TAIWANESE JOURNAL OF MATHEMATICS
Vol. 1, No. 3, pp. 333-342, September 1997

DERIVATIONS AND CENTRALIZING MAPPINGS IN PRIME RINGS

Tsiu-Kwen Lee

Abstract. Let R be a prime ring with extended centroid C and ρ a nonzero right ideal of R. In this paper we investigate the derivations δ, d on R such that $[\delta(x), d(x)] \in C$ for all $x \in \rho$. As an application, we prove that any centralizing additive mapping f on ρ must be of the form $f(x) = \lambda x + \mu(x)$ for all $x \in \rho$, where $\lambda \in C$ and $\mu : \rho \to C$, except when $[\rho, \rho]\rho = 0$.

Let R be a ring with center Z and A a subset of R. A mapping f from A into R is said to be *commuting* if $[f(x), x] = 0$ for all $x \in A$ and *centralizing* if $[f(x), x] \in Z$ for all $x \in A$. The study of such mappings was initiated by a paper of E. Posner. In [22] Posner proved that a prime ring R must be commutative if it possesses a nonzero centralizing derivation. Over the last twenty years, many related results have been published (for instance, see the references of [1], [2], [4] and [20]). In [1] Brešar obtained a characterization of commuting additive mappings on prime rings and in [3] he extended the result to the semiprime case. Basing on these results Brešar initiated the study of functional identities (see [4] and [5]). The goal of the present paper is to give a characterization of centralizing additive mappings on one–sided ideals in prime rings. To state more precisely we first fix some notations.

Throughout this paper, R will be always a prime ring with center Z, extended centroid C, right Utumi quotient ring U and two–sided Martindale quotient ring Q (see [9] for these definitions). Brešar proved that every commuting additive mapping $f : \rho \to R$ is of the form $f(x) = \lambda x + \mu(x), x \in \rho$, for some $\lambda \in C$ and additive mapping $\mu : \rho \to C$, unless $[\rho, \rho]\rho = 0$ [4, Theorem 5.2]. In a recent paper [20] Lee and Lee obtained the same conclusion

Received July 9, 1996; revised March 24, 1997.
Communicated by P.-H. Lee.
1991 *Mathematics Subject Classification*: 16W25, 16N60, 16D15.
Key words and phrases: Derivation, PI, GPI, prime ring, quotient ring, centralizing mapping.

by assuming $f : \rho \to U$. For $x, y \in U$ we write $[x, y]_1 = [x, y] = xy - yx$ and $[x, y]_n = [[x, y]_{n-1}, y]$ for $n > 1$. Applying the theorem on functional identities [5], Brešar proved the following theorem [6].

Theorem B. *Let R be a prime ring and $f : R \to R$ an additive mapping. Suppose that there is a positive integer n such that $[f(x), x]_n = 0$ for all $x \in R$. If $\operatorname{char} R = 0$ or $\operatorname{char} R > n$, then $[f(x), x] = 0$ for all $x \in R$.*

We remark that Theorem B still holds without the restriction on $\operatorname{char} R$ if f is a derivation of R. Indeed, in [17] the author proved the following result.

Theorem L. *Let R be a semiprime ring with a derivation d and ρ a nonzero right ideal of R. Suppose that there exist $n, k \geq 1$ such that $[d(x^n), x^n]_k = 0$ for all $x \in \rho$. Then $[\rho, R]d(R) = 0$.*

Clearly, in the theorem above if R is a prime ring, then the conclusion is that either $d = 0$ or R is commutative. Therefore it seems natural to ask if Theorem B still holds without the restriction on $\operatorname{char} R$. More generally, we raise the following.

Conjecture. *Let R be a prime ring, ρ a nonzero right ideal of R and $f : \rho \to U$ an additive mapping. Suppose that there is a positive integer n such that $[f(x), x]_n = 0$ for all $x \in \rho$. Then $f(x) = \lambda x + \mu(x)$ for all $x \in \rho$, where $\lambda \in C$ and $\mu : \rho \to C$, unless $[\rho, \rho]\rho = 0$.*

We begin with the special case where f is a centralizing additive mapping. To arrive at the aim we need a theorem concerning derivations. Explicitly, we will prove the following two main results in this paper. Recall that a ring is called an S_4–ring or an S_4–free ring according as it satisfies the standard identity S_4 of degree 4 or not.

Theorem 1. *Let R be a prime S_4-free ring, ρ a nonzero right ideal of R, and δ and d two nonzero derivations of R with $\delta \notin Cd$. Suppose that $[\delta(x), d(x)]$ is central for all $x \in \rho$. Then there exist $p_0, q_0 \in Q$ with $p_0\rho = 0 = q_0\rho$ such that $d(x) = [p_0, x], \delta(x) = [q_0, x]$ for all $x \in \rho$, unless $\operatorname{char} R = 2$ and ρ satisfies the identity $\mathrm{S}_4(X_1, X_2, X_3, X_4)X_5$ (in which case $\rho C = eRC$ for some idempotent $e \in RC$ with $eRCe$ an S_4–ring).*

Theorem 2. *Let R be a prime ring and ρ a nonzero right ideal of R. Then every centralizing additive mapping $f : \rho \to U$ is of the form $f(x) = \lambda x + \mu(x)$ for all $x \in \rho$, where $\lambda \in C$ and $\mu : \rho \to C$, unless $[\rho, \rho]\rho = 0$.*

Remark. Let R be a prime ring and ρ a nonzero right ideal of R. In [4, Lemma 5.1] it was shown that $[\rho, \rho]\rho = 0$ if and only if RC is a strongly primitive ring with minimal right ideal ρC and commuting division ring C. We refer to [18] and [19] for a characterization of PI one–sided ideals in prime or semiprime rings.

We begin with some preliminary results. The first is an immediate consequence of [21, Theorem 2 (a)]. Therefore we give its statement without proof.

Lemma 1. *Let R be a prime ring. Suppose that $\sum_{i=1}^{m} a_i x_i b_i + \sum_{j=1}^{n} c_j x d_j = 0$ for all $x \in R$, where $a_i, b_i, c_j, d_j \in RC$, $1 \le i \le m, 1 \le j \le n$. 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 $c_1, \ldots, c_n$.*

As an application of Lemma 1 we have the following result which will be used in the proof of Theorem 1.

Lemma 2. *Let R be a prime ring and a, b elements in R. Suppose that $[ax, bx] \in Z$ for all $x \in R$. Then a and b are linearly dependent over C.*

Proof. In view of [8, Theorem 2] we have $[ax, bx] \in C$ for all $x \in U$. In particular, $[a, b] \in Z$ by setting $x = 1$. Expansion of $[a(x+1), b(x+1)] \in Z$ yields $[a, bx] + [ax, b] \in Z$ for all $x \in R$. Replacing x by xa we obtain that $ax[a, b] + [ax, b]a + [a, bx]a \in Z$. Commuting with a we arrive at $a[a, b][a, x] = 0$ for all $x \in R$. Thus $a[a, b] = 0$ and so $[a, b] = 0$ since $[a, b] \in Z$. For each $y \in R$, we have $[(ay)x, (by)x] \in Z$ for all $x \in R$. Hence $[ay, by] = 0$ for all $y \in R$ and, by [8, Theorem 2] again, $[ay, by] = 0$ for all $y \in U$. Expansion of $[a(x+1), b(x+1)] = 0$ yields $axb - bxa = 0$ for all $x \in R$. Therefore a and b are linearly dependent over C by Lemma 1.

Let ρ be a right ideal of a ring R. Denote by $\ell_R(\rho)$ the set $\{x \in R \mid x\rho = 0\}$, the left annihilator of ρ in R. Set $\overline{\rho} = \rho/(\rho \cap \ell_R(\rho))$. It is easily seen that $\overline{\rho}$ is a prime ring if R is. Though the next lemma is intuitively true, we give its proof here for the sake of completeness.

Lemma 3. *Let R be a prime ring with extended centroid C and ρ a nonzero right ideal of R. Then the extended centroid F of $\overline{\rho}$ is isomorphic to C in such a way that if $\gamma \in C$ maps to $\overline{\gamma} \in F$ then for any ideal J of ρ with $\gamma J \subseteq \rho$ and $J_\rho \ne 0$ we have $\overline{\gamma x} = \bar{\gamma}\bar{x}$ for all $x \in J$. In particular, if R has C as its center, then $\overline{\gamma x} = \bar{\gamma}\bar{x}$ for all $x \in \rho$ and $\gamma \in C$.*

Proof. Let $\gamma \in C$ and J an ideal of ρ such that $J\rho \neq 0$ and $\gamma J \subseteq \rho$. (For instance $J = \rho I$ where I is a nonzero ideal of R such that $\gamma I \subseteq R$.) The map $\overline{x} \mapsto \overline{\gamma x}$ is a $(\overline{\rho}, \overline{\rho})$–homomorphism of $\overline{J}$ into $\overline{\rho}$, so there exists $\overline{\gamma} \in F$ such that $\bar{\gamma}\bar{x} = \overline{\gamma x}$ for all $x \in J$. The element $\bar{\gamma} \in F$ is independent of the choice of J. Indeed, if $\overline{\gamma}' \in F$ satisfies $\bar{\gamma}'\bar{x} = \overline{\gamma x}$ for all $x \in J'$ where J' is an ideal of ρ such that $J'\rho \neq 0$ and $\gamma J' \subseteq \rho$, then $(J \cap J')\rho \neq 0$ and $\bar{\gamma}'\bar{x} = \bar{\gamma}\bar{x}$ for all $x \in J \cap J'$ and so $\bar{\gamma}' = \bar{\gamma}$. It is easily seen that the mapping $\gamma \mapsto \bar{\gamma}$ is an isomorphism of C into F.

Now let $\mu \in F$. Choose a nonzero ideal J of ρ such that $J\rho \neq 0$ and $\mu\overline{J} \subseteq \overline{\rho}$. Fix a nonzero element $h \in \rho$ and consider the mapping of $RJ\rho$ into R defined by $\sum_i r_i x_i y_i \mapsto \sum_i r_i t_i y_i h$ for $r_i \in R, x_i \in J, y_i \in \rho$ and $t_i \in \rho$ with $\mu\overline{x_i} = \overline{t_i}$. Then the mapping is well–defined; for if $\sum_i r_i x_i y_i = 0$, then $\sum_i u r_i x_i y_i = 0$ for all $u \in \rho$ so $\sum_i \overline{ur_i}\overline{x}_i\overline{y}_i = 0$ and $\sum_i \overline{ur_i}\overline{t_i}\overline{y_i} = 0$, that is, $\Big(u\sum_i r_i t_i y_i\Big)\rho = 0$ for all $u \in \rho$ and hence $\big(\sum_i r_i t_i y_i\big)\rho = 0$ and, in particular, $\sum_i r_i t_i y_i h = 0$. This mapping is obviously a homomorphism of left R–modules and so there exists a in the left Martindale quotient ring of R such that $rxya = rtyh$ for all $r \in R$, $x \in J$, $y \in \rho$ and $t \in \rho$ with $\mu\overline{x} = \bar{t}$. Hence $xya = tyh$ and so $xyra = tyrh$ for all $r \in R$. Since $xy \neq 0$ for some $x \in J$, $y \in \rho$, there exists $\beta \in C$ such that $a = \beta h$. Then $(\beta xy - ty)Rh = 0$ and so $\beta xy = ty$. That is, $\beta J\rho \subseteq \rho$. Note that $J\rho$ is an ideal of ρ with $(J\rho)\rho \neq 0$ and so $\overline{\beta}\overline{xy} = \overline{\beta xy} = \overline{ty} = \bar{t}\bar{y} = \mu\bar{x}\bar{y} = \mu\overline{xy}$ for all $x \in J$, $y \in \rho$. Hence $\overline{\beta} = \mu$ and so C is isomorphic to F via $\gamma \mapsto \bar{\gamma}$. The last statement is obvious.

Recall that a derivation d of R is called *X–inner* if d is induced by some element $a \in Q$, that is, $d(x) = ax - xa$ for all $x \in R$ (see [12] and [13]). In this case write $d = \mathrm{ad}(a)$. Also, d is called *outer* if d is not X–inner. Let D_{int} stand for the C–subspace of all X–inner derivations of Q. We are now in a position to prove Theorem 1.

Proof of Theorem 1.

First, we claim that d and δ are C–dependent modulo D_{int}. By assumption, we have $\Big[\delta(xr), d(xr)\Big] = \Big[\delta(x)r + x\delta(r), d(x)r + xd(r)\Big] \in C$ for all $x \in \rho$ and $r \in R$. Assume on the contrary that d and δ are C–independent modulo D_{int}; then it follows from Kharchenko's theorem [13] that $\Big[\delta(x)r + xr_1, d(x)r + xr_2\Big] \in C$ for all $x \in \rho$ and $r, r_1, r_2 \in R$. In particular, we have $[xr_1, xr_2] \in Z$ for all $x \in \rho$ and $r_1, r_2 \in R$. Thus, for any nonzero x in ρ, the nonzero right ideal xR satisfies $[xR, xR] \subseteq Z$ which yields the commutativity of R, a contradiction. Therefore we may write $\delta = \alpha d + \mathrm{ad}(b)$ for some $\alpha \in C$ and $b \in Q$. Note that $b \notin C$ since $\delta \notin Cd$. We claim next that d, as well as δ, must be X–inner. Now $[\delta(xr), d(xr)] = [\alpha d(xr) + [b, xr], d(xr)] = [[b, xr], d(xr)] =$

$[[b, xr], d(x)r + xd(r)] \in C$ for all $x \in \rho$ and $r \in R$. Assume on the contrary that d is outer. Then, by Kharchenko's theorem again, $[[b, xr], d(x)r+xr_1] \in C$ for all $x \in \rho$ and $r, r_1 \in R$. By setting $r_1 = 0$, we have $[[b, xr], d(x)r] \in C$ for all $x \in \rho$ and $r \in R$. Hence $[[b, xr], xr_1] \in C$ for all $x \in \rho$ and $r, r_1 \in R$. Thus, for any nonzero x in ρ, the nonzero right ideal xR satisfies $[[b, xR], xR] \subseteq C$. Hence $[b, xR] \subseteq C$ and so $b \in C$, contrary to our choice of b. Therefore d must be X–inner.

Thus we write $d = \mathrm{ad}(p)$ and $\delta = \mathrm{ad}(q)$ for some $p, q \in Q$. Then we have

$$\left[[[p, x], [q, x]]\,, y\right] = 0 \tag{1}$$

for all $x \in \rho$ and all $y \in R$. By [8, Theorem 2], we see that (1) holds for all $x \in \rho Q$ and $y \in Q$. Replacing R and ρ by Q and ρQ respectively, we may assume that $1, p, q \in R, \rho C = \rho$ and R is centrally closed over its center C. In case C is infinite, set $\overline{R} = R \otimes_C \overline{C}$ and $\overline{\rho} = \rho \otimes_C \overline{C}$ where $\overline{C}$ is the algebraic closure of C. Then $\overline{R}$ is centrally closed ovre its center $\overline{C}$ [10] and (1) holds for all $x \in \overline{\rho}$ and $y \in \overline{R}$ by a standard argument (see, for instance, [23, Ex. 7.6.3, p. 287] or [15, Proposition]). Thus, replacing R, ρ and C with $\overline{R}$, $\overline{\rho}$ and $\overline{C}$ respectively, we may assume further that C is either finite or algebraically closed and proceed to show that $(p - \mu)\rho = (q - \nu)\rho = 0$ for some $\mu, \nu \in C$ except when $\mathrm{char}\, R = 2$ and ρ satisfies the polynomial identity $S_4(X_1, X_2, X_3, X_4)X_5$.

Note that $1, p$ and q are C–independent. Suppose first that $1, p$ and q are C–dependent modulo $\ell_R(\rho)$. That is, there exist $\alpha, \beta, \gamma \in C$, not all zero, such that $(\alpha + \beta p + \gamma q)\rho = 0$. Note that either $\beta \neq 0$ or $\gamma \neq 0$. Say, assume $\gamma \neq 0$ and set $q' = \alpha+\beta p+\gamma q$. Then $q'\rho = 0$ and so $[[p, x], xq'] = -[[p, x], [q', x]] \in C$ for all $x \in \rho$. We claim that $(p - \mu)\rho = 0$ for some $\mu \in C$. Assume on the contrary, then by [16, Lemma 3] either R is a PI–ring or there exists $x_0 \in \rho$ such that x_0 and px_0 are C–independent. In the latter case, $\left[[[p, x_0X], x_0Xq'], Y\right]$ is a nontrivial GPI for R. Hence R must be a GPI–ring in either case. By Martindale's theorem [21], R is a primitive ring with $\mathrm{soc}(R) \neq 0$ having C as commuting division ring.

Let $H = \mathrm{soc}(R)$ and $e = e^2 \in \rho H$ with rank $e = 1$. Then rank $(1 - e) \geq 2$ since R is S_4–free. For each $r \in R$, we have

$$[[p, er], erq'] \in C, \tag{2}$$

and so $(1-e)[[p, er], erq'] \in C(1-e)$. Expanding $(1-e)[[p, er], erq']$, we obtain that

$$(1 - e)pererq' \in C(1 - e). \tag{3}$$

for all $r \in R$. Since $(1-e)pererq'$ has rank at most 1 while nonzero elements in $C(1-e)$ have rank at least 2, it follows that $(1-e)pererq' = 0$ for all $r \in R$ and so $(1-e)pe = 0$ by [22, Lemma 2]. Thus $q'pe = q'epe \in q'\rho H = 0$ and so (2) reduces to $[p, er]erq' \in C$ which gives

$$[p, er]erq' = 0 \tag{4}$$

for all $r \in R$ since $q'\rho = 0$. Linearization of (4) yields

$$peserq' - esperq' + [p, er]esq' = 0 \tag{5}$$

for all $r, s \in R$. If pe and e are C–independent, it follows from Lemma 1 that, for each $r \in R$, we have $erq' = \lambda_r q'$ for some $\lambda_r \in C$. In case $\lambda_r \neq 0$, (4) reduces to $[p, er]q' = 0$. Thus, for each $r \in R$, either $erq' = 0$ or $[p, er]q' = 0$. Hence, either $eRq' = 0$ or $[p, eR]q' = 0$. Since R is prime, $eRq' \neq 0$ and so $[p, eR]q' = 0$. In view of [11], $(p-\lambda)eR = 0$ for some $\lambda \in C$ and so $pe = \lambda e$, a contradiction. Hence pe and e must be C–dependent, that is, $pe = \mu e$ for some $\mu \in C$. Suppose that ρ_1 and ρ_2 are two distinct minimal right ideals contained in ρH. By what we have just proved, there exist $\mu_1, \mu_2 \in C$ such that $px = \mu_1 x$ for all $x \in \rho_1$ and $py = \mu_2 y$ for all $y \in \rho_2$. Then expansion of $[[p, x+y], (x+y)q'] \in C$ yields $(\mu_1 - \mu_2)[x, y]q' \in C$ and so $(\mu_1 - \mu_2)[x, y]q' = 0$ for all $x \in \rho_1$ and $y \in \rho_2$. If $\mu_1 \neq \mu_2$, then, for each $x \in \rho_1$, we have $[x, \rho_2]q' = 0$. Again, by [11], $(x - \xi)\rho_2 = 0$ for some $\xi \in C$. Thus $x\rho_2 = \xi\rho_2 \subseteq \rho_1 \cap \rho_2 = 0$ for each $x \in \rho_1$, a contradiction. Therefore, $\mu_1 = \mu_2$. In other words, there exists $\mu \in C$ such that $(p-\mu)\rho' = 0$ for each minimal right ideal ρ' contained in ρH. Since ρH is a sum of minimal right ideals, we have $(p-\mu)\rho H = 0$ and so $(p-\mu)\rho = 0$. Set $p_0 = p - \mu$ and $q_0 = q + \gamma^{-1}(\alpha + \beta\mu)$; then $d = \mathrm{ad}(p_0), \delta = \mathrm{ad}(q_0)$ and $p_0\rho = q_0\rho = 0$.

Suppose next that $(\alpha + \beta p + \gamma q)\rho = 0$ implies $\alpha = \beta = \gamma = 0$ for $\alpha, \beta, \gamma \in C$. By [16, Lemma 3], either R is a PI–ring or there exists $x_0 \in \rho$ such that x_0, px_0 and qx_0 are C–independent. However, in the latter case, $\Big[[[p, x_0X], [q, x_0X]], Y\Big]$ is a nontrivial GPI for R, and therefore R must be a GPI–ring in either case. Then R is a primitive ring with nonzero socle H having C as commuting division ring. Let $e = e^2 \in \rho H$ with rank $e = 1$. Then rank $(1-e) \geq 2$ and so $(1-e)R(1-e)$ is not commutative. We claim first that $(1-e)pe = 0$ if and only if $(1-e)qe = 0$. For each $r \in R$, we have $(1-e)[[p, er], [q, er]] \in C(1-e)$. Suppose that $(1-e)pe = 0$. Expanding $(1-e)[[p, er], [q, er]]$, we obtain $(1-e)qer[p, er] \in C(1-e)$ and comparison of ranks yields

$$(1-e)qer[p, er] = 0 \tag{6}$$

for all $r \in R$. Linearization of (6) yields

$$(1-e)qer[p,es] + (1-e)qes[p,er] = 0 \tag{7}$$

for all $r, s \in R$. Replacing r by $r(1-e)$ in (7), we have

$$(1-e)qes[p,er(1-e)] = 0 \tag{8}$$

for all $r, s \in R$. Hence either $(1-e)qe = 0$ or $[p, er(1-e)] = 0$ for all $r \in R$. In the latter case, $per(1-e) - er(1-e)p = 0$ for all $r \in R$. Since $1 - e \neq 0$, it follows from Lemma 1 that $pe = \lambda e$ for some $\lambda \in C$. Then (6) reduces to $(1-e)qerer(\lambda - p) = 0$ for all $r \in R$ and so $(1-e)qe = 0$. Conversely, $(1-e)pe = 0$ follows from $(1-e)qe = 0$ symmetrically. We continue to show that both $(1-e)pe = 0$ and $(1-e)qe = 0$ as a matter of fact.

Assume that $(1-e)pe \neq 0$. For $r, s \in R$ we have

$$(1-e)[[p, er(1-e)s(1-e)], [q, er(1-e)s(1-e)]] \in C(1-e) \tag{9}$$

for all $r, s \in R$. Expansion of (9) yields

$$[(1-e)per(1-e)s(1-e), (1-e)qer(1-e)s(1-e)] \in C(1-e) \tag{10}$$

for all $r, s \in R$. By Lemma 2, we see that $(1-e)per(1-e)$ and $(1-e)qer(1-e)$ are C–dependent for each $r \in R$. Suppose that $(1-e)pet(1-e) = 0$ for some $t \in R$. Replacing r by $r + t$ in (10), we obtain

$$[(1-e)per(1-e)s(1-e), (1-e)qet(1-e)s(1-e)] \in C(1-e) \tag{11}$$

for all $r, s \in R$. If $(1-e)qet(1-e) \neq 0$, then $(1-e)per(1-e) \in C(1-e)qet(1-e)$ for all $r \in R$. Thus $(1-e)peR(1-e)$ is a nonzero commutative right ideal of $(1-e)R(1-e)$, a contradiction. Hence $(1-e)qet(1-e) = 0$ whenever $(1-e)pet(1-e) = 0$. Thus, for each $t \in R$, we have $(1-e)qet(1-e) = \lambda_t(1-e)pet(1-e)$ for some $\lambda_t \in C$. Since $(1-e)peR(1-e)$ has dimension at least 2 over C, a standard argument shows that there exists $\lambda \in C$ such that $(1-e)qet(1-e) = \lambda(1-e)pet(1-e)$ for all $t \in R$, or equivalently, $(1-e)(q - \lambda p)eR(1-e) = 0$. Hence, $(1-e)(q - \lambda p)e = 0$. Set $q' = q - \lambda p$; then $(1-e)q'e = 0$. Note that q' enjoys the same properties as q does; namely, $[[p,x],[q',x]] \in C$ for all $x \in \rho$ and $(\alpha + \beta p + \gamma q')\rho = 0$ implies $\alpha = \beta = \gamma = 0$. In view of the previous paragraph, $(1-e)pe = 0$ follows from $(1-e)q'e = 0$ and hence $(1-e)qe = 0$ holds too. Thus $p(eR) = epeR \subseteq eR$ and similarly $q(eR) \subseteq eR$. Hence $p(\rho H) \subseteq \rho H$ and $q(\rho H) \subseteq \rho H$ since ρH is a sum of minimal right ideals of the form eR with $e^2 = e$ and rank $e = 1$.

Let $S = \rho H/(\rho H \cap \ell_R(\rho H))$; then S is a prime ring. Since R has C as its center, it follows from Lemma 3 that the elements of the extended centroid of S are of the form $\overline{\gamma}$ with $\gamma \in C$ such that $\bar{\gamma}\bar{x} = \overline{\gamma x}$ for all $x \in \rho H$ where $\overline{x}$ denotes the canonical image of x in S. The derivations d and δ induce naturally derivations $\overline{d}$ and $\overline{\delta}$ on S given by $\overline{d}(\overline{x}) = \overline{[p,x]}$ and $\overline{\delta}(\overline{x}) = \overline{[q,x]}$ for $x \in \rho H$. By assumption we have $\Big[[\overline{d}(\overline{x}), \overline{\delta}(\overline{x})], \overline{y}\Big] = 0$ for all $\overline{x}, \overline{y} \in S$. In view of [14, Theorem 4], either $\overline{d} = 0$ or $\overline{\delta} = \bar{\lambda}\bar{d}$ for some $\lambda \in C$ except when $\operatorname{char} S = 2$ and S satisfies S_4.

Suppose that either $\overline{d} = 0$ or $\overline{\delta} = \bar{\lambda}\bar{d}$ for some $\lambda \in C$. That is, $[p, \rho H]\rho H = 0$ or $[q - \lambda p, \rho H]\rho H = 0$. By [11] again, we have either $(p - \mu)\rho H = 0$ or $(q - \lambda p - \nu)\rho H = 0$ for some μ or ν in C, contrary to the C–independence of $1, p$ and q modulo $\ell_R(\rho)$. Hence $\operatorname{char} S = 2$ and S satisfies S_4. Thus $2(\rho H)^2 = 0$ and so $2\rho H = 0$. Therefore R has characteristic 2. Now S satisfies $\mathrm{S}_4(X_1, X_2, X_3, X_4)$, so ρH satisfies $\mathrm{S}_4(X_1, X_2, X_3, X_4)X_5$. Then $\rho R = \rho$ satisfies $\mathrm{S}_4(X_1, X_2, X_3, X_4)X_5$ by [8, Theorem 2]. The last statement in the parenthesis follows immediately from [18, Proposition]. This completes the proof of Theorem 1.

We next come to the proof of Theorem 2.

Proof of Theorem 2.

Suppose that $[\rho, \rho]\rho \neq 0$. Choose a subset $\{v_i\}_i$ of ρ to form a basis of ρC over C. Define $\widetilde{f} : \rho C \to U$ by the rule $\widetilde{f}(\sum_i \beta_i v_i) = \sum_i \beta_i f(v_i)$ for $\beta_i \in C$. Then $\widetilde{f}$ is a centralizing C–linear mapping on ρC. Following the same argument in the proof of [7, Lemma 6.3] we have

$$\Big[[\widetilde{f}(a), x], [a, x]\Big] \in C \tag{12}$$

for all $a, x \in \rho C$. We claim that $\widetilde{f}$ is commuting.

Consider first the situation when $\rho C = RC$. By [20, Theorem 4] it suffices to check the case when $\operatorname{char} R = 2$ and $\dim_C RC = 4$. Note that $U = RC$ in this case. Denote by F the algebraic closure of C. Then $RC \otimes_C F \cong \mathrm{M}_2(F)$. We extend $\widetilde{f}$ to $RC \otimes_C F$ by the rule $\widetilde{f}(\sum_i x_i \otimes \gamma_i) = \sum_i \widetilde{f}(x_i) \otimes \gamma_i$ for $x_i \in RC$ and $\gamma_i \in F$. Then $[\widetilde{f}(y), y] \in F$ for all $y \in RC \otimes_C F$. Let $\{e_{ij} \mid 1 \leq i, j \leq 2\}$ be the set of the usual matix units in $RC \otimes_C F \cong \mathrm{M}_2(F)$. Note that $\widetilde{f}$ is an F–linear mapping. Therefore $\widetilde{f}$ is determined by the values $\widetilde{f}(e_{ij})$ for $i, j = 1, 2$. For $e = e^2 \in RC \otimes_C F$ we have $[\widetilde{f}(e), e] = 0$ because $[a, e]_3 = [a, e]$ for all $a \in RC \otimes_C F$. Thus we obtain that $\widetilde{f}(e_{11}) = ae_{11} + be_{22}$ and $\widetilde{f}(e_{22}) = ce_{11} + de_{22}$ for some $a, b, c, d \in F$ by computing $[\widetilde{f}(e_{11}), e_{11}] = 0 = [\widetilde{f}(e_{22}), e_{22}]$. Using the fact that $\operatorname{char} R = 2$ and $[\widetilde{f}(e_{12}), e_{12}] \in F$ to expand $[\widetilde{f}(e_{11} + e_{12}), e_{11} + e_{12}] = 0$ we see that $\widetilde{f}(e_{12}) = \lambda e_{12} + \alpha(e_{11} + e_{22})$ where $\alpha \in F$ and $\lambda = a + b$. Also, expansion of $[\widetilde{f}(e_{12} + e_{22}), e_{12} + e_{22}] = 0$ yields $\lambda = c + d$ too. Similarly,

$\widetilde{f}(e_{21}) = \lambda e_{21} + \gamma(e_{11} + e_{22})$ for some $\gamma \in F$. Then $\widetilde{f}(e_{ij}) - \lambda e_{ij} \in F$ for $i, j = 1, 2$. Since $\widetilde{f}$ is an F–linear map, we have $\widetilde{f}(x) - \lambda x \in F$ for all $x \in RC \otimes_C F$. In particular, $\widetilde{f}$ is commuting on $\rho C = RC$.

So we may assume that $\rho C \neq RC$. If ρ does not satisfy any polynomial identity, then, by Theorem 1, it follows from (12) that for each $a \in \rho C$ we have $a \in C$, or $\widetilde{f}(a) \in Ca + C$, or $(\widetilde{f}(a) - \lambda_a)\rho C = 0$ for some $\lambda_a \in C$. It is obvious that $[\widetilde{f}(a), a] = 0$ follows from the first two cases. As to the last case, we have $[\widetilde{f}(a), a]\rho C = [\widetilde{f}(a) - \lambda_a, a]\rho C = -a(\widetilde{f}(a) - \lambda_a)\rho C = 0$ and so $[\widetilde{f}(a), a] = 0$ since $[\widetilde{f}(a), a] \in C$. That is, $\widetilde{f}$ is commuting on ρC. Suppose that ρ satisfies some polynomial identity. Then, by [18, Proposition], $\rho C = eRC$ for some $e = e^2 \in RC$. Note that $\rho U \neq U$; for otherwise $U = \rho U$ would be a PI–ring by [8, Theorem 2] and so $RC = U = \rho U = \rho C$, a contradiction. Since $[\widetilde{f}(e), e] = 0$, expansion of $(1 - e)([\widetilde{f}(e), ex] + [\widetilde{f}(ex), e])e = 0$ yields $(1 - e)\widetilde{f}(ex)e = 0$, that is, $\widetilde{f}(ex)e = e\widetilde{f}(ex)e \in \rho U$ for all $x \in RC$. Hence $[\widetilde{f}(ex), ex] \in C \cap \rho U = 0$ for all $x \in RC$. Hence $\widetilde{f}$ is commuting.

Thus we have shown that $\widetilde{f}$ is commuting. By [20, Theorem 2] there exists $\lambda \in C$ such that $\widetilde{f}(x) - \lambda x \in C$ for all $x \in \rho C$. In particular, $f(v_i) - \lambda v_i \in C$ for all basis elements v_i of ρC over C. For each $t \in \rho$, we have $[f(t) - \lambda t, v_i] = [f(t), v_i] + [\lambda v_i, t] = [f(t), v_i] + [f(v_i), t] \in C$ for each v_i. Thus $[f(t) - \lambda t, \rho C] \subseteq C$ and so $f(t) - \lambda t \in C$ for all $t \in \rho$. This completes the proof of Theorem 2.

Acknowledgement

The author would like to thank Professor P. H. Lee for thorough reading the original manuscript and for polishing the whole paper. In particular, the present shorter proofs of Lemma 2 and Theorem 1 are suggested by Professor P. H. Lee.

References

1. M. Brešar, Centralizing mappings and derivations in prime rings, *J. Algebra* **156** (1993), 385-394.

2. M. Brešar, Commuting traces of biadditive mappings, commutativity–preserving mappings and Lie mappings, *Trans. Amer. Math. Soc.* **355** (1993), 525-546.

3. M. Brešar, On certain pairs of functions of semiprime rings, *Proc. Amer. Math. Soc.* **120** (1994), 709-713.

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

5. M. Brešar, Functional identities of degree two, *J. Algebra* **172** (1995), 690-720.

6. M. Brešar, Applying the theorem on functional identities, *Nova J. Math., Game Theory, and Algebra* **4** (1995), 43-54.

7. M. Brešar, W. S. Martindale 3rd, and C. R. Miers, Centralizing maps in prime rings with involution, *J. Algebra* **161** (1993), 342-357.

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

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

10. T. S. Erickson, W. S. Martindale 3rd, and J. Osbern, Prime nonassociative algebras, *Pacific J. Math.* **60** (1975), 49-63.

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

12. V. K. Kharchenko, Differential identities of prime rings, *Algebra and Logic* **17** (1978) (2), 220-238.

13. V. K. Kharchenko, Differential identities of semiprime rings, *Algebra and Logic* **18** (1979) (1), 86-119.

14. C. Lanski, Differential identities of prime rings, Kharchenko's theorem, and applications, *Contemp. Math.* **124** (1992), 111-128.

15. P. H. Lee and T. L. Wong, Derivations cocentralizing Lie ideals, *Bull. Inst. Math. Acad. Sinica* **23** (1995), 1-5.

16. T. K. Lee, Left annihilators characterized by GPIs, *Trans. Amer. Math. Soc.* **347** (1995), 3159-3165.

17. T. K. Lee, Semiprime rings with hypercentral derivations, *Canad. Math. Bull.* **38** (1995), 445-449.

18. T. K. Lee, Power reduction property for generalized identities of one-sided ideals, *Algebra Colloquium* **3** (1996), 19-24.

19. T. K. Lee, A characterization of left ideals satisfying polynomial identities, *Chinese J. Math.* **24** (1996), 359-368.

20. T. K. Lee and T. C. Lee, Commuting additive mappings in semiprime rings, *Bull. Inst. Math. Acad. Sinica* **24** (1996), 259-268.

21. W. S. Martindale, III, Prime rings satisfying a generalized polynomial identity, *J. Algebra* **12** (1969), 576-584.

22. E. C. Posner, Derivations in prime rings, *Proc. Amer. Math. Soc.* **8** (1957), 1093-1100.

23. L. H. Rowen, Polynomial Identities in Ring Theory, Academic Press, New York, 1980.

Department of Mathematics, National Taiwan University
Taipei, Taiwan 10764
E-mail: tklee@math.ntu.edu.tw