行政院國家科學委員會補助專題研究計畫成果報告

質環上的泛導算等式
Identities of Generalized Derivations in Prime Rings

計畫類別：☑ 個別型計畫　　□整合型計畫
計畫編號： NSC 89-2115-M-002-013
執行期間： 88 年 8 月 1 日至 89 年 7 月 31 日

計畫主持人：李秋坤教授
共同主持人：

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計劃國外研究報告書一份

執行單位：國立台灣大學理學院數學系

中 華 民 國 89 年 12 月 18 日

摘 要

若 R 為一質環。一個加法映射 $g:R\to R$ 如果滿足 $(xy)^g = x^g y + x y^\delta \ \forall x,y\in R$, 其中 δ 是 R 上的一個導算，則稱 g 為質環 R 上的一個泛導算。本篇論文主要目的在證明質環上泛導算恆等式的 Kharchenko 理論，經由這個觀點所建立的理論，我們可以解決許多有關泛導式的問題。

由本人執行之８９年度之貴會研究計劃" 質環上之泛導算等式" (NSC 89-2115-M-002-013), 項下之出席國際會議經費10萬元, 因故並未使用, 計劃經費已繳回學校結算.

台大數學系教授

李秋坤 90 年 2 月5 日

關鍵詞：質環、泛導算、泛導算等式

IDENTITIES OF GENERALIZED DERIVATIONS IN PRIME RINGS

Tsiu–Kwen Lee

Department of Mathematics, National Taiwan University

Taipei 106, Taiwan

E–mail: tklee@math.ntu.edu.tw

Abstract. Let R be a prime ring with extended centroid C. By a generalized derivation of R we mean an additive map $g: R \to R$ such that $(xy)^g = x^g y + xy^\delta$ for all $x \in R$, where δ is a derivation of R. In this paper we prove a version of Kharchenko's theorem for generalized derivations and show some results concerning identities of generalized derivations.

1991 *Mathematics Subject Classification.* 16W25, 16R50, 16N60.

Key words and phrases. Prime ring, generalized derivation, reduced identity.

§1. Introduction

Throughout this paper R always denotes a prime ring with extended centroid C, Q its two–sided Martindale quotient ring and U its right Utumi quotient ring. In [6] Hvala gave an algebraic study of generalized derivations of prime rings. An additive map $g: R \to R$ is called a generalized derivation of R if there exists a derivation δ of R such that $(xy)^g = x^g y + xy^\delta$ for all $x, y \in R$. In [13] the author extended the definition as follows. By a generalized derivation we mean an additive map $g: \rho \to U$ such that $(xy)^g = x^g y + xy^\delta$ for all $x, y \in \rho$, where ρ is a dense right ideal of R and δ is a derivation from ρ into U. The author proved that every generalized derivation can be uniquely extended to a generalized derivation of U. In fact, there exist $a \in U$ and a derivation δ of U such that $x^g = ax + x^\delta$ for all $x \in U$ [13, Theorem 3]. Therefore, a generalized derivation g can be assumed $g: U \to U$ in this paper. For identities of derivations, Kharchenko established the structure theorems of differential identities (see [8] and [9]) which are powerful tools for reducing a differential identity to a generalized polynomial identity. Thus, to study identities of generalized derivations, it seems reasonable to find a corresponding theorem for identities of generalized derivations. Roughly speaking, we will prove that if $f(X_i^{\Gamma_j})$ is an identity for R, where the $\Gamma_j's$ are distinct regular words in generalized derivations, then $f(Z_{ij})$ is a generalized polynomial identity (GPI) for U. In section 3, as applications to the structure theorem, we will prove some results concerning identities of generalized derivations. In particular, we generalize [6, Theorem 1] and [6, Theorem 2] to prime rings without the characteristic assumption. In section 4, we will prove an analogous theorem for prime rings with involution.

§2. Reduced Identities

Let $g: U \to U$ be a generalized derivation. We write $x^g = ax + x^\delta$ for all $x \in U$, where $a \in U$ and δ is a derivation of U. Since a and δ are uniquely determined by the generalized derivation g, we say δ to be the associated derivation of g. A generalized derivation of U is said to be *generalized inner* if its associated derivation is U–inner. Thus a generalized inner derivation g must be of the form $x^g = ax + xb$ for some $a, b \in U$. We shall prove the version of Kharchenko's theorem [9] for generalized derivations. To state the theorem we want to prove, we have to fix some notation. We denote by $\mathrm{Gder}(U)$ the set of all generalized derivations of U. Let $g, h \in \mathrm{Gder}(U)$. If $\beta \in C$, define $x^{g\beta} = x^g\beta$. It follows that $\mathrm{Gder}(U)$ forms a right C–space. Set G_{int} to be the C–subspace of $\mathrm{Gder}(U)$ consisting of all generalized inner derivations of U. Then the following statement holds:

Let $g, h \in \mathrm{Gder}(U)$ and let δ and d be the associated derivations of g and h, respectively. Then $[g, h] \in \mathrm{Gder}(U)$ with associated derivation $[\delta, d]$ and $g^p \in \mathrm{Gder}(U)$ with associated derivation δ^p if $\mathrm{char}\, R = p > 0$.

The first part is easily checked. We prove the second part. Let $x, y \in U$. Then $(xy)^g = x^g y + xy^\delta$. Since $\mathrm{char}\, R = p > 0$, we see that $(xy)^{g^p} = \sum_{i=0}^{p} \binom{p}{i} x^{g^{p-i}} y^{\delta^i} = x^{g^p} y + xy^{\delta^p}$. In particular, if we set $x = 1$, then $y^{g^p} =$

$1^{g^p}y + y^{\delta^p}$ for all $y \in U$. Therefore, g^p is still a generalized derivation of U with associated derivation δ^p.

By a generalized derivation word we mean an additive map Γ from U into itself assuming the form $\Gamma = g_1 g_2 \dots g_t$, where $g_i \in \mathrm{Gder}(U)$. If Γ is empty, we define $x^\Gamma = x$ for $x \in U$. A generalized differential polynomial means a generalized polynomial with coefficients in U and with noncommuting variables which are acted upon by generalized derivation words. Thus every generalized differential polynomial can be written in the form $\phi(X_i^{\Gamma_j})$, where $\phi(Z_{ij})$ is a generalized polynomial over U in distinct variables Z_{ij}, and the Γ_j's are generalized derivation words. A generalized differential polynomial $\phi(X_i^{\Gamma_j})$ is called a *generalized differential identity* (GDI) for a subset T of U if $\phi(X_i^{\Gamma_j})$ assumes 0 for any assignment of values from T to its variables X_i. Recall the following basic identities:

(B1) $(XY)^g = X^g Y + XY^\delta$ for $g \in \mathrm{Gder}(U)$ with associated derivation δ.

(B2) $X^\delta = X^g - aX$ for $g \in \mathrm{Gder}(U)$ if $x^g = ax + x^\delta$ for all $x \in U$, where δ is the associated derivation of g.

(B3) $(X+Y)^g = X^g + Y^g$ for $g \in \mathrm{Gder}(U)$.

(B4) $X^g = aX + Xb$ if g is the generalized inner derivation defined by $x^g = ax + xb$ for all $x \in U$.

(B5) $X^{[g,h]} = (X^g)^h - (X^h)^g$ for $g, h \in \mathrm{Gder}(U)$.

(B6) $X^{g^p} = (\dots((X^g)^g)\dots)^g$ (p–times) for $g \in \mathrm{Gder}(U)$ and $\mathrm{char}\, R =$

$p > 0$.

(B7) $X^{g\alpha+h\beta} = X^g\alpha + X^h\beta$ for $g, h \in \mathrm{Gder}(U)$ and $\alpha, \beta \in C$.

Choose a fixed basis G_0 for G_{int} and augment it to a basis G for $\mathrm{Gder}(U)$ over C. Fix a total order $>$ in the set G such that $g_0 > g$ for $g_0 \in G_0$ and $g \in G \setminus G_0$, and then extend this order to the set of all generalized derivation words by assuming that a longer word is greater than a shorter one and that words of the same length are ordered lexicographically. By a *regular word* we mean a generalized derivation word of the form $\Gamma = g_1^{s_1} g_2^{s_2} \dots g_m^{s_m}$ possessing the following properties:

(W1) $g_i \in G \setminus G_0$ for $1 \le i \le m$,

(W2) $g_1 < g_2 < \cdots < g_m$ and

(W3) $s_i < p$ for $1 \le i \le m$, if $\mathrm{char}\, R = p > 0$.

Applying the same viewpoint of Kharchenko's papers ([8] and [9]) for differential identities, each generalized differential identity can be transformed, via the basic identities (B1)–(B7), into a form $\phi(X_i^{\Gamma_j})$ such that

(R1) $\phi(Z_{ij})$ is a generalized polynomial over U in noncommuting variables Z_{ij} and

(R2) the Γ_j's are distinct regular words.

A generalized differential polynomial is called *reduced* if it assumes the form $\phi(X_i^{\Gamma_j})$ satisfying (R1) and (R2). Now we are ready to state our main theorem.

Theorem 1. *Let R be a prime ring. If $\phi(X_i^{\Gamma_j})$ is a reduced* GDI *for a nonzero ideal of R, then $\phi(Z_{ij})$ is a* GPI *for U.*

We shall derive Theorem 1 from Kharchenko's theorem (see [8] and [9]). The key viewpoint of our proof is implicit in [12]. For convenience we give the statement of Kharchenko's theorem here. We remark that Kharchenko's theorem holds for nonzero ideals.

Kharchenko's Theorem. *Let R be a prime ring. If $\phi(\Delta_i(X_j))$ is a differential identity for a nonzero ideal of R, where Δ_i are distinct regular words and X_j are distinct indeterminates, then $\phi(Z_{ij})$ is a* GPI *for R.*

Denote by $\mathrm{Der}(U)$ the set of all derivations of U. Then $\mathrm{Der}(U)$ is a C–submodule of $\mathrm{Gder}(U)$. Consider the set $M_{out} = \{\delta \mid \delta$ is an associated derivation of some $g \in G \setminus G_0\}$. Then M_{out} is C–independent modulo U–inner derivations. A canonical linear order can be defined as follows: For $g, h \in G \setminus G_0$ with associated derivations δ, d respectively, we have $g < h$ if and only if $\delta < d$. Let M_0 be a basis of the U–inner derivations over C. It is clear that the union of M_{out} and M_0 forms a basis of $\mathrm{Der}(U)$ over C. For $\Gamma = g_1 g_2 \ldots g_n$, a regular word in generalized derivations g_i with associated derivations δ_i, we set $\widetilde{\Gamma} = \delta_1\delta_2\ldots\delta_n$, which is called the associated word of Γ. It is clear that $\widetilde{\Gamma}$ is a regular word in derivations δ_i. For a regular word $\Gamma = g_1 g_2 \ldots g_n$, by a subword of Γ we mean a generalized word of the form $\emptyset$, the empty word, or $g_{i_1} g_{i_2} \ldots g_{i_s}$ with $1 \le i_1 < i_2 \cdots < i_s \le n$. It is clear that a subword of a regular word is still regular. For two subwords $E = g_{i_1} g_{i_2} \ldots g_{i_s}$ and $F = g_{j_1} g_{j_2} \ldots g_{j_t}$ of Γ, $(E, \widetilde{F})$ is called a pair of subwords of

Γ if $s+t=n$ and these i_k and j_ℓ are distinct. We are now ready to give the

Proof of Theorem 1. Suppose that $\phi(X_i^{\Gamma_j})$ is a reduced GDI for I with distinct regular words Γ_j, where I is a nonzero ideal of R. In view of [10, Theorem 2], I and U satisfy the same differential identities (DIs) with coefficients in U. Thus they also satisfy the same GDIs with coefficients in U. Hence, we may assume that $I=U$. We proceed the proof by induction on the largest regular word involved in $\phi(X_i^{\Gamma_j})$, say Γ_1. Assigning $X_2, X_3, \cdots$ to fixed elements in U, we may assume that ϕ only involves one variable with coefficients in U. Write $\phi=\phi(X^{\Gamma_j})$, where the $\Gamma_1,\ldots,\Gamma_t$ are all distinct regular words occurring in ϕ and $\Gamma_1>\cdots>\Gamma_t$.

Suppose that Γ_1 is empty. Then ϕ is a GPI for U and there is nothing to prove. Therefore we suppose that Γ_1 is not empty. Let $x,y\in U$. Then

$$(1)\qquad (xy)^{\Gamma_j}=\sum_{k=1}^{\ell_j} x^{E_{jk}}y^{\widetilde{F_{jk}}},$$

where the $(E_{jk},\widetilde{F_{jk}})$'s run over all pairs of subwords of Γ_j. Moreover, let $E_{j1}=\Gamma_j$ and so $\widetilde{F_{j1}}$ is empty for each j. Let $x_1,\ldots,x_t,y_1,\ldots,y_t\in U$. By assumption we have $\phi\Big(\sum_{i=1}^t (x_iy_i)^{\Gamma_j}\Big)=0$. In view of (1), we have

$$(2)\qquad \phi\Big(\sum_{i=1}^{t}\sum_{k=1}^{\ell_j} x_i^{E_{jk}}y_i^{\widetilde{F_{jk}}}\Big)=0.$$

Applying Kharchenko's theorem to (2) by setting $y_i^{\widetilde{F_{jk}}}=0$ for $\widetilde{F_{jk}}\neq\widetilde{\Gamma}_i$, we reduce (2) to

$$\phi\Big(W_j(x_i^{E_{jk}},y_i^{\widetilde{F_{jk}}})\Big)=0,$$

where, for $1 \le j \le t$,

$$W_j(X_i^{E_{jk}}, y_i^{\widetilde{F_{jk}}}) = X_j y_j^{\widetilde{\Gamma}_j} + \sum_{i=j+1}^{t} \sum_{k \in \Lambda_{ij}} X_i^{E_{jk}} y_i^{\widetilde{F_{jk}}}$$

with $\Lambda_{ij} = \{k \mid \widetilde{F_{jk}} = \widetilde{\Gamma}_i, 1 \le k \le \ell_j\}$. Fix $y_i \in U$ and set $\psi = \phi\Big(W_j(X_i^{E_{jk}}, y_i^{\widetilde{F_{jk}}})\Big)$.

We remark that E_{jk} is not empty and $E_{jk} < \Gamma_1$ if E_{jk} occurs in ψ and, moreover, ψ is a GDI for U. Applying the inductive hypothesis, we may replace X_i with x_i and $X_i^{E_{jk}}$ with 0 for E_{jk} nonempty to obtain that $\phi(x_j y_j^{\widetilde{\Gamma}_j}) = 0$ for all $x_j, y_j \in U$. In view of Kharchenko's theorem [9] again, we see that $\phi(x_j y_j) = 0$ for all $x_j, y_j \in U$. In particular, setting $y_j = 1$ for each j we see that $\phi(Z_j)$ is a GPI for U. This proves the theorem.

The following result generalizes [8, Corollary 2] to the case of algebraic generalized derivations.

Corollary. *Let R be a prime ring with extended centroid C and right Utumi quotient ring U, g a generalized derivation of U and $\phi(X)$ a monic polynomial over C of degree $n > 1$. Suppose that $\phi(g)$ is a generalized derivation of U and that either* $\operatorname{char} R = 0$ *or $p > n$. Then both g and $\phi(g)$ are generalized inner.*

Proof. Write $\phi(X) = X^n + X^{n-1}\beta_{n-1} + \cdots + X\beta_1 + \beta_0 \in C[X]$. Suppose, on the contrary, that g is not a generalized inner derivation. By assumption, we write

$$x^{g^n} + x^{g^{n-1}}\beta_{n-1} + \cdots + x^g\beta_1 + x\beta_0 = x^{\phi(g)} \tag{3}$$

for all $x \in U$. If g and $\phi(g)$ are C–independent modulo G_{int}, then $g, g^2, \ldots, g^n$ and $\phi(g)$ are distinct regular words as either char $R = 0$ or $p > n$. Applying Theorem 1 to (3) we see that $x_n + x_{n-1}\beta_{n-1} + \cdots + x_1\beta_1 + x_0\beta_0 = y$ for all $y, x_i \in U$, a contradiction. This proves that $\phi(g) = g\beta + \mu$ for some $\beta \in C$ and μ a generalized inner derivation. Thus $x^{\mu} = ax + xb$, where $a, b \in U$ and hence

$$x^{g^n} + x^{g^{n-1}}\beta_{n-1} + \cdots + x^g\beta_1 + x\beta_0 = x^g\beta + ax + xb$$

for all $x \in U$. Since g is not generalized inner, we can derive a contradiction from the argument given as above. Thus g is generalized inner. Now it is clear that the associated derivation of $\phi(g)$ is defined by a generalized linear map. By Kharchenko's theorem, the associated derivation of $\phi(g)$ is inner and so $\phi(g)$ is a generalized inner derivation, as desired.

§3. Certain Identities of Generalized Derivations

Let R be a prime ring of characteristic not 2. In [15] Posner proved that if d_1 and d_2 are derivations of R such that its product d_1d_2 is also a derivation, then one of d_1 and d_2 is zero. In [6] Hvala extended Posner's theorem by characterizing generalized derivations f_1 and f_2 of R when its product f_1f_2 is also a generalized derivation of R [6, Theorem 1]. On the other hand, Hvala also proved that generalized derivations g_1 and g_2 are C–dependent if $[x^{g_1}, x^{g_2}] = 0$ for all $x \in R$. Applying Theorem 1, we will give a complete description of Hvala's theorems without the assumption that char $R \neq 2$. For $a \in U$, we denote by a_ℓ and a_r the left and right multiplications by a, respectively. Let $\mathcal{L}(U)$ ($\mathcal{R}(U)$) be the set of all left (right resp.) multiplications of U. We will prove the following two theorems.

Theorem 2. *Let R be a prime ring with extended centroid C and let g_1 and g_2 be generalized derivations of R. Then the product g_1g_2 is also a generalized derivation if and only if one of the following holds:*

(i) there exists $\lambda \in C$ such that either $g_1 = \lambda_\ell$ or $g_2 = \lambda_\ell$;

(ii) either $g_1, g_2 \in \mathcal{L}(U)$ or $g_1, g_2 \in \mathcal{R}(U)$;

(iii) there exist $\lambda, \mu \in C$ and $a, b \in U$ such that $x^{g_1} = ax + xb$ and $x^{g_2} = \lambda x + \mu(ax - xb)$ for all $x \in U$;

(iv) $\operatorname{char} R = 2$ *and there exist $\lambda, \mu \in C$ such that $g_2 = \lambda_\ell + g_1\mu$.*

Theorem 3. *Let R be a noncommutative prime ring with extended centroid C and let g_1 and g_2 be nonzero generalized derivations of R. Suppose that $[x^{g_1}, x^{g_2}] = 0$ for all $x \in R$. Then there exists $\lambda \in C$ such that $x^{g_2} = \lambda x^{g_1}$ for all $x \in R$.*

To prove the two theorems we first state a preliminary result, which is an immediate consequence of [14, Theorem 2 (a)] and [3, Theorem 2]. Therefore we only give its statement without proof.

Lemma 1. *Let R be a prime ring. Suppose that $\sum_{i=1}^{m} a_i x b_i + \sum_{j=1}^{n} c_j x d_j = 0$ for all $x \in R$, where $a_i, b_i, c_j, d_j \in U$, $1 \le i \le m, 1 \le j \le n$. If $a_1, \ldots, a_m$ are C-independent, then each b_i is C-dependent on $d_1, \ldots, d_n$. Similarly, if $b_1, \ldots, b_m$ are C-independent, then each a_i is C-dependent on $c_1, \ldots, c_n$.*

We first deal with two special cases of Theorem 2.

Lemma 2. *Let R be a prime ring with extended centroid C, $a, b \in U$ and g a generalized derivation of U. Suppose that the map $x^h = ax^g + x^g b$ ($x^h = (ax + xb)^g$) is also a generalized derivation of U. Then either $a, b \in C$, or $b \in C$ and $g \in \mathcal{L}(U)$, or $a \in C$ and $g \in \mathcal{R}(U)$, or there exist $\lambda, \mu \in C$ such that $x^g = \mu x + \lambda(ax - xb)$ for all $x \in U$.*

Proof. Suppose that the map $x^h = (ax + xb)^g$ is a generalized derivation of U. Write $x^g = ux + x^\delta$ for some $u \in U$ and δ a derivation of U. Then $x^h = (ax + xb)^g = a^g x + ax^\delta + x^g b + xb^\delta = a^g x + a(x^g - ux) + x^g b + xb^\delta = (ax^g + x^g b) + \big((a^g - au)x + xb^\delta\big)$. This implies that the map $x \mapsto (ax + xb)^g$ is a generalized derivation if and only if so is the map $x \mapsto ax^g + x^g b$. Hence it suffices to prove the case that $x^h = ax^g + x^g b$ for $x \in U$.

Suppose first that g is not a generalized inner derivation. If g and h are C-independent modulo G_{int}, then $ax + xb = y$ for all $x, y \in U$ by Theorem 1. This is a contradiction. Thus $x^h = x^g\beta + cx + xd$ for some $\beta \in C$ and $c, d \in U$. Thus $ax^g + x^g b = x^g\beta + cx + xd$ for all $x \in U$. Applying Theorem 1 yields that $ay + yb = y\beta + cx + xd$ for all $x, y \in U$. Then $cx + xd = 0$ for all $x \in U$ and $a, b \in C$, as desired.

Suppose next that g is a generalized inner derivation. Then there exist $c, d \in U$ such that $x^g = cx + xd$ for all $x \in U$. Thus $x^h = a(cx + xd) + (cx + xd)b$ for $x \in U$. This implies that the associated derivation of h is a generalized linear map. In view of Kharchenko's theorem, the associated derivation of h is inner and so h itself is generalized inner. Write $x^h = ux + xv$ for all $x \in U$, where $u, v \in U$. Then we see that

$$(4) \qquad (u - ac)x - axd - cxb + x(v - db) = 0$$

for all $x \in U$. If $a, c, 1$ are C–independent, then, by Lemma 1, we have $d, b, v - db \in C$. Hence, $b \in C$ and $g = (c + d)_\ell \in \mathcal{L}(U)$, as desired.

Suppose next that a, c and 1 are C–dependent. If $c \in C$, then $g = (c + d)_r \in \mathcal{R}(U)$ and hence we are done for the case that $a \in C$. Suppose that $a \notin C$. Since $c \in C$, (4) is reduced to $(u - ac)x - axd + x(v - db - cb) = 0$ for all $x \in U$, implying, by Lemma 1, that $d \in C$. Set $\mu = c + d \in C$. Then $x^g = \mu x$ for all $x \in U$, as desired.

Hence we assume that $c \notin C$. If $a \in C$, then (4) is reduced to $(u - ac)x - cxb + x(v - db - ad) = 0$ for all $x \in U$, implying, by Lemma 1, that $b \in C$. We are done in this case. So we assume that $a \notin C$. Then $c = \lambda a + \nu$, where $\lambda, \nu \in C$ and $\lambda \neq 0$. Now we reduce (4) to $(u - ac)x - ax(d + \lambda b) + x(v - db - \nu b) = 0$ for all $x \in U$. Since $1, a$ are C–independent, applying Lemma 1 yields that $d + \lambda b = \gamma \in C$. Thus, for $x \in U$, $x^g = cx + xd = (\nu + \gamma)x + \lambda(ax - xb)$. Set $\mu = \nu + \gamma \in C$. This proves the lemma.

Proof of Theorem 2. Let $h = g_1 g_2$. Suppose that one of g_1 and g_2 is generalized inner. Then we are done by Lemma 2. Thus we suppose that neither g_1 nor g_2 is generalized inner. If g_1 and g_2 are C–independent modulo G_{int}, applying Theorem 1 yields that $y = x^h$ for all $x, y \in U$, a contradiction. Thus $x^{g_2} = x^{g_1}\mu + ax + xb$ for some $0 \neq \mu \in C$ and $a, b \in U$. Thus we have

$x^h = x^{{g_1}^2}\mu + ax^{g_1} + x^{g_1}b$ for $x \in U$. If $\operatorname{char} R \neq 2$, then ${g_1}^2$ is a regular word of length two. Applying Theorem 1 yields that $x^h = y\mu + ax^{g_1} + x^{g_1}b$ for $x, y \in U$. Since $\mu \neq 0$, this is a contradiction. So we have $\operatorname{char} R = 2$. Then ${g_1}^2$ is still a generalized derivation. Hence the map $x \mapsto ax^{g_1} + x^{g_1}b$ defines a generalized derivation of U. Since g_1 is not generalized inner, by Lemma 2 the only possibility is that $a, b \in C$. Set $\lambda = a + b \in C$. So we have $g_2 = g_1\mu + \lambda_\ell$. This proves the theorem.

We next turn to the proof of Theorem 3. Let R be a prime GPI–ring with extended centroid C. By Martindale's theorem [14], RC is a strongly primitive ring. For simplicity, we will fix some notations in this case. We denote by F the algebraic closure of C if C is infinite and set $F = C$ if C is finite. Set $\widetilde{R} = RC \otimes_C F$. Then $\widetilde{R}$ is a centrally closed prime F–algebra [5, Theorem 3.5] with nonzero socle, denoted by H, and possesses nontrivial idempotents if R is not commutative. Moreover, applying [3, Theorem 2] together with a standard argument proves that R and $\widetilde{R}$ satisfy the same GPIs with coefficients in $RC + C$. In addition, $1 \in H$ if and only if $\widetilde{R} \cong \mathrm{M}_n(F)$ for some $n \geq 1$.

We begin with some special cases. The first is a special case of [11, Lemma 2].

Lemma 3. *Let R be a prime ring and $a, c \in R$. Suppose that $[ax, cx] = 0$ for all $x \in R$. Then a and c are linearly dependent over C.*

Lemma 4. *Let R be a noncommutative prime ring and $a, b \in R$. Suppose* *that* $ax + xb \in Z(R)$. *Then* $a = -b \in Z(R)$.

Proof. Let $x, y \in R$. Then $x[b, y] = (ax + xb)y - (a(xy) + (xy)b) \in Z(R)y + Z(R)$, implying that $[y, x[b, y]] = 0$. That is, $[y, R[b, y]] = 0$ for all $y \in R$. This implies that $b \in Z(R)$. So $(a + b)R \subseteq Z(R)$ and so $a + b = 0$, since R is not commutative. This proves the lemma.

Lemma 5. *Let* R *be a prime ring,* $a, c, d \in R$ *and* $a \neq 0$. *Suppose that* $[ax, cx + xd] = 0$ *for all* $x \in R$. *Then* $d \in C$ *and there exists* $\lambda \in C$ *such that* $c + d = \lambda a$.

Proof. If R is commutative, then the conclusion trivially holds. We assume that R is not commutative. If $c \notin Ca + C$, then $[aX, cX + Xd]$ is a nontrivial GPI for R. Suppose that $c = \lambda a + \beta$, where $\alpha, \beta \in C$. By assumption, we have $[ax, x(d + \beta)] = 0$ for all $x \in R$. If $a \in C$, then we are done by Lemma 3. Thus we assume that $a \notin C$. If $d + \beta = 0$, then we see that $c + d = \lambda a$, as desired. So we also assume that $d + \beta \neq 0$. It is clear that $[aX, X(d + \beta)]$ is a nontrivial GPI for R. In other others, we may assume that R is a GPI–ring. As noted, we have $H \neq 0$ and

$$[ax, cx + xd] = 0 \tag{5}$$

for all $x \in \widetilde{R}$.

Let e be an idempotent in H. Replacing x by xe in (5) and expanding $[axe, cxe + xed](1 - e) = 0$, we see that $axexed(1 - e) = 0$ for all $x \in \widetilde{R}$. Thus, by [15, Lemma 2], we have $ed(1 - e) = 0$. Analogously, $(1 - e)de = 0$. In particular, we have $[d, e] = 0$. Denote by E the additive subgroup of H

generated by all idempotents in H. Then $[H,H] \subseteq E$ [7, Corollary p.19] and hence, $[d,[H,H]]=0$. By [3, Theorem 2], we have $[d,[\widetilde{R},\widetilde{R}]]=0$, implying that $d \in C$. It follows from (5) that $[ax,(c+d)x]=0$ for all $x \in \widetilde{R}$. In view of Lemma 3, there exists $\lambda \in C$ such that $c+d=\lambda a$, proving the lemma.

Lemma 6. *Let R be a prime ring, $f\colon R \to RC$ a generalized linear map, defined by $x \mapsto \sum_{i=1}^{n} b_i x c_i$ where $\{b_1,\cdots,b_n\}$ and $\{c_1,\cdots,c_n\}$ are C-independent subsets of RC. Suppose that $f(x)xa=0$ ($axf(x)=0$) for all $x \in R$, where $0 \neq a \in R$. Then $aRCa=Ca$ and $c_iRCc_i=Cc_i$ (resp. $b_iRCb_i=Cb_i$) for each i.*

Proof. We only give the proof of the case that $f(x)xa=0$ for all $x \in R$. The another case can be proved by an analogous argument. Linearizing the GPI $(\sum_{i=1}^{n} b_i X c_i)Xa$ for R, we see that

$$\sum_{i=1}^{n} b_i x c_i y a + \sum_{i=1}^{n} b_i y c_i x a = 0 \tag{6}$$

for all $x,y \in RC$. Replacing x by xaz in (6) we get

$$\sum_{i=1}^{n} b_i(xaz)c_i y a + \sum_{i=1}^{n} b_i y c_i (xaz) a = 0.$$

On the other hand,

$$\Big(\sum_{i=1}^{n} b_i x c_i y a + \sum_{i=1}^{n} b_i y c_i x a\Big) z a = 0.$$

Comparing the last two relations we arrive at

$$\sum_{i=1}^{n} b_i x [az, c_i y] a = 0$$

for all $x, y, z \in RC$. Since $\{b_1, \cdots, b_n\}$ is C–independent, by Lemma 1 we see that $[aRC, c_iRC]a = 0$ for each i. In particular, $[aRC, c_iRCaRC]a = 0$, implying that $c_iRC[aRC, aRC]a = 0$. The primeness of RC implies that $[aRC, aRC]a = 0$ and so $[aRC, aRC]aRC = 0$. An analogous argument proves that $[c_iRC, c_iRC]c_iRC = 0$ for each i. Thus we get that $aRCa = Ca$ and $c_iRCc_i = Cc_i$ for each i (see, for instance, the proof of [2, Lemma 5.1]).

Lemma 7. *Let $R = \mathrm{M}_n(F)$, the $n \times n$ matrix ring over a field F, and $e = e^2 \in R$ with rank 1, where $n > 1$. Suppose that $ax(cx + exd) = 0$ for all $x \in R$, where $a, c, d \in R$ and $a \neq 0$. Then $d \in F$.*

Proof. Since e is of rank 1, we may assume, without loss of generality, that $e = e_{11}$. Let $x \in R$. By assumption, we have $0 = axe_{11}(cxe_{11} + e_{11}xe_{11}d)(1 - e_{11}) = axe_{11}xe_{11}d(1 - e_{11})$, implying that $e_{11}d(1 - e_{11}) = 0$ [15, Lemma 2]. That is, $e_{11}d = e_{11}de_{11}$. Thus there exists $\beta \in F$ such that the first row of $d - \beta$ is zero. Thus we can choose a nonzero element $w \in R$ such that $(d - \beta)w = 0$. By assumption, we see that

$$0 = ax((c + \beta e_{11})x + e_{11}x(d - \beta))w = ax(c + \beta e_{11})xw,$$

implying that $c + \beta e_{11} = 0$ [15, Lemma 2]. Thus we have $axe_{11}x(d - \beta) = 0$ for all $x \in R$. By [15, Lemma 2] again, $d = \beta \in F$ follows, a contradiction.

We are now in a position to give the proof of Theorem 3.

Proof of Theorem 3. By assumption, $[x^{g_1}, x^{g_2}] = 0$ for all $x \in R$. If g_1 and g_2 are C–independent modulo generalized inner derivations, by Theorem 1 we see that $[x_1, x_2] = 0$ for all $x_1, x_2 \in R$. So R is commutative, a contradiction. Suppose that one of g_1 and g_2 is outer, say g_1. Then there exist $\lambda \in C$ and $a, b \in U$ such that $x^{g_2} = \lambda x^{g_1} + ax + xb$ for all $x \in R$. By assumption, $[x^{g_1}, \lambda x^{g_1} + ax + xb] = 0$ for all $x \in R$ and hence for all $x \in U$ [10, Theorem 2]. By Theorem 1, we have $[y, \lambda y + ax + xb] = 0$ for all $x, y \in U$. So $ax + xb \in C$ for all $x \in U$ and, by Lemma 4, $a = -b \in C$. Thus $x^{g_2} = \lambda x^{g_1}$ for all $x \in R$, as desired.

From now on, we assume that both g_1 and g_2 are generalized inner. Write $x^{g_1} = ax + xb$ and $x^{g_2} = cx + xd$ for $x \in R$, where $a, b, c, d \in U$. Since R and U satisfy the same GPIs [3, Theorem 2], we may assume that $R = U$. In particular, R is a centrally closed prime C–algebra. By Lemma 5, we may assume that $a, b, c, d \notin C$. By assumption, we see that

$$[ax + xb, cx + xd] = 0 \tag{7}$$

for all $x \in R$. To prove $g_2 = g_1\lambda$ for some $\lambda \in C$, it is equivalent to claim that $d - \beta = \lambda b$ and $c + \beta = \lambda a$ for some $\beta \in C$. Suppose not. Then $[aX + Xb, cY + Yd] + [aY + Yb, cX + Xd]$ is a nontrivial GPI for R. As noted, (7) holds for all $x \in \widetilde{R}$. We claim that $d = \lambda b + \beta$ for some $\lambda, \beta \in F$. We divide the argument into two cases.

Suppose first that $1 \notin H$. In this case, we see that $\dim_F \widetilde{R} = \infty$. Denote by E the additive subgroup of R generated by all idempotents in H of rank 2. Note that if e is an idempotent in H of rank 2, then so are both $e + ex(1-e)$ and $e + (1-e)xe$ for each $x \in H$. In particular, $[E, H] \subseteq E$ and so E is a noncentral Lie ideal of H. Thus, by Herstein's theorem [7], we have $[H, H] \subseteq E$. Since $a \notin C$, then $[a, E] \neq 0$. Thus we can choose

$e = e^2 \in \widetilde{R}$ with rank 2 such that either $(1-e)ae \neq 0$ or $ea(1-e) \neq 0$. Note that $(1-e)\widetilde{R}(1-e) \neq F(1-e)$ and $e\widetilde{R}e \neq Fe$. We may assume that $(1-e)ae \neq 0$. We remark that an analogous argument can be applied to the case that $ea(1-e) \neq 0$. Substituing $ex(1-e)$ for x in (7), we see that

$$(8) \qquad [aex(1-e) + ex(1-e)b, cex(1-e) + ex(1-e)d] = 0.$$

Multiplying (8) by $1-e$ from the left obtains

$$\big((1-e)aex(1-e)ce - (1-e)cex(1-e)ae\big)x(1-e) = 0$$

for all $x \in \widetilde{R}$. Since $(1-e)\widetilde{R}(1-e) \neq F(1-e)$, Lemma 6 implies that $(1-e)aex(1-e)ce-(1-e)cex(1-e)ae = 0$ for all $x \in \widetilde{R}$. By Lemma 1, there exists $\lambda \in F$ such that $(1-e)ce = \lambda(1-e)ae$. Substituting ex for x in (7) and then multiplying by $1-e$ from the left, we see that $(1-e)aex(cex+exd) = (1-e)cex(aex+exb)$. Thus

$$(9) \qquad (1-e)aex\big((c-\lambda a)ex + ex(d-\lambda b)\big) = 0$$

for all $x \in \widetilde{R}$. Since $e\widetilde{R}e \neq Fe$, Lemma 6 implies that either $(c-\lambda)e \in Fe$ or $d - \lambda b \in F$. If $(c-\lambda)e = -\beta e$, where $\beta \in F$, then, by (9), we have $(1-e)aexex(d-\lambda b-\beta) = 0$ for all $x \in \widetilde{R}$. Thus we have $d-\lambda b-\beta = 0$ [15, Lemma 2]. Thus, in either case, there exists $\beta \in F$ such that $d-\lambda b-\beta = 0$.

Suppose next that $1 \in H$. Suppose on the contrary that $d \notin Fb+F$. In this case, we see that $\widetilde{R} \cong \mathrm{M}_n(F)$,where $n \geq 2$. Write $a = \sum_{i,j=1}^n \beta_{ij}e_{ij}$ and $c = \sum_{i,j=1}^n \mu_{ij}e_{ij}$, where $\beta_{ij}, \mu_{ij} \in F$. Suppose that $\beta_{ij} \neq 0$ for some $i \neq j$.

Replacing x by $e_{jj}x$ in (7) and expanding $e_{ii}[ae_{jj}x+e_{jj}xb, ce_{jj}x+e_{jj}xd]=0$, we see that

$$(10) \qquad \beta_{ij}e_{ij}x\Big((c-\lambda a)e_{jj}x+e_{jj}x(d-\lambda b)\Big)=0,$$

where $\lambda=\mu_{ij}\beta_{ij}^{-1}\in F$. Applying Lemma 7 to (10), we have $d-\lambda b\in F$, a contradiction. Thus a is a diagonal matrix. For an invertible matrix $u\in\widetilde{R}$, by (7) we have

$$(11) \qquad [uau^{-1}x+xubu^{-1}, ucu^{-1}x+xudu^{-1}]=0$$

for all $x\in\widetilde{R}$. The above argument says that uau^{-1} is a diagonal matrix. In particular, for $i>1$ we compute $(1+e_{1i})a(1-e_{1i})=a+(\beta_{ii}-\beta_{11})e_{1i}$, implying that $\beta_{ii}=\beta_{11}$. This means $a\in F$, a contradiction. So $d\in Fb+F$.

Up to now we have proved the claim $d-\lambda b=\beta\in F$. Replacing c,d by $c+\beta, d-\beta$ respectively, we may assume that $d=\lambda b$. The rest is to prove that $c=\lambda a$. Suppose that $c\neq\lambda a$. Let $f=f^2\in H$. Substituting xf for x in (7) and then multiplying by $1-f$ from the right, we see that $(\lambda a-c)xfxfb(1-f)=0$ for all $x\in\widetilde{R}$, where we also use $d=\lambda b$. Thus, by [15, Lemma 2], $fb(1-f)=0$. Analogously, $(1-f)bf=0$ and so $[b,f]=0$ follows. As before, this implies that $b\in F$, a contradiction. This proves $c=\lambda a$. This proves the theorem.

§4. Rings with Involution

Throughout this section, let R be a prime ring with involution $*$, right Utumi quotient ring U and two–sided Martindale quotient ring Q. It is well–

known that the involution $*$ can be uniquely extended to an involution on Q. We denote this involution by $*$ also. Denote by $\mathrm{Der}(U)$ the set of all derivations of U. Thus $\mathrm{Der}(U) \subseteq \mathrm{Gder}(U)$. Let $\mathbf{D}$ be the C–submodule of $\mathrm{Der}(U)$ defined by

$$\mathbf{D} = \{\delta \in \mathrm{Der}(U) \mid I^{\delta} \subseteq R \text{ for some nonzero ideal } I, \text{ depending on } \delta, \text{ of } R\}.$$

We denote by $\mathbf{GD}$ be the C–submodule of $\mathrm{Gder}(U)$ consisting of all elements g of the form $x^g = ax + x^{\delta}$ for some $a \in Q$ and $\delta \in \mathbf{D}$. Let $g \in \mathbf{GD}$. Then $Q^g \subseteq Q$, and so one can define a generalized derivation, say g^*, on Q. For $x \in Q$, let $x^{g^*} = ((x^*)^g)^*$. Write $x^g = ax + x^{\delta}$ for some $a \in Q$ and $\delta \in \mathbf{D}$. Then a direct computation proves that $x^{g^*} = a^*x + x^{\delta^* - \mathrm{ad}(a^*)}$. Thus $g^* \in \mathbf{GD}$ and $(g^*)^* = g$. Moreover, if $g_1, \cdots, g_n \in \mathbf{GD}$, then $(x^{g_1 g_2 \cdots g_n})^* = (x^*)^{g_1^* g_2^* \cdots g_n^*}$ for all $x \in Q$.

A $*$–generalized differential polynomial ($*$–GDP) means a generalized polynomial with coefficients in U and with noncommuting variables which are acted by the involution $*$ as well as generalized derivation words (in $\mathbf{GD}$). Recall the following basic $*$–identities as given in [4]:

(B8) $(XY)^* = Y^*X^*$.

(B9) $(X + Y)^* = X^* + Y^*$.

(B10) $(X^g)^* = (X^*)^{(g^*)}$ for $g \in \mathbf{GD}$.

(B11) $(X^{g_1 g_2 \cdots g_n})^* = (X^*)^{g_1^* g_2^* \cdots g_n^*}$ for $g_1, \cdots, g_n \in \mathbf{GD}$.

Applying the basic identities (B1)–(B11), every $*$–GDP can be transformed into the form $\phi(X_i^{\Gamma_j}, (X_i^{\Gamma_j})^*)$, where $\phi(Z_{ij}, Z_{ij}^*)$ is a $*$–generalized polynomial over U in distinct variables Z_{ij} and the Γ_j's are generalized derivation words (in **GD**). A $*$–GDP $\phi(X_i^{\Gamma_j}, (X_i^{\Gamma_j})^*)$ is called a $*$–generalized differential identity ($*$–GDI) for a subset T of Q if $\phi(X_i^{\Gamma_j}, (X_i^{\Gamma_j})^*)$ assumes 0 for any assignment of values from T to its variables X_i. Each $*$–GDI can be transformed, via the basic identities (B1)–(B11), into a form $\phi(X_i^{\Gamma_j}, (X_i^{\Gamma_j})^*)$ such that

($*$–R1) $\phi(Z_{ij}, Z_{ij}^*)$ is a $*$–generalized polynomial over U in noncommuting variables Z_{ij} and

($*$–R2) the Γ_j's are distinct regular words.

Now a $*$–GDP is called *reduced* if it assumes the form $\phi(X_i^{\Gamma_j}, (X_i^{\Gamma_j})^*)$ satisfying ($*$–R1) and ($*$–R2). The following powerful result was due to Chuang [4]. We remark that the theorem actually holds for $*$–DIs with coefficients in U.

Chuang's Theorem. *Let R be a prime ring with involution $*$. If $\phi(X_i^{\Delta_j}, (X_i^{\Delta_j})^*)$ is a reduced $*$-DI for a nonzero ideal of R, then $\phi(Z_{ij}, Z_{ij}^*)$ is a $*$-GPI for R.*

We are now ready to state our result.

Theorem 4. *Let R be a prime ring with involution $*$, right Utumi quotient ring U and two-sided Martindale quotient ring Q. If $\phi(X_i^{\Gamma_j}, (X_i^{\Gamma_j})^*)$ is a reduced $*$-GDI for a nonzero ideal of R, then $\phi(Z_{ij}, {Z_{ij}}^*)$ is a $*$-GPI for Q.*

Proof. For its proof, we only give its outline. We apply the same argument as given in the proof of Theorem 1 by replacing [10, Theorem 2] with Chuang's theorem. Hence, we obtain that $\phi(Z_{ij}, Z_{ij}^*)$ is a $*$-GPI for R. In view of [1, Theorem 1.4.1], R and Q satisfy the same $*$-GPIs with coefficients in U. Hence, $\phi(Z_{ij}, Z_{ij}^*)$ is a $*$-GPI for Q. This proves the theorem.

REFERENCES

1. K. I. Beidar, A. V. Mihhalev and C. Salavova, *Generalized identities and semiprime rings with involution*, Math. Z. **178** (1981), 37-62.

2. M. Brešar, *On generalized biderivations and related maps*, J. Algebra **172** (1995), 764–786.

3. C. L. Chuang, GPI*s having coefficients in Utumi quotient rings*, Proc. Amer. Math. Soc. **103** (1988), 723–728.

4. C. L. Chuang, *$*$-Differential identities of prime rings with involution*, Tran. Amer. Math. Soc. **316** (1989), 251–279.

5. T. S. Erickson, W. S. Martindale 3rd, and J. Osborn, *Prime nonassociative algebras*, Pacific J. Math. **60** (1975), 49–63.

6. B. Hvala, *Generalized derivations in rings*, Comm. Algebra **26**(4) (1998), 1147–1166.

7. I. N. Herstein, "Topics in Ring Theory", University of Chicago Press, Chicago, 1969.

8. V. K. Kharchenko, *Differential identities of prime rings*, Algebra i