonzero two–sided ideal I of R, then $t \in Q$, $b = at$ and $x^\delta = x^\sigma t - tx^\tau$ for all $x \in R_{\mathcal{F}}$.*

Proof. Note that δ, together with their automorphisms σ, τ, can be uniquely extended to $R_{\mathcal{F}}$. Let $y \in R_{\mathcal{F}}$ be arbitrary. Pick a two–sided ideal J of R such that $0 \neq J \subseteq I$ and $Jy \subseteq I$. For $x \in J$, we have $xy \in I$ and hence $a(xy)^\delta + b(xy)^\tau = a(xy)^\sigma t$. Expand this: $ax^\sigma y^\delta + ax^\delta y^\tau + bx^\tau y^\tau = ax^\sigma y^\sigma t$. Replace ax^δ by $ax^\sigma t - bx^\tau$ in this expression. It follows that $ax^\sigma\big(y^\delta + ty^\tau - y^\sigma t\big) = 0$. So $a^{\sigma^{-1}}J\big(y^\delta + ty^\tau - y^\sigma t\big)^{\sigma^{-1}} = 0$. Since $a \neq 0$, the primeness of R implies that $y^\delta = y^\sigma t - ty^\tau$. Since $y \in R_{\mathcal{F}}$ is arbitrary, we have $x^\delta = x^\sigma t - tx^\tau$ for all $x \in R_{\mathcal{F}}$. Substitute this expression of δ back into $ax^\delta + bx^\tau = ax^\sigma t$. We have $a(x^\sigma t - tx^\tau) + bx^\tau = ax^\sigma t$, implying that $(b - at)x^\tau = 0$. So $(b - at)^{\tau^{-1}}R = 0$ and hence $b = at$. We show $t \in Q$: By the continuity of δ and σ, we pick an ideal $J \neq 0$ of R such that $J^\delta \subseteq R$ and such that $J^\sigma t \subseteq R$. We have $tJ^\tau \subseteq J^\sigma t + J^\delta \subseteq R$. By the continuity of τ^{-1}, J^τ contains a nonzero two–sided ideal of R. So $t \in Q$ follows. This proves the lemma.

It is convenient to have the following:

Definition: (1) Given $\delta \in \mathcal{L}(R)$, let $\Gamma(\delta)$ be the set of expressions of the form

$$\varphi(x) = \sum_{i \geq 0} \sum_{j,k} b_{ijk} x^{\delta^i g_j} c_{ijk},$$

where $b_{ijk}, c_{ijk} \in R_{\mathcal{F}}$ and $g_j \in \mathcal{A}(R)$. The largest i such that δ^i occurs nontrivially in $\varphi(x)$ is called the δ–order or simply the order of φ.

(2) Let Λ be the set of expressions of the form

$$\varphi(x) = \sum_{i,j} a_{ij} x^{g_i} b_{ij},$$

where $a_{ij}, b_{ij} \in R_{\mathcal{F}}$ and $g_i \in \mathcal{A}(R)$. For a finite subset S of $\mathcal{L}(R)$, let $\Lambda(S)$ be the set of expressions in the form

$$\sum_{\mu \in S} \sum_{j,k} a_{\mu jk} x^{\mu g_j} b_{\mu jk} + \lambda(x),$$

where $b_{\mu jk}, c_{\mu jk} \in R_{\mathcal{F}}$, where $g_j \in \mathcal{A}(R)$ and where $\lambda(x) \in \Lambda$. Note that $\Lambda(\emptyset) \stackrel{\text{def.}}{=} \Lambda$.

(3) We say that $\varphi(x) \in \Gamma(\delta)$ is defined by $\Lambda(S)$ if there exists $\rho(x) \in \Lambda(S)$ such that $\varphi(x) = \rho(x)$ for all $x \in R$.

We have come to the crucial step:

Lemma 4. (Existence of K–polynomials) *Let $\delta \in \mathcal{L}_\sigma(R)$ be X–outer and $S \subseteq \mathcal{L}(R)$, empty or nonempty. If there exists $\varphi(x) \in \Gamma(\delta)$ of δ–order $m \geq 1$ which is defined by $\Lambda(S)$, then δ has a K–polynomial of δ–order $\leq m$, which is also defined by $\Lambda(S)$.*

We have to use Proposition 9 [10]. Let us explain some notions there: We say that $\delta_i \in \mathcal{L}_{\sigma_i}(R)$, $i = 1, 2, \ldots$, are reduced if σ_i, σ_j are mutually outer for $\sigma_i \neq \sigma_j$ and if for any given $g \in \mathcal{A}(R)$, no nontrivial C–linear combination of δ_i with $\sigma_i = g$ can be X–inner. Let $\delta_{i_1}, \delta_{i_2}, \ldots$ enumerate those δ_i with $\sigma_i = g$. The second condition above says that if $x \mapsto \alpha_1 x^{\delta_{i_1}} + \alpha_2 x^{\delta_{i_2}} + \cdots$, where $\alpha_i \in C$ vanish for all but finitely many i, defines an inner g–derivation, then all $\alpha_i = 0$. Proposition 9 [10] says that any linear GPI with mutually outer automorphisms and a reduced set of skew derivations is trivial. It is convenient here to have the following more general notion of [6, 10]: For $g \in \mathcal{A}(R)$, we define $\Phi_g \stackrel{\text{def.}}{=} \{u \in Q \mid ux^g = xu \quad \text{for all } x \in Q\}$. We say that $\delta_i \in \mathcal{L}_{\sigma_i}(R)$, $i = 1, 2, \ldots$, are outer independent if the following condition is satisfied: For any $g \in \mathcal{A}(R)$ and $u_i \in \Phi_{g^{-1}\sigma_i}$, if $x \mapsto \sum_i u_i x^{\delta_i}$ (a finite sum) defines an inner g–derivation of Q, then all $u_i = 0$. Given $\delta_i \in \mathcal{L}_{\sigma_i}(R)$, let us fix a maximal mutually outer subset of automorphisms σ_i, say τ_j, $j = 1, 2, \ldots$. If σ_i and τ_j are equivalent modulo inner automorphisms, then the map $\partial_i \colon x \mapsto u_i x^{\delta_i}$, where $u_i \in \Phi_{\tau_j^{-1}\sigma_i}$ defines a τ_j–derivation. Obviously, $\delta_i \in \mathcal{L}_{\sigma_i}(R)$ are outer independent if and only if the set ∂_i are reduced. We can thus write

Proposition 9 [10] (Restated). *Any linear GPI with mutually outer automorphisms and with outer independent skew derivations is trivial.*

Here skew derivations are put on the left hand side of automorphisms. But the same proposition remains valid if skew derivations are put on the right hand side of automorphisms. This can be proved in the same way or deduced immediately from the original statement. We are now ready for

Proof of Lemma 4: Let T be a maximal outer independent subset of S. The expressions defined by $\Lambda(S)$ and by $\Lambda(T)$ are the same. Replacing S by T, we may assume that S is outer independent. We may also assume that the δ–order m of $\varphi(x) \in \Gamma(\delta)$ is minimum possible among all generalized polynomials of $\Gamma(\delta)$ which have δ–order ≥ 1 and which are defined by $\Lambda(S)$. We may assume $m > 1$, for otherwise the K–polynomial $\psi(x) = x^\delta$ is already defined by $\Lambda(S)$ by Proposition 9 [10]. Let $\rho(x) \in \Lambda(S)$ be such that $\varphi(x) = \rho(x)$ for $x \in R$. For any $u_s, v_s \in R$, $\sum_s v_s\rho(u_s x) \in \Lambda(S)$ and $\sum_s v_s\varphi(u_s x) = \sum_s v_s\rho(u_s x)$ holds for $x \in R$. So $\sum_s v_s\varphi(u_s x)$ is also defined by $\Lambda(S)$. We shall choose various u_s, v_s to simplify $\varphi(x)$. Write

$$\varphi(x) = \sum_{i=0}^{m} \sum_{j} \sum_{k=1}^{k_{ij}} b_{ijk} x^{\delta^i g_j} c_{ijk},$$

where $g_j \in \mathcal{A}(R)$ may be assumed to be mutually outer. Let us choose $\varphi(x)$ such that $\sum_j k_{mj}$, the number of terms involving δ^m, is minimal possible. We *claim* that $\sum_j k_{mj} = 1$: Suppose on the contrary that $\sum_j k_{mj} > 1$. By the minimality of $\sum_j k_{mj}$, for each j, the set $\{b_{mjk} : k = 1, \ldots, k_{mj}\}$ is C–independent. Since g_j are mutually outer, so are $\sigma^m g_j$. By Proposition 1 [6], there exist $u_s, v_s \in R$ such that $\sum_s v_s b_{m11} u_s^{\sigma^m g_1} \neq 0$ but such that $\sum_s v_s b_{mjk} u_s^{\sigma^m g_j} = 0$ for all $(j,k) \neq (1,1)$. The only term in $\sum_s v_s\varphi(u_s x)$ involving δ^m is then

$$\big(\sum_s v_s b_{m11} u_s^{\sigma^m g_1}\big) x^{\delta^m g_1} c_{m11}.$$

This contradicts the assumption that $\sum_j k_{mj} > 1$ is minimal possible. So $\sum_j k_{mj} = 1$. By reindexing g_j, we may hence assume $k_{m1} = 1$ and $k_{mj} = 0$ for $j \neq 1$. That is, $c_{m11} \neq 0$ but $c_{mjk} = 0$ for $(j,k) \neq (1,1)$.

Extend $c_1 \overset{\text{def.}}{=} c_{m11}$ into a C–basis $c_1, c_2, \ldots$ of the C–linear span of c_{ijk}. Collecting terms of $\varphi(x)$ according to the right coefficients c_ν, we rewrite

$$\varphi(x) = \sum_\nu \big(\sum_k \sum_{j=0}^{m} b_{jk}^{(\nu)} x^{\delta^{m-j} g_k}\big) c_\nu,$$

where $b_{jk}^{(\nu)}, c_\nu \in R_{\mathcal{F}}$. We may also assume that all

$$\phi_{\nu,k}(x) \overset{\text{def.}}{=} \sum_{j=0}^{m} b_{j,k}^{(\nu)} x^{\delta^{m-j} g_k} = b_{0,k}^{(\nu)} x^{\delta^m g_k} + b_{1,k}^{(\nu)} x^{\delta^{m-1} g_k} + \cdots + b_{m,k}^{(\nu)} x^{g_k}$$

are nontrivial. Note that only $\phi_{1,1}(x)$ involves δ^m. Let us concentrate on $\phi_{1,1}(x)$ and write $\phi(x)$ for $\phi_{1,1}(x)$, b_j for its coefficients $b_{j,1}^{(1)}$ and g for g_1. So $\phi(x) = \phi_{1,1}(x) =$

$\sum_{j=0}^{m} b_j x^{\delta^{m-j}g}$. We compute

$$\begin{aligned}
\phi(xy) &= \sum_{j=0}^{m}\sum_{k=0}^{m-j} b_j x^{D_{k,m-j-k}g} y^{\delta^{m-j-k}g} \\
&= \sum_{j=0}^{m}\sum_{i=j}^{m} b_j x^{D_{i-j,m-i}g} y^{\delta^{m-i}g} \qquad \text{(by setting } i \stackrel{\text{def.}}{=} j+k\text{)} \\
&= \sum_{i=0}^{m}\sum_{j=0}^{i} b_j x^{D_{i-j,m-i}g} y^{\delta^{m-i}g} \qquad \text{(by switching summations)} \\
&= b_0 x^{\sigma^m g} y^{\delta^m g} + \sum_{i=1}^{m-1}\Big(\sum_{j=0}^{i} b_j x^{D_{i-j,m-i}g}\Big) y^{\delta^{m-i}g} + \Big(\sum_{j=0}^{m} b_j x^{D_{m-j,0}g}\Big) y^{g},
\end{aligned}$$

where the last equality follows by singling out terms with $i = 0$ and $i = m$. By the continuity of δ and σ, we pick a two–sided ideal $I \neq 0$ of R such that $Ib_i \subseteq R$ for $i = 0, \ldots, m-1$ and such that $I^{D_{s,t}g_k} \subseteq R$ for $0 \leq s, t \leq m$ and all g_k involoved. We *claim* that the map

$$f_i\colon \sum_s v_s b_0 u_s^{\sigma^m g} \mapsto \sum_s v_s \sum_{j=0}^{i} b_j u_s^{D_{i-j,m-i}g},$$

where $u_s, v_s \in I$, is well–defined for $1 \leq i \leq m-1$: Let $u_s, v_s \in I$ satisfy $\sum_s v_s b_0 u_s^{\sigma^m g} = 0$. We must show that $\sum_s v_s \sum_{j=0}^{i} b_j u_s^{D_{i-j,m-i}g} = 0$ for $i = 1, \ldots, m-1$. We compute

$$\begin{aligned}
\sum_s v_s \phi(u_s y) =& \Big(\sum_s v_s b_0 u_s^{\sigma^m g}\Big) y^{\delta^m g} + \sum_{i=1}^{m-1}\Big(\sum_{j=0}^{i}\sum_s v_s b_j u_s^{D_{i-j,m-i}g}\Big) y^{\delta^{m-i}g} \\
&+ \sum_s v_s \Big(\sum_{j=0}^{m} b_j u_s^{D_{m-j,0}g}\Big) y^{g} \\
=& \sum_{i=1}^{m-1}\Big(\sum_{j=0}^{i}\sum_s v_s b_j u_s^{D_{i-j,m-i}g}\Big) y^{\delta^{m-i}g} + \sum_s v_s \Big(\sum_{j=0}^{m} b_j u_s^{D_{m-j,0}g}\Big) y^{g}.
\end{aligned}$$

Let us go back to examine the originally given $\varphi(x)$: In $\varphi(x)$, only $\phi(x) \stackrel{\text{def.}}{=} \phi_{1,1}(x)$ involves δ^m and in $\phi(x)$, only the term $b_0 x^{\delta^m g}$ involves δ^m. Since $\sum_s v_s b_0 u_s^{\sigma^m g} = 0$, $\sum_s v_s \varphi(u_s y)$ involves only δ^i, $i < m$ and must have δ–order 0 by the minimality of m. That is, in $\sum_s v_s \varphi(u_s y)$, the sum of terms with δ^i, $i \geq 1$, must be trivial. The expression $\sum_s v_s \varphi(u_s y)$ still has the right coefficients $c_1, c_2, \ldots$. Particularly, the right coefficient of $y^{\delta^{m-i}g_1} c_1$, where $g = g_1$, must vanish:

$$\sum_{j=0}^{i}\sum_s v_s b_j u_s^{D_{i-j,m-i}\, g} = 0$$

for $1 \leq i \leq m-1$. The additive map f_i is thus well–defined as claimed.

Each f_i is clearly a left R–module map from the left ideal $Ib_0I^{\sigma^m g}$ into R. Since both σ^{-1} and g^{-1} are continuous, $Ib_0I^{\sigma^m g}$ contains a nonzero ideal of R. Thus there exist $t_i \in R_{\mathcal{F}}$ such that $f_i(x) = xt_i$ for all $x \in Ib_0I^{\sigma^m g}$. That is, $vb_0u^{\sigma^m g}t_i = v\sum_{j=0}^{i} b_j u^{D_{i-j,m-i}\, g}$ for all $u, v \in I$. This implies that for $1 \leq i \leq m-1$, the equality

$$b_0 x^{\sigma^m g} t_i = \sum_{j=0}^{i} b_j x^{D_{i-j,m-i}\, g}$$

holds for all $x \in I$. Set $\tilde{b}_j \overset{\text{def.}}{=} b_j^{g^{-1}}$ and $\tilde{t}_i \overset{\text{def.}}{=} t_i^{g^{-1}}$. Then, for $1 \leq i \leq m-1$, the equality

$$\tilde{b}_0 x^{\sigma^m} \tilde{t}_i = \sum_{j=0}^{i} \tilde{b}_j x^{D_{i-j,m-i}}$$

holds for all $x \in I$. For $i = 1$, we have

$$\tilde{b}_0 x^{\sigma^m} \tilde{t}_1 = \tilde{b}_0 x^{D_{1,m-1}} + \tilde{b}_1 x^{\sigma^{m-1}}$$

for all $x \in I$. Notice that $D_{1,m-1}$ is a (σ^m, σ^{m-1})–derivation of Q. In view of Lemma 3, we have that $\tilde{t}_1 \in Q$, $\tilde{b}_1 = \tilde{b}_0\tilde{t}_1$ and $x^{D_{1,m-1}} = x^{\sigma^m}\tilde{t}_1 - \tilde{t}_1 x^{\sigma^{m-1}}$ for all $x \in Q$. That is,

$$D_{1,m-1} = \sigma^m r(\tilde{t}_1) - \sigma^{m-1}\ell(\tilde{t}_1).$$

We proceed by induction on $n \leq m-1$ to show that $\tilde{t}_n \in Q$, $\tilde{b}_n = \tilde{b}_0\tilde{t}_n$ and that $\psi_n \overset{\text{def.}}{=} D_{n,m-n} + \sum_{j=1}^{n-1} D_{n-j,m-n}\ell(\tilde{t}_j)$ is equal to $\sigma^m r(\tilde{t}_n) - \sigma^{m-n}\ell(\tilde{t}_n)$: As the induction hypothesis, suppose that for $1 \leq k \leq n-1$ we have $\tilde{b}_k = \tilde{b}_0\tilde{t}_k$ and

$$\psi_k \overset{\text{def.}}{=} D_{k,m-k} + \sum_{j=1}^{k-1} D_{k-j,m-k}\ell(\tilde{t}_j) = \sigma^m r(\tilde{t}_k) - \sigma^{m-k}\ell(\tilde{t}_k).$$

From the defining equality for $\tilde{t}_n$, we see that

$$\tilde{b}_0 x^{\sigma^m}\tilde{t}_n - \tilde{b}_n x^{\sigma^{m-n}} = \tilde{b}_0 x^{\psi_n}.$$

By Lemma 1, ψ_n is a continuous (σ^m, σ^{m-n})–derivation. Applying Lemma 3, we see that $\tilde{b}_n = \tilde{b}_0\tilde{t}_n$ and $\psi_n = \sigma^m r(\tilde{t}_n) - \sigma^{m-n}\ell(\tilde{t}_n)$, as asserted. The induction is completed. With all these and by Lemma 1 again, $\psi \overset{\text{def.}}{=} \psi_m$ gives rise to a K–identity of δ and defines a continuous σ^m–derivation, which we denote by μ:

$$x^{\mu} = x^{\psi_m} = x^{\delta^m} + \sum_{j=1}^{m-1} t_j x^{\delta^{m-j}}$$

for $x \in Q$. Recall that S is outer independent. If $S \cup \{\mu\}$ is not outer independent, then μ is defined by $\Lambda(S)$ by Proposition 9 [10] and so is the K–polynomial $\psi(x)$. We thus assume that $S \cup \{\mu\}$ is outer independent. Substitute

$$x^{\delta^m} = -\sum_{j=1}^{m-1} t_j x^{\delta^{m-j}} + x^{\mu}$$

for x^{δ^m} in $\varphi(x)$ and write the expression thus resulted as $\varphi'(x) + \rho'(x)$, where $\varphi'(x)$ is the sum of terms involving δ_i, $1 \leq i < m$ and where $\rho'(x) \stackrel{\text{def.}}{=} \varphi(x) - \varphi'(x)$ is the sum of terms involving μ. If $\varphi'(x)$ is trivial, the $\rho'(x)$, a linear GP involving μ only, is defined by $\Lambda(S)$, contradicting the outer independence of $S \cup \{\mu\}$ by Proposition 9 [10]. So the δ–order m' of $\varphi'(x)$ is ≥ 1. But obviously $m' < m$. Since $\rho'(x) \in \Lambda(S \cup \{\mu\})$, $\varphi'(x)$ is defined by $\Lambda(S \cup \{\mu\})$. Apply the previous argument to $\varphi'(x)$ defined by $\Lambda(S \cup \{\mu\})$ and obtain a K–polynomial ψ' of δ–order $m' < m$. Continue in this manner. We finally stop at, say, the $(n+1)$–st step and obtain a finite sequence of skew derivations $\mu, \mu', \ldots, \mu^{(n)}$, defined respectively by K–polynomials $\psi, \psi', \ldots, \psi^{(n)}$ of strictly decreasing δ–orders $m > m' > \cdots > m^{(n)} \geq 1$, such that each $\mu^{(i)}$ is a $\sigma^{m^{(i)}}$–derivation and such that $S \cup \{\mu, \ldots, \mu^{(n-1)}\}$ is outer independent but $S \cup \{\mu, \ldots, \mu^{(n-1)}, \mu^{(n)}\}$ is not. So there is an identity of R in the form

$$x^{\mu^{(n)}} + \sum_{j=0}^{n-1} u_j x^{\mu^{(j)}} + \sum_k v_k x^{\partial_k} = 0,$$

where $u_j \in \Phi_{\sigma^{m^{(j)}-m^{(n)}}}$, $\partial_k \in S \cap \mathcal{L}_{g_k}(R)$ and $v_k \in \Phi_{\sigma^{-m^{(n)}} g_k}$. By Lemma 2,

$$\psi^{(n)}(x) + \sum_{j=0}^{n-1} u_j \psi^{(j)}(x)$$

is also a K–polynomial and is defined by $-\sum_k v_k x^{\partial_k}$ in $\Lambda(S)$, as asserted.

We need two more lemmas, both due to Kharchenko. They are extremely useful in analyzing skew derivations:

Lemma 5. (Kharchenko) *Let δ be a continuous X–outer σ–derivation of R. Then for $\alpha \in C$, we have $\alpha^\sigma = \alpha$ and α^δ, if it is nonzero, is a unit of Q such that $x^\sigma = \alpha^\delta x (\alpha^\delta)^{-1}$ for $x \in Q$.*

Proof. Let $\alpha \in C$. We compute

$$\alpha^\delta x + \alpha^\sigma x^\delta = (\alpha x)^\delta = (x\alpha)^\delta = x^\delta \alpha + x^\sigma \alpha^\delta.$$

It follows that $(\alpha - \alpha^\sigma) x^\delta = \alpha^\delta x - x^\sigma \alpha^\delta$. If $\alpha \neq \alpha^\sigma$, then δ would be inner. So we have $\alpha^\sigma = \alpha$. If $\alpha^\delta \neq 0$, then the identity $\alpha^\delta x = x^\sigma \alpha^\delta$ implies that α^δ is a unit of Q and that $x^\sigma = \alpha^\delta x (\alpha^\delta)^{-1}$ for all $x \in Q$.

Lemma 6. (Kharchenko) *If R satisfies GPIs, then any continuous skew derivation δ of R is either X–inner or of the form $\delta: x \mapsto ux^d$, where $u \in Q$ is a unit and d is a continuous ordinary X–outer derivation.*

Proof. Let δ be a continuous σ–derivation. We may assume that δ is X–outer. By Lemma 5, $\alpha^\sigma = \alpha$ for $\alpha \in C$. By a result in p.140 [6], σ is X–inner. Say, $x^\sigma = uxu^{-1}$ for $x \in Q$. We check easily that the map $d: x \mapsto u^{-1}x^\delta$ is an ordinary derivation of Q. So $x^\delta = ux^d$ for $x \in Q$. The continuity of d follows from the continuity of δ.

Proof of Theorem 1: Let ϕ denote $\varphi(x_i^{\delta^j g_k})$ or $\varphi(x_i^{\delta^j g_k})_{j<m}$ according as the first case or the second case of Theorem 1 holds.

Case 1. ϕ is linear: In this case, we may write $\phi \stackrel{\text{def.}}{=} \varphi(x^{\delta^j g_k})$ or $\phi \stackrel{\text{def.}}{=} \varphi(x^{\delta^j g_k})_{j<m}$. Assume toward a contradiction that ϕ is nontrivial and has δ–order n. Apply Lemma 4 with $S \stackrel{\text{def.}}{=} \emptyset$: There is a K–polynomial ψ of δ–order $\leq n$ defined by Λ. By Lemma 1, K–polynomials always define skew derivations and, by Proposition 9 [10], skew derivations defined by Λ must be X–inner. So ψ defines an X–inner skew derivation. Particularly, δ is left $R_{\mathcal{F}}$–algebraic modulo inner skew derivations and, in this case, $\phi \stackrel{\text{def.}}{=} \varphi(x^{\delta^j g_k})_{j<m}$, where m is the minimum δ–order of left $R_{\mathcal{F}}$–algebraicity of δ modulo inner skew derivations. By the minimality of m, $m \leq$ the δ–order of $\psi \leq n$, a contradiction. So ψ is trivial. The expression resulted from ψ by substituting z_{jk} for $x^{\delta^j g_k}$ is also trivial and is certainly a GPI.

Case 2. ϕ is multilinear: Assign arbitrarily fixed values to all x_i except x_1. The resulted expression is linear in x_1. By Case 1, the expression ϕ' obtained from ϕ by substituting z_{1jk} for $x_1^{\delta_j g_k}$ is a GPI. The values assigned to x_i, $i \neq 1$, are arbitrary. So ϕ', now considered as a GP in the indeterminates z_{1jk} and x_i, $i > 2$, is also an identity of R. Now, assign arbitrarily fixed values to all indeterminates of ϕ' except x_2 and proceed in the same way. We conclude that the expression ϕ'' obtained from ϕ' by substituting z_{2jk} for $x_2^{\delta_j g_k}$ is a GPI. But ϕ'' is also the expression obtained from ϕ by substituting z_{1jk}, z_{2jk} for $x_1^{\delta_j g_k}$, $x_2^{\delta_j g_k}$ respectively. Continue in this manner. We finally replace all $x_i^{\delta_j g_k}$ by z_{ijk} and obtain the desired GPI in z_{ijk}.

Case 3. General: We may assume that ϕ is nontrivial, for otherwise there is nothing to prove. The multilinear μ obtained by linearizing ϕ is then also nontrivial. Apply Case 2 to μ. We conclude that R is a GPI–ring. By Lemma 6, δ is of the form $x^\delta = ux^d$, where u is a unit in Q and d is an ordinary X–outer derivation. We have already seen in Example 1 that δ is left $R_{\mathcal{F}}$–algebraic modulo inner skew derivations if and only if d is C–algebraic modulo inner derivations. Their algebraic dependence relations also have the same order. As demonstrated in Example 1,

$$x^{\delta^n} = u^n x^{d^n} + \text{terms of the form } ax^{d^i}, \text{ where } a \in Q \text{ and } 1 \leq i < n.$$

It thus suffices to prove the case when δ is an ordinary derivation. We now refer to Kharchenko's Theorem cited at the beginning and thus finish the proof.

Proof of Theorem 2: Since all K–identities are universally valid on the whole $R_{\mathcal{F}}$, we may assume, without loss of generality, that $\varphi(x_i^{\delta^j g_k})$ is reduced in the following sense: (1) g_k are mutually outer and (2) $\varphi(x_i^{\delta^j g_k})$ involves only δ^j, $j < m$ if δ is left

$R_{\mathcal{F}}$–algebraic of the minimum δ–order m modulo inner skew derivations. We may also assume that $\varphi(x_i^{\delta^j g_k})$ is nontrivial, for otherwise, there is nothing to prove. If R is a GPI–ring, then, by Lemma 6, δ is either X–inner or of the form $\delta\colon x \mapsto ux^d$, where $u \in Q$ is a unit and d is an ordinary derivation. In this case, $\varphi(x_i^{\delta^j g_k})$ reduces to a GP with automorphisms and ordinary derivations. The result follows from Theorem 1 [4]. It thus suffices to show that R is a GPI–ring.

For this purpose, we assume that $\varphi(x_i^{\delta^j g_k})$ vanishes on a nonzero ideal I of R. Firstly, the symmetric (or respectively left) Martindale quotient ring of I coincides with that of R. Secondly, the ideal topology of Q defined by ideals of R is the same as that defined by ideals of I. So $\mathcal{A}(I) = \mathcal{A}(R)$ and $\mathcal{L}(I) = \mathcal{L}(R)$. Applying Corollary 1 to the nontrivial identity $\varphi(x_i^{\delta^j g_k})$ of I yields that I is a GPI–ring and so is R, as asserted.

Replacing $\varphi(x_i^{\delta^j g_k})$ by $\varphi(x_i^{g_k \delta^j})$ in Theorems 1 and 2, we notice that the conclusions still hold by applying an analogous argument. For convenience of the applications in forthcoming papers, we explicitly give the statements:

Theorem 3. *Let R be a prime ring and δ, an X–outer continuous σ–derivation of R. If δ is not left $R_{\mathcal{F}}$–algebraic modulo inner skew derivations, then any GPI of the form $\varphi(x_i^{g_k \delta^j})$, where $g_k \in \mathcal{A}(R)$ are mutually outer, yields the GPI $\varphi(z_{ijk})$, where z_{ijk} are distinct indeterminates. If δ is left $R_{\mathcal{F}}$–algebraic modulo inner skew derivations, then (i) such algebraic dependence of minimal δ–order assumes the form*

$$\psi(x) = x^{\sigma^m} b - bx,$$

where $b \in Q$ and $\psi(x)$ is a K–polynomial of δ–order $m \geq 1$ and (ii) any GPI of the form $\varphi(x_i^{g_k \delta^j})_{j<m}$, where $g_j \in \mathcal{A}(R)$ are mutually outer, yields the GPI $\varphi(z_{ijk})_{j<m}$, where z_{ijk} are distinct indeterminates.

Theorem 4. *Given $\delta \in \mathcal{L}_\sigma(R)$, if a GP of the form $\varphi(x_i^{g_k \delta^j})$, where $g_k \in \mathcal{A}(R)$, vanishes on a nonzero two–sided ideal of R, then it also vanishes on $R_{\mathcal{F}}$.*

References

[1] T. A. Andreeva, I. V. L'vov, and V. K. Kharchenko, *The rings of quotients of free algebras*, Algebra i Logika, **35**(6) (1996), 366–3370. (Engl. Transl., Algebra and Logic **35**(6) (1996), 655–662.)

[2] K.I. Beidar, W.S. Martindale 3rd and A.V. Mikhalev, "Rings with Generalized Identities", Monographs and Textbooks in Pure and Applied Mathematics, **196**. Marcel Dekker, Inc., New York, 1996.

[3] C.-L. Chuang, *Differential identities with automorphisms and antiautomorphisms, I*, J. Algebra **149** (1992), 371–404.

[4] C.-L. Chuang, *Differential identities with automorphisms and antiautomorphisms, II*, J. Algebra **160** (1993), 292–335.

[5] C.-L. Chuang, *Identities with skew derivations*, J. Algebra **224**(2) (2000), 292–335.

[6] V. K. Kharchenko, *Generalized identities with automorphisms*, Algebra i Logika, **14**(2) (1975), 215–237. (Engl. Transl., Algebra and Logic **14**(2) (1975), 132–148.)

[7] V. K. Kharchenko, *Differential identities of prime rings*, Algebra i Logika **17** (1978), 220–238. (Engl. Transl., Algebra and Logic **17** (1978), 154–168.)

[8] V. K. Kharchenko, *Differential identities of semiprime rings*, Algebra i Logika **18** (1979), 86–119. (Engl. Transl., Algebra and Logic **18** (1979), 58–80.)

[9] V. K. Kharchenko, "Automorphisms and Derivations of Associative Rings" 1991 Kluver academic publisher p.385.

[10] V. K. Kharchenko and A. Z. Popov, *Skew derivations of prime rings*, Comm. Algebra **20**(11), (1992), 3321–3345.

[11] A. N. Koryukin, *Primitive algebraic relations of skew derivations of prime rings*, Algebra i Logika **36**(4), (1997), 407–421. (Engl. Transl., Algebra and Logic **36**(4) (1997), 236–244.)

[12] A. Leroy, *S–derivations algebriques sur les anneaux premiers.* (French) [Algebraic S–derivations over prime rings] Ring theory (Antwerp, 1985), 114–120, Lecture Notes in Math., **1197**, Springer, Berlin, 1986.

[13] A. Leroy and J. Matczuk, *The extended centroid and X–inner automorphisms of Ore extensions*, J. Algebra **145** (1992), 143–177.

[14] W. S. Martindale 3rd, *Prime rings satisfying a generalized polynomial identity*, J. Algebra **12** (1969), 576–584.

[15] M. E. Sweedler, "Hopf Algebras", 1969 Benjamin, Inc., New York.