*Publ. Math. Debrecen*
**61 / 1-2** (2002), 75–85

# Derivations and co-radical extensions of rings

By TSIU-KWEN LEE (Taipei) and CHING-YUEH PAN (Taipei)

**Abstract.** A ring $R$ is said to be *co-radical* over a subring $A$ if for each $x \in R$ there exists a polynomial $g_x(t)$ (depending on $x$) having integral coefficients so that $x - x^2 g_x(x) \in A$. Herstein proved that a ring which is co-radical over its center must be commutative. In this paper we give a generalization of Herstein's theorem for the prime case in terms of derivations with assumptions on one-sided ideals.

## §1. Introduction and main results

Throughout this paper all rings are associative, not necessarily with unity. We denote by $\mathbb{Z}[t]$ the polynomial ring with indeterminate $t$ over $\mathbb{Z}$, the ring of integers. A ring $R$ is called *co-radical* over a subring $A$ if for each $x \in R$ there exists a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $x - x^2 g_x(x) \in A$. In [8] Herstein proved that a ring which is co-radical over its center must be commutative. In [4] Chacron gave a generalization of Herstein's theorem for the semiprime case by the use of the *cohypercenter* $T(R)$ of a ring $R$. An element $a \in R$ belongs to $T(R)$ if for each $x \in R$ there exists a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $[a, x - x^2 g_x(x)] = 0$. Chacron proved that if $R$ is a semiprime ring, then $T(R)$ coincides with the center of $R$. In terms of derivations he just proved that if $d$ is an inner derivation of the semiprime ring $R$ satisfying $d(x - x^2 g_x(x)) = 0$ for all $x \in R$, then $d = 0$. For the general case of derivations, in a recent paper [3] Bell proved the theorem: Let $R$ be a prime ring with $\operatorname{char} R \neq 2$, and let $d$ be a derivation of $R$ such that $d^3 \neq 0$. If there exists a fixed integer $n > 1$ such that $d(x - x^n) \in \mathcal{Z}(R)$, the center of $R$, for all $x \in R$, then $R$ is commutative. The goal of this paper is to extend these results by proving the following theorems.

*Mathematics Subject Classification*: 16W25, 16N60, 16R50, 16U80.
*Key words and phrases*: derivation, co-radical, GPI, prime ring, differential identity.

**Theorem 1.** *Let $R$ be a noncommutative prime ring and $a, b \in R$. Suppose that for each $x \in R$, there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $a(x - x^2 g_x(x))b = 0$. Then either $a = 0$ or $b = 0$.*

**Theorem 2.** *Let $R$ be a noncommutative prime ring, $\rho$ a right ideal of $R$ and $a, b \in R$. Suppose that for each $x \in \rho$, there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $a\big(x - x^2 g_x(x)\big)b = 0$. Then $a\rho b = 0$ unless $\rho = eR$, where $e = e^2 \in R$, such that $eRe$ is a field.*

**Theorem 3.** *Let $R$ be a prime ring, $\rho$ a nonzero right ideal of $R$ and $d$ a nonzero derivation of $R$. Suppose that for each $x \in \rho$, there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $d(x - x^2 g_x(x)) = 0$. Then $R$ is commutative except when $\rho = eR$, where $e = e^2 \in R$, such that $eRe$ is a field, and $d = \mathrm{ad}(b)$ and $b\rho = 0$ for some $b \in Q$, the symmetric Martindale quotient ring of $R$.*

As an immediate consequence of Theorem 3 we have the following

**Theorem 4.** *Let $R$ be a prime ring and let $d$ be a nonzero derivation of $R$. Suppose that for each $x \in R$, there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $d(x - x^2 g_x(x)) = 0$. Then $R$ is commutative.*

Finally we will extend Theorem 4 to the central case. However, we cannot conclude the commutativity of the prime ring $R$. The following provides counterexamples.

*Examples.* Let $R = \mathrm{M}_2(C)$, the 2 by 2 matrix ring over a field $C$, $b \in [R, R] \setminus C$ and $d$ the inner derivation of $R$ defined by the element $b$. If $C$ is algebraic over $\mathrm{GF}(2)$, the Galois field of two elements, then for each $x \in R$, there is a positive integer $q = q(x) > 1$ (depending on $x$) so that $d(x - x^q) \in C$.

PROOF. We denote by $F$ the algebraic closure of $C$ and let $S = \mathrm{M}_2(F)$. Then $R \subseteq S$. Let $x, y \in [R, R]$. A direct computation proves that $xy + yx = (x + y)^2 - x^2 - y^2 \in C$. Since $\operatorname{char} R = 2$, we have $[x, y] \in C$. That is, $\big[[R, R], [R, R]\big] \subseteq C$. In particular, $[b, [R, R]] \subseteq C$. Let $x \in R$. Then there exists an invertible matrix $u \in S$ such that $uxu^{-1}$ is an upper triangular matrix in $S$. Since $F$ is algebraic over $\mathrm{GF}(2)$, there exists a positive integer $q = q(x) > 1$ such that $uxu^{-1} - ux^q u^{-1}$ is a strictly upper triangular matrix in $S$. In particular, the trace of $x - x^q \in R$ is zero. Therefore, $x - x^q \in [R, R]$ and so $[b, x - x^q] \in \big[b, [R, R]\big] \subseteq C$, as desired. This proves our result. $\square$

In fact, the examples above are the only exceptional cases. Indeed, we will prove the following

**Theorem 5.** *Let $R$ be a prime ring with center $\mathcal{Z}(R)$ and $d$ a nonzero derivation of $R$. Suppose that for each $x \in R$, there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $d(x - x^2 g_x(x)) \in \mathcal{Z}(R)$. Then $R$ is commutative except when $RC \cong \mathrm{M}_2(C)$ with $C$ algebraic over $\mathrm{GF}(2)$, where $C$ denotes the extended centroid of $R$.*

## §2. Proofs of theorems

From now on, $R$ will denote a prime ring with extended centroid $C$ and symmetric Martindale quotient ring $Q$. We denote by $\mathcal{Z}(R)$ the center of $R$ and by $J(R)$ the Jacobson radical of $R$. For $p \in Q$ we denote by $\mathrm{ad}(p)$ the inner derivation of $Q$ induced by the element $p$, that is, $\mathrm{ad}(p)(x) = [p, x] = px - xp$ for $x \in Q$. A derivation $d$ of $R$ is called $X$-inner if $d = \mathrm{ad}(p)$ for some $p \in Q$. Otherwise, $d$ is called $X$-outer. It is well-known that each derivation of $R$ can be uniquely extended to a derivation of $Q$. We first state a result due to Chacron [5].

**Lemma 1.** *Let $R$ be a prime ring and $a, b \in R$. Suppose that for each $x \in R$, there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $a(x - x^2 g_x(x))b = 0$. If $ab = 0$, then either $a = 0$ or $b = 0$.*

Proof. See the proof of [5, Lemma 3]. □

**Lemma 2.** *Let $R$ be a noncommutative prime ring and $a \in R$. Suppose that for each $x \in R$, there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $a(x - x^2 g_x(x)) = 0$. Then $a = 0$.*

Proof. Suppose first that $J(R) \neq 0$. Then, by assumption, for each $x \in J(R)$ there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $a(x - x^2 g_x(x)) = 0$. Thus $ax(1 - xg_x(x)) = 0$. From the fact that $xg_x(x) \in J(R)$ it follows that $ax = 0$. That is, $aJ(R) = 0$ and so $a = 0$ by the primeness of $R$.

Suppose next that $J(R) = 0$. We first consider the case that $R$ is a right primitive ring. By the density theorem, $R$ acts densely on ${}_DV$, where ${}_DV$ is a left vector space over a division ring $D$. Suppose that there is a $v \in V$ such that $va$ and $v$ are $D$-independent. Then we can choose an $x \in R$ such that $vax = v$ and $vx = 0$. Then $vax^2 = 0$ and so $0 = va(x - x^2 g_x(x)) = vax = v$, which is absurd. Therefore, for each $v \in V$ we see that $va$ and $v$ are $D$-dependent. Now, a standard argument proves that $a$ is central in $R$. We turn next to the general case. Let $P$ be a right primitive ideal of $R$. Then $R/P$ is a right primitive ring preserving our assumptions. Thus $\overline{a} = a + P$ is central in $R/P$ and so $[a, R] \subseteq P$. Since $J(R) = 0$, the intersection of all right primitive ideals of $R$ is zero. Therefore we have $[a, R] = 0$, implying that $a \in \mathcal{Z}(R)$. If $a \neq 0$, then for each $x \in R$, there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $x - x^2 g_x(x) = 0$. In view of Herstein's theorem [8], $R$ is commutative, a contradiction. This proves the lemma. $\square$

Proof of Theorem 1. Clearly, we may assume that $a = b$. Denote by $\rho$ the right ideal of $R$ generated by $a$, that is, $\rho = aR + \mathbb{Z}a$. Set $\overline{\rho} = \rho/\rho \cap \ell_R(\rho)$, where $\ell_R(\rho)$ is the left annihilator of $\rho$ in $R$. It is clear that $\overline{\rho}$ is still a prime ring. By assumption, for each $\overline{x} \in \overline{\rho}$, there is a polynomial $g_{\overline{x}}(t) \in \mathbb{Z}[t]$ (depending on $\overline{x}$) so that $\overline{a}(\overline{x} - \overline{x}^2 g_{\overline{x}}(\overline{x})) = 0$. In view of Lemma 2, either $\overline{a} = 0$ or $[\overline{\rho}, \overline{\rho}] = 0$. The first case gives $a^2 = 0$, implying that $a = 0$ by Lemma 1. The latter case implies that $[\rho, \rho]\rho = 0$ and hence $R$ is a prime GPI-ring. In view of Martindale's theorem [14], $RC$ is a strongly primitive ring, where $C$ is the extended centroid of $R$. If $RC$ is a division ring, then there is nothing to prove. Suppose that $RC$ is not a division ring. Denote by $H$ the socle of $RC$. Then $H$ is a simple ring with minimal one-sided ideals and possesses nontrivial idempotents. Let $e$ be an idempotent in $H$. Choose a nonzero ideal $I$ of $R$ so that $eI + Ie + eIe \subseteq R$. For $x \in I$ we have $ex(1 - e) \in R$. Since $ex(1 - e)$ is an element of square zero, by assumption we have $aex(1 - e)a = 0$. Thus $(1 - e)ae = 0$ follows. Analogously, $ea(1 - e) = 0$ and hence $[a, e] = 0$. Denote by $E$ the additive subgroup of $H$ generated by all idempotents in $H$. In view of [9, Corollary p. 18], $[H, H] \subseteq E$. Thus $[a, [H, H]] = 0$. By [9, Corollary p. 9], the subring generated by $[H, H]$ is equal to $H$ and so $[a, H] = 0$. Thus $a$ is central in $R$. If $a \neq 0$, then for each $x \in R$, there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $x - x^2 g_x(x) = 0$. In view of Herstein's theorem [8], $R$ is a commutative ring, a contradiction. This proves the theorem. $\square$

The following lemma is due to Babkov [1, Lemma 7].

**Lemma 3.** *Let $R$ be a noncommutative prime ring, $\rho$ a nonzero right ideal of $R$ and $a \in R$. Suppose that for each $x \in \rho$, there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $(x - x^2 g_x(x))a = 0$. Then $a = 0$*

*unless $R$ is a primitive ring with nonzero socle and its associated division ring is a field.*

For simplicity, we say that a ring $R$ has the property $(*)$ if it is a primitive ring with nonzero socle and its associated division ring is a field. We are now ready to give the proof of Theorem 2.

Proof of Theorem 2. Suppose that $R$ does not satisfy the property $(*)$. By assumption we have that $axb = 0$ for each $x \in \rho$ with $x^2 = 0$.

We first consider the case that $ab = 0$. Let $x \in \rho$. We claim that $axb = 0$. Suppose not. By assumption, there is a polynomial $h(x) = x + r_2x^2 + \cdots + r_kx^k$ with $k \geq 2$ and $r_kx^k \neq 0$, where each $r_i$ is an integer, satisfying

$$a(x + r_2x^2 + \cdots + r_kx^k)b = 0. \tag{1}$$

By (1), each element in $xbRa(1 + r_2x + \cdots + r_kx^{k-1})$ lies in $\rho$ and has square zero. Thus we have $axbRa(1 + r_2x + \cdots + r_kx^{k-1})b = 0$, implying $a(1 + r_2x + \cdots + r_kx^{k-1})b = 0$ as $axb \neq 0$. Since $ab = 0$, we have $a(r_2+r_3x+\cdots+r_kx^{k-2})xb = 0$. Repeating the same process we eventually conclude that $r_kaxb = 0$ and so $axb = 0$ follows, a contradiction. Hence, $a\rho b = 0$ follows, as desired.

We next consider the general case. Let $x \in \rho$; then $xa \in \rho$. By assumption, there is a polynomial $g_{xa}(t) \in \mathbb{Z}[t]$ so that $a(xa - xaxag_{xa}(xa))b = 0$ and so $\big(ax - (ax)^2g_{xa}(ax)\big)(ab) = 0$. Since $R$ does not satisfy the property $(*)$, applying Lemma 3 to the right ideal $a\rho$ we conclude that $ab = 0$. Therefore we have $a\rho b = 0$ by the first case.

Finally, when $a\rho b \neq 0$ we must prove that $\rho = eR$, where $e = e^2 \in R$ is such that $eRe$ is a field. Indeed, suppose that $a\rho b \neq 0$; then $R$ has the property $(*)$. Denote by $H$ the socle of $R$. If $\rho$ is a minimal right ideal of $R$, then we are done. Thus we may assume that $\rho$ is not minimal, nor is $\rho H$. Since $a\rho b \neq 0$, we have $a\rho Hb \neq 0$ and so there exists an idempotent $g \in \rho H$ such that $ag \neq 0$. Let $r \in R$; then $gr(1 - g)$ is an element in $\rho$ with square zero. By assumption, $agr(1 - g)b = 0$. Then $agR(1 - g)b = 0$ and so $b = gb \in \rho$. Let $\overline{\rho H} = \rho H/\rho H \cap \ell_R(\rho H)$. We claim that $\overline{\rho H}$ is a noncommutative prime ring. Since $\rho H$ is not a minimal right ideal of $R$, it contains an idempotent $f$ of rank 2. Then it is clear that $fHf$ can be canonically embedded in $\overline{\rho H}$. However, $fHf$ is isomorphic to $\mathrm{M}_2(F)$, the

2 by 2 matrix ring over $F$, where $F$ is the associated field of $R$. Thus $\overline{\rho H}$ is not commutative, as asserted.

Let $u, x \in \rho H$ and $z \in H$. Then there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $\overline{ua}\big(\overline{x} - \overline{x}^2 g_{\overline{x}}(\overline{x})\big)\overline{bz} = 0$ in $\overline{\rho H}$. In view of Theorem 1, either $\overline{ua} = 0$ or $\overline{bz} = 0$. That is, either $\rho H a \rho H = 0$ or $b H \rho H = 0$. So either $a\rho = 0$ or $b = 0$, a contradiction. This proves the theorem. □

We turn next to the proof of Theorem 3. For our proof we need a special case of KHARCHENKO's theorem [11, Theorem 1]. For the convenience of reference, we give its statement here.

**Lemma 4** (KHARCHENKO [11]). *Let $R$ be a prime ring and let $d$ be an $X$-outer derivation of $R$. Suppose that $\sum_{i=1}^m a_i d(x) b_i + \sum_{j=1}^n c_j x d_j = 0$ for all $x \in I$, a nonzero ideal of $R$, where $a_i, b_i, c_j, d_j \in Q$. Then $\sum_{i=1}^m a_i y b_i + \sum_{j=1}^n c_j x d_j = 0$ for all $x, y \in R$.*

In Lemma 4 we only assume that the linear identity holds on a nonzero ideal $I$, not on the whole prime ring $R$. Indeed, we remark that, applying the same argument with some minor modifications, [11, Theorem 1] still remains true even if the linear differential identity considered holds only on a nonzero ideal (instead of holding on the whole prime ring).

**Lemma 5.** *Let $R$ be a prime ring with a nonzero derivation $d$ and $e$ a nontrivial idempotent of $Q$. Suppose that $d(ex(1-e)) = 0$ for all $x \in I$, a nonzero ideal of $R$. Then there exists $b \in Q$ such that $d = \mathrm{ad}(b)$ and $be = 0$.*

PROOF. By assumption, we have

$$d(e)x(1-e) + ed(x)(1-e) - exd(e) = 0 \tag{2}$$

for all $x \in I$. Suppose on the contrary that $d$ is $X$-outer. Applying Lemma 4 to (2) yields

$$d(e)x(1-e) + ey(1-e) - exd(e) = 0 \tag{3}$$

for all $x, y \in R$. In particular, $eR(1-e) = 0$ and so either $e = 0$ or $e = 1$, which is a contradiction since $e$ is nontrivial. Thus $d$ is $X$-inner. Write $d = \mathrm{ad}(p)$ for some $p \in Q$. Expanding $d(ex(1-e)) = 0$ yields $pex(1-e) = ex(1-e)p$ for all $x \in I$ and hence for all $x \in R$ [7, Theorem 2]. It follows from MARTINDALE's lemma [14] that $pe = \beta e$ for some $\beta \in C$.

We set $b = p - \beta \in Q$. Then it is clear that $d = \mathrm{ad}(b)$ and $be = 0$. This proves the lemma. $\square$

Proof of Theorem 3. Let $A = \{x \in \rho \mid d(x) = 0\}$.Then $A$ is a subring of the ring $\rho$ and $\rho$ is co-radical over $A$. Set $\overline{\rho} = \rho/\rho \cap \ell_R(\rho)$ and let $\overline{A}$ be the canonical image of $A$ in $\overline{\rho}$. It is clear that $\overline{\rho}$ is also co-radical over $\overline{A}$ and $\overline{A}$ is a prime ring [5, Lemma 4]. In view of [1, Theorem 2], either $\overline{\rho}$ is commutative, or $\overline{A}_{\overline{A}}$ is a dense submodule of $\overline{\rho}_{\overline{A}}$.

Suppose that $\overline{\rho}$ is not commutative. Let $x \in \rho$. Then there exists a dense right ideal $\overline{I}$ of $\overline{A}$ such that $\overline{x}\overline{I} \subseteq \overline{A}$, where $I$ denotes the preimage of $\overline{I}$ in $A$. Let $a_1 \in I$. There exists an element $a_2 \in A$ such that $(xa_1 - a_2)\rho = 0$. In particular, $(xa_1 - a_2)A = 0$. Since $d(A) = 0$, we conclude that $d(x)a_1A = 0$. In particular, $\overline{\rho d(x)}\,\overline{I}\,\overline{A} = 0$. Since $\overline{I}\,\overline{A}$ is still a dense right ideal of $\overline{A}$, we conclude that $\overline{\rho d(x)} = 0$ in $\overline{\rho}$. That is, $\rho d(x)\rho = 0$ for all $x \in \rho$ and, hence, $d(\rho)\rho = 0$ follows. In view of Herstein's theorem [10], there exists $b \in Q$ such that $d = \mathrm{ad}(b)$ and $b\rho = 0$. Now, by assumption, for each $x \in \rho$ there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $d(x - x^2g_x(x)) = 0$. But $b\rho = 0$, so we have $(x - x^2g_x(x))b = 0$. Choose a nonzero ideal $J$ of $R$ such that $bJ \subseteq R$. Then $(x - x^2g_x(x))bJ = 0$. In view of Theorem 2, either $\rho bJ = 0$ or $\rho = eR$, where $e = e^2 \in R$, such that $eRe$ is a field. The latter case implies that $\overline{\rho}$ is a field, a contradiction. Thus $\rho bJ = 0$ follows and so $b = 0$, a contradiction again.

Thus we may always assume that $\overline{\rho}$ is commutative, that is, $[\rho, \rho]\rho = 0$. In view of [13, Proposition], $\rho C = gRC$ for some nonzero idempotent $g$ in the socle of $RC$. Note that each element in $[\rho, \rho]$ has square zero. By assumption, we have $d([\rho, \rho]) = 0$. Since $g \in \rho C$, we can choose a nonzero ideal $I$ of $R$ such that $Ig \subseteq R$ and $gI \subseteq \rho$. Then $gI^2g + gI^2(1-g) \subseteq \rho$ and so $gI^2gI^2(1-g) = [gI^2g, gI^2(1-g)] \subseteq [\rho, \rho]$. Thus $d(gI^2gI^2(1-g)) = 0$ follows. Note that $I^2gI^2$ is a nonzero ideal of $R$. If $\rho C = RC$, then $R$ is commutative, as desired. Suppose that $\rho C \neq RC$ and hence $g$ is a nontrivial idempotent in $RC$. In view of Lemma 5, we see that $d = \mathrm{ad}(b)$ for some $b \in Q$ such that $b\rho = 0$. By assumption, for $x \in \rho$ there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) so that $0 = [x - x^2g_x(x), b] =$

$(x - x^2 g_x(x))b$. But $\rho b \neq 0$, so, in view of Theorem 2, $\rho = eR$, where $e = e^2 \in R$, such that $eRe$ is a field, proving the theorem. □

We turn finally to the proof of Theorem 5. Following the notation given in [2], we let $Alg = \{t^n - t^{n+1}p(t) \mid n \geq 1,\ n \in \mathbb{Z},\ p(t) \in \mathbb{Z}[t]\}$. A ring $R$ is called a *special algebraic extension* of its subring $A$ if for each $x \in R$ there is a polynomial $f_x(t) \in Alg$, depending on $x$, such that $f_x(x) \in A$. The following theorem we need is a special case of [2, Theorem 1].

**Theorem 6.** *Let $R$ be a noncommutative domain. Suppose that $R$ is a special algebraic extension of its subring $A$. Then the complete rings of right quotients of $R$ and $A$ coincide.*

We need one more lemma in the proof of Theorem 5. Since it is an easy observation, we only give its statement without proof.

**Lemma 6.** *Let $R$ be a domain of characteristic $0$, $d$ a derivation of $R$ and $a \in R$. Suppose that there is a polynomial $f(t) \in \mathbb{Z}[t]$ with $\deg_t f(t) > 1$ such that both $d(a) \in \mathcal{Z}(R)$ and $d(f(a)) \in \mathcal{Z}(R)$. Then either $d(a) = 0$ or $a \in \mathcal{Z}(R)$.*

Proof of Theorem 5. We first dispose of two cases.

*Case 1.* Suppose that $R$ is a domain of characteristic zero. Let $a \in R$ be such that $d(a) \in \mathcal{Z}(R)$. By assumption, there is a polynomial $p(t) \in \mathbb{Z}[t]$, depending on $a^2$, such that $d(a^2 - a^4 p(a^2)) \in \mathcal{Z}(R)$. In view of Lemma 6, either $d(a) = 0$ or $a \in \mathcal{Z}(R)$. Thus we have proved the conclusion: for $a \in R$ if $d(a) \in \mathcal{Z}(R)$, then either $d(a) = 0$ or $a \in \mathcal{Z}(R)$. Set $B = \{a \in R \mid d(a) \in \mathcal{Z}(R)\}$. Now, $B$ is an additive group and since $d(\mathcal{Z}(R)) \subseteq \mathcal{Z}(R)$, $B$ is the union of its two additive subgroups: $\mathcal{Z}(R)$ and $\{a \in R \mid d(a) = 0\}$. Thus either $B = \mathcal{Z}(R)$ or $B = \{a \in R \mid d(a) = 0\}$.

Suppose first that $B = \mathcal{Z}(R)$. Then, by assumption, for each $x \in R$ there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) such that $d(x - x^2 g_x(x)) \in \mathcal{Z}(R)$ and, hence, $x - x^2 g_x(x) \in \mathcal{Z}(R)$. Applying Herstein's theorem [8] yields that $R$ is commutative. Suppose next that $B = \{a \in R \mid d(a) = 0\}$. Then for each $x \in R$ there is a polynomial $g_x(t) \in \mathbb{Z}[t]$ (depending on $x$) such that $d(x - x^2 g_x(x)) = 0$. In view of Theorem 4, $R$ is commutative. Case 1 is then proved.

*Case 2.* Suppose that $R$ is a domain of characteristic $p>0$. Let $x\in R$. By assumption, there is a polynomial $g_x(t)\in\mathbb{Z}[t]$ (depending on $x$) such that $d(x-x^2g_x(x))\in\mathcal{Z}(R)$ and so $d((x-x^2g_x(x))^p)=p(x-x^2g_x(x))^{p-1}d(x-x^2g_x(x))=0$. Thus $(x-x^2g_x(x))^p\in\ker(d)$. That is, $R$ is a special algebraic extension of its subring $\ker(d)$. If $R$ is commutative, we are done in this case. Hence, we assume that $R$ is not commutative. In view of Theorem 6, $\ker(d)$ is a dense submodule of $R$ as right $\ker(d)$-modules. Let $x\in R$. Choose a dense right ideal $\rho$ of $\ker(d)$ such that $x\rho\subseteq\ker(d)$. Thus $0=d(x\rho)=d(x)\rho$ as $d(\rho)=0$. Since $R$ is a domain, $d(x)=0$ follows. This proves $d=0$, a contradiction.

We turn to the general case. By Case 1 and Case 2, we may assume that $R$ is not a domain. Since $R$ is a prime ring, there is $0\neq a\in R$ with $a^2=0$. Let $x\in R$; then $(axa)^2=0$. Thus, by assumption, $d(axa)\in\mathcal{Z}(R)$ and so

$$d(a)xa+ad(x)a+axd(a)\in\mathcal{Z}(R). \tag{4}$$

Suppose for the moment that $d$ is $X$-outer. Applying Lemma 4 yields that $d(a)xa+aya+axd(a)\in\mathcal{Z}(R)$ for all $x,y\in R$. In particular, $aRa\subseteq\mathcal{Z}(R)$ and so $a=0$, a contradiction. Thus $d$ must be $X$-inner. Write $d=\operatorname{ad}(b)$ for some $b\in Q$. We now reduce (4) to

$$baxa-axab\in\mathcal{Z}(R) \tag{5}$$

for all $x\in R$. Suppose for the moment that

$$baxa=axab \tag{6}$$

for all $x\in R$. In view of Martindale's lemma [14], there exists $\beta\in C$ such that $(b-\beta)a=0$. Since $d=\operatorname{ad}(b)=\operatorname{ad}(b-\beta)$, replacing $b$ by $b-\beta$ we may assume that $ba=0$. For $x\in R$ there exists a polynomial $g_{ax}(t)\in\mathbb{Z}[t]$ such that

$$\big[b,ax-(ax)^2g_{ax}(ax)\big]\in\mathcal{Z}(R)$$

and so

$$\big(ax-(ax)^2g_{ax}(ax)\big)b=0 \tag{7}$$

for all $x \in R$. Applying Lemma 3 to (7) yields that $RC$ is a strongly primitive ring. Suppose next that $baxa - axab \neq 0$ for some $x \in R$. Applying [6, Theorem 1] we have $\dim_C RC = 4$. Thus $RC$ is also a strongly primitive ring.

In either case, $RC$ is a primitive ring with nonzero socle $H$ and $H$ possesses nontrivial idempotents as $R$ is not a domain. For each idempotent $e \in H$ we choose a nonzero ideal $I$ of $R$ such that $eI(1-e)+(1-e)Ie \subseteq R$. Thus, by assumption, $[b, ex(1-e)] \in \mathcal{Z}(R)$ and $[b,(1-e)xe] \in \mathcal{Z}(R)$ and so $[b,[e,x]] \in \mathcal{Z}(R)$ for all $x \in I$ and hence $[b,[e,x]] \in C$ for all $x \in H$ (see [7, Theorem 2]). Also, the additive subgroup of $H$ generated by all idempotents in $H$ contains $[H,H]$ and, moreover, $[[H,H],H] = [H,H]$ as $H$ is a noncommutative simple ring. Therefore, we have $[b,[H,H]] \subseteq C$, implying that $[b,[Q,Q]] \subseteq C$ by [7, Theorem 2] again. It is clear that $[Q,Q]$ is a noncentral Lie ideal of the prime ring $Q$. Since $b \notin C$, applying [12, Lemma 8] we conclude that $\operatorname{char} R = 2$ and $\dim_C RC = 4$. But $RC$ is not a domain, so $RC = Q \cong \mathrm{M}_2(C)$. We claim that $C$ is algebraic over GF(2). Let $\beta \in C$. By assumption, there is a polynomial $g(t) \in \mathbb{Z}[t]$ such that $[b, \beta e_{11} - (\beta e_{11})^2 g(\beta e_{11})] \in C$, implying $[b,y] \in C$, where $y = \big(\beta - \beta^2 g(\beta)\big)e_{11}$. If $y \notin [RC,RC]$, then $Cy + [RC,RC] = RC$ and so $[b,RC] \subseteq C$, implying that $b \in C$, a contradiction. Thus $y \in [RC,RC]$ and so the trace of $y$ is 0. That is, $\beta - \beta^2 g(\beta) = 0$. Thus $\beta$ is algebraic over GF(2), as desired. This proves the theorem. □

*Acknowledgement.* The authors would like to express their sincere thanks to the referee for her/his valuable suggestions and for pointing out several misprints, which help to clarify the whole paper.

## References

[1] O. K. Babkov, Algebraic extensions of rings and rings of quotients, *Algebra i Logika* **19** (1) (1980), 5–22.

[2] O. K. Babkov, On rings of quotients of special algebraic extensions of semiprime rings, *Soviet Math. Dokl.* **29** no. 2 (1984), 368–371.

[3] H. E. Bell, On the commutativity of prime rings with derivations, *Quaest. Math.* **22** (3) (1999), 329–335.

[4] M. Chacron, A commutativity theorem for rings, *Proc. Amer. Math. Soc.* **59** (1976), 211–216.

[5] M. Chacron, Co-radical extension of *PI*-rings, *Pacific J. Math.* **62** (1976), 61–64.

[6] C.-M. Chang and T.-K. Lee, Derivations and central linear generalized polynomials in prime rings, *Southeast Asian Bull. Math.* **21** (1997), 215–225.

[7] C.-L. Chuang, GPIs having coefficients in Utumi quotient rings, *Proc. Amer. Math. Soc.* **103** (1988), 723–728.

[8] I. N. Herstein, The structure of a certain class of rings, *Amer. J. Math.* **75** (1953), 864–871.

[9] I. N. Herstein, Topics in Ring Theory, *University of Chicago Press*, *Chicago*, 1969.

[10] I. N. Herstein, A condition that a derivation be inner, *Rend. Cir. Mat. Palermo Ser.* II **37** (1988), 5–7.

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

[12] C. Lanski and S. Montgomery, Lie structure of prime rings of characteristic 2, *Pacific J. Math.* **42** (1972), 117–136.

[13] T.-K. Lee, Power reduction property for generalized identities of one-sided ideals, *Algebra Colloq.* **3** (1996), 19–24.

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

TSIU–KWEN LEE
DEPARTMENT OF MATHEMATICS
NATIONAL TAIWAN UNIVERSITY
TAIPEI 106
TAIWAN

*E-mail*: tklee@math.ntu.edu.tw

CHING–YUEH PAN
DEPARTMENT OF MATHEMATICS
NATIONAL TAIWAN UNIVERSITY
TAIPEI 106
TAIWAN

*E-mail*: cypan@math.ntu.edu.tw

*(Received December 27, 2000; revised September 7, 2001)*