TAIWANESE JOURNAL OF MATHEMATICS
Vol. 2, No. 4, pp. 457-467, December 1998

DERIVATIONS COCENTRALIZING POLYNOMIALS

Tsiu-Kwen Lee and Wen-Kwei Shiue

Abstract. Let R be a prime ring with extended centroid C and $f(X_1, \ldots, X_t)$ a polynomial over C which is not central-valued on RC. Suppose that d and δ are two derivations of R such that

$$d(f(x_1, \ldots, x_t))f(x_1, \ldots, x_t) - f(x_1, \ldots, x_t)\delta(f(x_1, \ldots, x_t)) \in C$$

for all $x_1, \ldots, x_t$ in R. Then either $d = 0 = \delta$, or $\delta = -d$ and $f(X_1, \ldots, X_t)^2$ is central-valued on RC, except when $\operatorname{char} R = 2$ and $\dim_C RC = 4$.

This paper is motivated by a result of Wong [14]. In [14], Wong proved the following result.

Theorem W. *Let K be a commutative ring with unity, R a prime K-algebra with center Z and $f(X_1, \ldots, X_t)$ a multilinear polynomial over K which is not central-valued on R. Suppose that d and δ are derivations of R such that*

$$d(f(x_1, \ldots, x_t))f(x_1, \ldots, x_t) - f(x_1, \ldots, x_t)\delta(f(x_1, \ldots, x_t)) \in Z$$

for all $x_1, \ldots, x_t$ in some nonzero ideal I of R. Then either $d = \delta = 0$ or $\delta = -d$ and $f(X_1, \ldots, X_t)^2$ is central-valued on R, except when $\operatorname{char} R = 2$ *and R satisfies the standard identity* S_4 *in* 4 *variables.*

We remark that the above theorem is a part of the study of a series of papers, initiated by Posner's paper [13], concerning derivations by a number of authors in the literature. We refer the reader to the references of [11]. For Theorem W, if $\delta = d$, the theorem can be regarded as Posner's theorem [13] on multilinear polynomials. For general polynomials, the first-named author proved the following result [11, Theorem 11].

Received May 8, 1997.
Communicated by P.-H. Lee.
1991 *Mathematics Subject Classification*: 16W25, 16R50, 16N60, 16U80.
Key words and phrases: Derivation, PI, GPI, prime ring, differential identity.

Theorem L. *Let R be a prime ring with extended centroid C and $f(X_1,\ldots,X_t)$ be a nonzero polynomial over C. Suppose that d is a nonzero derivation of R such that $\Big[d(f(x_1,\ldots,x_t)), f(x_1,\ldots,x_t)\Big] \in C$ for all $x_1,\ldots,x_t$ in R. Then*
(I) *$f(X_1,\ldots,X_t)^2$ is central-valued on RC if $\operatorname{char} R = 2$, unless $\dim_C RC = 4$.*
(II) *$f(X_1,\ldots,X_t)$ is central-valued on RC if $\operatorname{char} R \neq 2$.*

In this paper we shall use Theorem L to generalize Theorem W to its full generality. More precisely, the following result will be proved.

Main Theorem. *Let R be a prime ring with extended centroid C and $f(X_1,\ldots,X_t)$ a polynomial over C which is not central-valued on RC. Suppose that d and δ are two derivations of R such that*

$$d(f(x_1,\ldots,x_t))f(x_1,\ldots,x_t) - f(x_1,\ldots,x_t)\delta(f(x_1,\ldots,x_t)) \in C$$

for all $x_1,\ldots,x_t$ in R. Then either $d = 0 = \delta$, or $\delta = -d$ and $f(X_1,\ldots,X_t)^2$ is central-valued on RC, except when $\operatorname{char} R = 2$ and $\dim_C RC = 4$.

By [10, Theorem 2], each nonzero ideal of R and the right Utumi quotient ring U of R satisfy the same differential identities with coefficients in U. Thus the Main Theorem holds if the condition is imposed only for elements $x_1,\ldots,x_t$ in a nonzero ideal of R. We begin the proof with a theorem on invariant subspaces in prime algebras. By a strongly primitive ring we mean a primitive ring with nonzero socle and with associated division ring which is a finite-dimensional central division algebra. We denote by $\operatorname{soc}(R)$ the socle of R.

Theorem 1. *Let R be a strongly primitive ring with extended centroid C, $R = RC$ and $1 \in R$. Suppose that M is a C-subspace of R such that $uMu^{-1} \subseteq M$ for all invertible elements $u \in R$. Then either $M \subseteq C$ or $[\operatorname{soc}(R), \operatorname{soc}(R)] \subseteq M$, except when $\operatorname{char} R = 2$ and $\dim_C RC = 4$.*

Proof. Suppose first that R contains no nontrivial idempotents. Then R is a division algebra algebraic over C. In view of Asano's theorem [1, Theorem 7] we have that either $M \subseteq C$ or $[R,R] \subseteq M$ as desired. Suppose next that R contains nontrivial idempotents. It follows from Chuang's theorem [2, Theorem 1] that either $M \subseteq C$ or $[I,R] \subseteq M$ for some nonzero ideal I of R, unless $\operatorname{char} R = 2$ and $\dim_C RC = 4$. Since $\operatorname{soc}(R)$ is the smallest nonzero ideal of R, $[\operatorname{soc}(R), \operatorname{soc}(R)] \subseteq [I,R]$ in the latter case. This completes the proof. ■

The next result is a special case of the Main Theorem. For brevity we often denote $f(X_1,\ldots,X_t)$ and $f(x_1,\ldots,x_t)$ by $f(X_i)$ and $f(x_i)$ respectively.

For a derivation d of R, denote by $f^d(X_1,\dots,X_t)$ the polynomial obtained from $f(X_1,\dots,X_t)$ by replacing each coefficient α with $d(\alpha)$. Analogously, we often denote $f^d(X_1,\dots,X_t)$ by $f^d(X_i)$. Denote by $\mathrm{ad}(u)$ the inner derivation induced by $u \in U$, that is, $\mathrm{ad}(u)(x) = [u,x]$ for all $x \in U$.

Theorem 2. *Let R be a prime ring with extended centroid C and $f(X_1,\dots,X_t)$ a polynomial over C which is not central-valued on RC. Suppose that d is a derivation of R such that $d(f(x_i))f(x_i) \in C$ (or $f(x_i)d(f(x_i)) \in C$) for all $x_1,\dots,x_t$ in R. Then $d = 0$, except when* $\mathrm{char}\, R = 2$ *and* $\dim_C RC = 4$.

For clarifying its proof we introduce t polynomials associated with $f(X_1,\dots,X_t)$ as given in [11]. Set $g_i(Y_i,X_1,\dots,X_t)$ to be the sum of all possible monomials which are obtained from each monomial involving X_i of $f(X_1,\dots,X_t)$ by replacing one of the X_i's with Y_i for $1 \le i \le t$. For instance, if $f(X_1,X_2) = X_1^2X_2 + X_2X_1$, then $g_1(Y_1,X_1,X_2) = Y_1X_1X_2 + X_1Y_1X_2 + X_2Y_1$ and $g_2(Y_2,X_1,X_2) = X_1^2Y_2 + Y_2X_1$. We remark that

$$[b, f(x_1,\dots,x_t)] = \sum_{i=1}^{t} g_i([b,x_i], x_1,\dots,x_t) \tag{1}$$

for all $b, x_1,\dots,x_t \in U$. Also, each $g_i(Y_i,X_1,\dots,X_t)$ is linear in Y_i.

Before giving the proof of Theorem 2, we first show a preliminary lemma.

Lemma 1. *Let R be a prime ring with center Z, extended centroid C, L a noncentral Lie ideal of R and $a, b \in R$, $a \ne 0$. Suppose that $[b,L]a \subseteq Z$ (or $a[b,L] \subseteq Z$). Then $b \in Z$ except when* $\mathrm{char}\, R = 2$ *and* $\dim_C RC = 4$.

Proof. We prove only the case when $[b,L]a \subseteq Z$. The proof for the other case is similar. Suppose that either $\mathrm{char}\, R \ne 2$ or $\dim_C RC > 4$. Set $I = R[L,L]R$. In view of [7, Lemma 7], $[L,L] \ne 0$ follows and so I is a nonzero ideal of R. Note that $[I,R] \subseteq L$. Thus $[b,[I,I]]a \subseteq Z$ and hence $[b,[R,R]]a \subseteq Z$ [3]. If $[b,[R,R]]a = 0$, then we are done by [9, Theorem 6] and [5, Lemma 3]. We may assume henceforth that $0 \ne [b,[R,R]]a \subseteq Z$. Then $b \notin Z$ and $\Big[[b,[X_1,X_2]]a, X_3\Big]$ is a nontrivial GPI for R. It follows from Martindale's theorem [12] that RC is a strongly primitive ring. By [3, Theorem 2], $0 \ne \Big[b, [\mathrm{soc}(RC), \mathrm{soc}(RC)]\Big]a \subseteq C$ and hence $\mathrm{soc}(RC)$ contains a nonzero central element and so RC is a finite-dimensional central simple C-algebra. In particular, a is invertible in RC. Thus we have $[b,[R,R]] \subseteq Ca^{-1}$. In particular, $\Big[[b,[R,R]], [b,[R,R]]\Big] = 0$. Since $[R,R]$ is a noncentral Lie ideal of R, in view of [9, Theorem 3] and [5, Corollary] we obtain $b \in Z$, a contradiction. This proves the lemma. ∎

Proof of Theorem 2. Suppose that either char $R \neq 2$ or $\dim_C RC > 4$. The aim is to prove that $d = 0$. Suppose on the contrary that $d \neq 0$. By symmetry we may assume that $d(f(x_i))f(x_i) \in C$ for all $x_i \in R$. Expansion of it yields that

$$\left(f^d(x_i) + \sum_{j=1}^{t} g_j(d(x_j), x_1, \dots, x_t)\right) f(x_i) \in C \tag{2}$$

for all $x_i \in R$. Suppose first that d is not a Q-inner derivation. Applying Kharchenko's theorem [6] to (2) we have

$$\left(f^d(x_i) + \sum_{j=1}^{t} g_j(y_j, x_1, \dots, x_t)\right) f(x_i) \in C \tag{3}$$

for all $x_i, y_i \in R$. Setting $y_i = 0$ for all i in (3) we obtain that $f^d(x_i)f(x_i) \in C$ and so

$$\left(\sum_{j=1}^{t} g_j(y_j, x_1, \dots, x_t)\right) f(x_i) \in C \tag{4}$$

for all $x_i, y_i \in R$. Let $u \in R$ and set $y_i = [u, x_i]$ in (4). By (1) we have $[u, f(x_i)]f(x_i) \in C$. By [3, Theorem 2], $[U, f(x_i)]f(x_i) \subseteq C$ for all $x_i \in U$. It follows from Lemma 1 that $f(X_i)$ is central-valued on U in this case, a contradiction.

Therefore we may assume that d is Q-inner, that is, $d = \mathrm{ad}(b)$ for some $b \in Q$, the two-sided Martindale quotient ring of R. Note that $b \notin C$ since $d \neq 0$. Now $[[b, f(X_i)]f(X_i), Y]$ is a nontrivial GPI for R and hence for U [3, Theorem 2]. By Martindale's theorem [12], U is a strongly primitive ring since U is a centrally closed prime C-algebra. Let $M = \{r \in U \mid [r, f(x_i)]f(x_i) \in C$ for all $x_i \in U\}$. Note that $b \in M$ and so $M \not\subseteq C$. Clearly, M is a C-subspace of U such that $uMu^{-1} \subseteq M$ for all invertible elements $u \in U$. Applying Theorem 1 we have that $[\mathrm{soc}(U), \mathrm{soc}(U)] \subseteq M$. By [3, Theorem 2] again, we have that

$$\Big[[[X, Y], f(X_i)]f(X_i), X_0\Big] \tag{5}$$

is a PI for U. In view of Lemma 1, $f(X_i)$ is central-valued on U and hence on RC, a contradiction. This completes the proof. ∎

From now on, we always make the following assumptions:

Let R be a prime ring with extended centroid C and $f(X_1, \dots, X_t)$ a nonzero polynomial over C which is not central-valued on RC. Suppose that

d and δ are two nonzero derivations of R such that

$$d(f(x_1,\dots,x_t))f(x_1,\dots,x_t) - f(x_1,\dots,x_t)\delta(f(x_1,\dots,x_t)) \in C \tag{6}$$

for all $x_1,\dots,x_t$ in R. Moreover, either $\operatorname{char} R \neq 2$ *or* $\dim_C RC > 4$.

If $\delta = -d$, by (6) we have $d(f(x_i)^2) \in C$ for all $x_i \in R$ and hence $f(X_i)^2$ central-valued on RC [11, Lemma 5]. *Thus we may assume further that $\delta \neq -d$.* The next lemma is to reduce δ and d to be Q-inner.

Lemma 2. *$d = \mathrm{ad}(p)$ and $\delta = \mathrm{ad}(q)$ for some $p, q \in Q$.*

Proof. Expanding (6) we have

$$\begin{aligned} &\left(f^d(x_i) + \sum_{j=1}^{t} g_j(d(x_j), x_1,\dots,x_t)\right) f(x_i) \\ &-f(x_i)\left(f^\delta(x_i) + \sum_{j=1}^{t} g_j(\delta(x_j), x_1,\dots,x_t)\right) \in C \end{aligned} \tag{7}$$

for all $x_i \in R$. Suppose first that d and δ are C-independent modulo Q-inner derivations. Applying Kharchenko's theorem [6] to (7) we have

$$\begin{aligned} &\left(f^d(x_i) + \sum_{j=1}^{t} g_j(y_j, x_1,\dots,x_t)\right) f(x_i) \\ &-f(x_i)\left(f^\delta(x_i) + \sum_{j=1}^{t} g_j(z_j, x_1,\dots,x_t)\right) \in C \end{aligned} \tag{8}$$

for all $x_i, y_i, z_i \in R$. Setting $y_i = 0 = z_i$ for all i in (8) we obtain $f^d(x_i)f(x_i) - f(x_i)f^\delta(x_i) \in C$ and hence

$$\left(\sum_{j=1}^{t} g_j(y_j, x_1,\dots,x_t)\right) f(x_i) - f(x_i)\left(\sum_{j=1}^{t} g_j(z_j, x_1,\dots,x_t)\right) \in C \tag{9}$$

for all $x_i, y_i, z_i \in R$. Let $u \in R$ and replacing y_i, z_i with $[u, x_i], 0$ respectively and then applying (1) we obtain $[u, f(x_i)]f(x_i) \in C$ for all $x_i \in R$ and hence for all $x_i \in U$ [3, Theorem 2]. It follows from Theorem 2 that $f(X_i)$ is central–valued on RC, a contradiction.

Suppose next that d and δ are C-dependent modulo Q-inner derivations. By symmetry we may assume that $\delta = \beta d + \mathrm{ad}(b)$ for some $\beta \in C$ and $b \in Q$.

If d is Q-inner, then so is δ and hence we are done in this case. Therefore we assume d to be outer. In view of (7) we have

$$\begin{aligned}&\left(f^d(x_i)+\sum_{j=1}^{t} g_j(d(x_j),x_1,\ldots,x_t)\right)f(x_i)\\ &-f(x_i)\left(\beta f^d(x_i)+\sum_{j=1}^{t} g_j(\beta d(x_j)+[b,x_j],x_1,\ldots,x_t)\right)\in C\end{aligned}\tag{10}$$

for all $x_i \in R$. Applying Kharchenko's theorem [6] to (10) yields

$$\begin{aligned}&\left(f^d(x_i)+\sum_{j=1}^{t} g_j(y_j,x_1,\ldots,x_t)\right)f(x_i)\\ &-f(x_i)\left(\beta f^d(x_i)+\sum_{j=1}^{t} g_j(\beta y_j+[b,x_j],x_1,\ldots,x_t)\right)\in C\end{aligned}\tag{11}$$

for all $x_i, y_i \in R$. Setting $y_i = 0$ in (11) and using (1) we have

$$f^d(x_i)f(x_i)-f(x_i)\left(\beta f^d(x_i)+[b,f(x_i)]\right)\in C\tag{12}$$

for all $x_i \in R$. Since $g_j(Y_j, X_1, \ldots, X_t)$ is linear in Y_j, it follows from (11) and (12) that

$$\left(\sum_{j=1}^{t} g_j(y_j,x_1,\ldots,x_t)\right)f(x_i)-\beta f(x_i)\left(\sum_{j=1}^{t} g_j(y_j,x_1,\ldots,x_t)\right)\in C\tag{13}$$

for all $x_i, y_i \in R$. Let $u \in R$ and replacing y_j with $[u, x_j]$ in (13) and using (1) we obtain

$$[u,f(x_i)]f(x_i)-\beta f(x_i)[u,f(x_i)]\in C\tag{14}$$

for all $x_i, u \in R$. Thus R is a PI-ring and so RC is a finite-dimensional central simple C-algebra by Posner's theorem for prime PI-rings. Suppose that $\dim_C RC = n^2$. Then $n \geq 2$. Note that RC and $\mathrm{M}_n(C)$ satisfy the same PIs. Thus, in view of (14), $[Y, f(X_i)]f(X_i) - \beta f(X_i)[Y, f(X_i)]$ is central-valued on $\mathrm{M}_n(C)$. Let e be an arbitrary idempotent in $\mathrm{M}_n(C)$ and let $y, x_i \in \mathrm{M}_n(C)$. Then

$$(1-e)\Big([ey(1-e),f(x_i)]f(x_i)-\beta f(x_i)[ey(1-e),f(x_i)]\Big)e=0.$$

That is, $(\beta+1)(1-e)f(x_i)ey(1-e)f(x_i)e = 0$. Suppose for the moment that $\beta \neq -1$. The primeness of R implies that $f(x_i)e = ef(x_i)e$. Analogously,

$ef(x_i) = ef(x_i)e$ and so $[f(x_i), e] = 0$. However, $\mathrm{M}_n(C)$ is spanned by idempotents over C. Thus $f(x_i) \in C$. That is, $f(X_i)$ is central-valued on $\mathrm{M}_n(C)$ and hence on RC, a contradiction. So $\beta = -1$ follows. By (14) we have $[R, f(x_i)^2] \subseteq C$ for all $x_i \in R$, implying that $f(X_i)^2$ is central-valued on RC. Replacing δ with $-d + \mathrm{ad}(b)$ in (6), we see that $d(f(x_i)^2) - f(x_i)[b, f(x_i)] \in C$ and hence $f(x_i)[b, f(x_i)] \in C$ for all $x_i \in R$. In view of Theorem 2, $b \in C$ follows and so $\delta = -d$, a contradiction. Thus δ and d are Q-inner. This completes the proof. ■

To continue our proof we define the following three sets, which are essential in the proof of the Main Theorem. Let

$$H = \{(a, b) \in U \times U \mid [a, f(x_i)]f(x_i) - f(x_i)[b, f(x_i)] \in C \text{ for all } x_i \in U\},$$

$$A = \{a \in U \mid (a, b) \in H \text{ for some } b \in U\}$$

and

$$E = \{a + b \mid (a, b) \in H\}.$$

By [3, Theorem 2], we may assume henceforth that $R = U$. In particular, R is a centrally closed prime C-algebra. Since $(p, q) \in H$, $p \notin C$ and $q \notin C$, R satisfies the nontrivial GPI $\Big[[p, f(X_i)]f(X_i) - f(X_i)[q, f(X_i)], Y\Big]$. It follows from Martindale's theorem [12] that R is a strongly primitive ring.

Lemma 3. *The Main Theorem holds if C is an infinite field.*

Proof. Recall that $R = U$. In this case, R is a strongly primitive ring. Denote by D its associated division C-algebra and let $\dim_C D = m^2$ for some $m \geq 1$. Then $\mathrm{soc}(R)$ is a simple ring with nonzero minimal right ideals. By Litoff's theorem [4], each element $x \in \mathrm{soc}(R)$ is contained in some eRe for some idempotent $e \in \mathrm{soc}(R)$. Note that $eRe \cong \mathrm{M}_\ell(D)$ where ℓ is the rank of e. Therefore x is algebraic over C.

Note that H is a C-subspace of $R \times R$. Let $(a, b) \in H$, $x \in \mathrm{soc}(R)$ and k the degree of the minimal polynomial of x over C. Since C is infinite, we can choose k distinct $\mu_i' s \in C$ such that $(x + \mu_i)^{-1}$ exists for each i. Then the C-subspace generated by these $(x + \mu_i)^{-1}$'s coincides with the C-subalgebra of R generated by x and 1. Now we have

$$\begin{aligned} & ((x + \mu_i)a(x + \mu_i)^{-1}, (x + \mu_i)b(x + \mu_i)^{-1}) - (a, b) \\ = \;& ([x, a](x + \mu_i)^{-1}, [x, b](x + \mu_i)^{-1}) \in H. \end{aligned}$$

Choose $\lambda_i \in C, 1 \leq i \leq k$, such that $1 = \sum_{i=1}^{k} \lambda_i (x + \mu_i)^{-1}$. Then

$$([x, a], [x, b]) = \sum_{i=1}^{k} \lambda_i([x, a](x + \mu_i)^{-1}, [x, b](x + \mu_i)^{-1}) \in H.$$

That is, $([a,x],[b,x]) \in H$ for all $x \in \mathrm{soc}(R)$. Let $x, y \in \mathrm{soc}(R)$. Then $([a,x],[b,x]) \in H$ and so

$$([[a,x],y],[[b,x],y]) \in H. \tag{15}$$

Note that $[a,x] \in \mathrm{soc}(R)$. Replacing y with $[a,x]$ in (15) yields that $(0,[[b,x],[a,x]]) \in H$. In view of Theorem 2 we see that $[[b,x],[a,x]] \in C$. In particular, $[[q,x],[p,x]] \in C$ for all $x \in \mathrm{soc}(R)$. By [8, Theorem 4], $q = \lambda p + \beta$ for some $\lambda, \beta \in C$, since either $\mathrm{char}\, R \neq 2$ or $\dim_C RC > 4$.

Replacing q with $\lambda p + \beta$ in (6) we see that

$$[p, f(x_i)]f(x_i) - \lambda f(x_i)[p, f(x_i)] \in C$$

for all $x_i \in R$. Consider the C-subspace of R:

$$L = \{r \in R \mid [r, f(x_i)]f(x_i) - \lambda f(x_i)[r, f(x_i)] \in C \text{ for all } x_i \in R\}.$$

Since $p \in L \setminus C$ and $uLu^{-1} \subseteq L$ for all invertible elements $u \in R$, it follows from Theorem 1 that $[\mathrm{soc}(R), \mathrm{soc}(R)] \subseteq L$. An application of [3, Theorem 2] yields that

$$\Big[[[X,Y], f(X_i)]f(X_i) - \lambda f(X_i)[[X,Y], f(X_i)], X_0\Big] \tag{16}$$

is a PI for R. By Posner's theorem for prime PI-rings, R is a finite-dimensional central simple C-algebra. Suppose that $\dim_C R = s^2$, where $s \geq 2$. Since R and $\mathrm{M}_s(C)$ satisfy the same PIs, it follows that (16) is also a PI for $\mathrm{M}_s(C)$. Let $x, x_i \in \mathrm{M}_s(C)$ and $e^2 = e \in \mathrm{M}_s(C)$. Note that $ex(1-e) = [e, ex(1-e)]$. By (16), $0 = (1-e)\Big([ex(1-e), f(x_i)]f(x_i) - \lambda f(x_i)[ex(1-e), f(x_i)]\Big)e$ and hence $(1+\lambda)(1-e)f(x_i)ex(1-e)f(x_i)e = 0$. If $\lambda = -1$, then $\delta = -d$, a contradiction. Thus $\lambda \neq -1$ and so $(1-e)f(x_i)e = 0$ follows from the primeness of R. Analogously, $ef(x_i)(1-e) = 0$. Therefore $[f(x_i), e] = 0$, which implies that $f(X_i)$ is central-valued on $\mathrm{M}_s(C)$ and hence on R, a contradiction. This completes the proof. ■

Proof of the Main Theorem. By Lemma 3 we assume that C is a finite field. Since R is a noncommutative strongly primitive ring, R is not a division ring. Recall that we may assume $R = U$. Therefore R contains nontrivial idempotents. We claim that $C = \mathrm{GF}(2)$, the Galois field of two elements. Suppose on the contrary that C has more than two elements. Let $w \in R$ with $w^2 = 0$, $(a,b) \in H$ and let $\beta \in C \setminus \{0,1\}$. Then $((1+w)a(1-w), (1+w)b(1-w)) - (a,b) \in H$ and $((1+\beta w)a(1-\beta w), (1+\beta w)b(1-\beta w)) - (a,b) \in H$. That is, $([a,w],[b,w]) + (waw, wbw) \in H$ and $([a,w],[b,w]) + \beta(waw, wbw) \in H$. These imply that $(waw, wbw) \in H$. Recalling the definition of H we see that

$$[waw, f(x_i)]f(x_i) - f(x_i)[wbw, f(x_i)] \in C$$

for all $x_i \in R$. Using $w^2=0$ to expand $w([waw, f(x_i)]f(x_i) - f(x_i)[wbw, f(x_i)])w$, we have $wf(x_i)w(a+b)wf(x_i)w = 0$. That is, $wf(x_i)wEwf(x_i)w = 0$. But E is a C-subspace of R invariant under inner automorphisms, it follows from Theorem 1 that either $E \subseteq C$ or $[\mathrm{soc}(R), \mathrm{soc}(R)] \subseteq E$. If the first case occurs, then $p+q \in C$ and so $\delta = -d$, a contradiction. Thus $[\mathrm{soc}(R), \mathrm{soc}(R)] \subseteq E$ and so $wf(x_i)w[\mathrm{soc}(R), \mathrm{soc}(R)]wf(x_i)w = 0$, implying $wf(x_i)w = 0$. In particular, let $w = ey(1-e)$ with $y \in R$, $1 \neq e = e^2 \in R$. Then $ey(1-e)f(x_i)ey(1-e) = 0$, implying $(1-e)f(x_i)e = 0$ [13, Lemma 2]. Similarly, $ef(x_i)(1-e) = 0$. Thus $[f(x_i), e] = 0$ and so $[f(x_i), W] = 0$, where W denotes the additive subgroup of R generated by the idempotents of R. Note that W is a noncentral Lie ideal of R. Since either $\mathrm{char}\, R \neq 2$ or $\dim_C RC > 4$, in view of [7, Lemma 8] we have $f(x_i) \in Z$. This proves that $f(X_i)$ is central-valued on R, a contradiction. Now we have shown that $C = \mathrm{GF}(2)$.

The next is to show that $R \cong \mathrm{M}_n(C)$ for some $n \geq 3$. By the fact that C is finite, it is enough to prove that R is a PI-ring. Suppose on the contrary that R is not a PI-ring. Let m be the degree of $f(X_i)$. Then there exists an idempotent e in $\mathrm{soc}(R)$ with $\mathrm{rank}(e) > m$. Note that $[\mathrm{soc}(R), \mathrm{soc}(R)] \subseteq A$. Let $x, x_i \in R$. Then there exists $y \in R$, depending only on $(1-e)xe \in A$, such that $[(1-e)xe, f(ex_ie)]f(ex_ie) - f(ex_ie)[y, f(ex_ie)] \in C$ and so

$$(1-e)\Big([(1-e)xe, f(ex_ie)]f(ex_ie) - f(ex_ie)[y, f(ex_ie)]\Big)e = 0.$$

That is, $(1-e)xf(ex_ie)^2 = 0$. It follows from the primeness of R and $e \neq 1$ that $f(ex_ie)^2 = 0$. Thus $f(X_i)^2$ is a PI for the simple Artinian C-algebra eRe and so $\dim_C eRe \leq m^2$ by the Kaplansky theorem for primitive PI-algebras. This is absurd as $\dim_C eRe = \mathrm{rank}(e)^2 > m^2$. Up to now we have proved that $R \cong \mathrm{M}_n(\mathrm{GF}(2)), n \geq 3$.

We claim that $f(X_1, \ldots, X_t)^2$ is central-valued on R. Since $p \in A \setminus C$, it follows from Theorem 1 that $[R, R] \subseteq A$. In particular, $e_{12} \in A$. Thus $(e_{12}, b) \in H$ for some $b \in R$. Note that $b \notin C$ by Theorem 2. Let $C_R(e_{12})$ denote the centralizer of e_{12} in R, namely $C_R(e_{12}) = \{x \in R \mid [x, e_{12}] = 0\}$. Let $u \in C_R(e_{12})$ be such that $1+u$ is invertible in R and $\mathrm{rank}(u) = 1$. Then $((1+u)e_{12}(1+u)^{-1}, (1+u)b(1+u)^{-1}) \in H$, that is, $(e_{12}, (1+u)b(1+u)^{-1}) \in H$ and hence

$$(0, [b, u](1+u)^{-1}) = (e_{12}, b) + (e_{12}, (1+u)b(1+u)^{-1}) \in H.$$

By Theorem 2, this implies that $[b, u](1+u)^{-1} \in C$ and so $[b, u] = 0$ since $\mathrm{rank}([b, u](1+u)^{-1}) \leq 2$.

Taking $u = e_{1j}$ with $j \geq 2$ or $u = e_{k2}$ with $k \geq 3$, we see that b commutes with these e_{1j} and e_{k2}. By a direct computation we see that $b \in C + Ce_{12}$ and hence $b = e_{12} + \mu$ for some $\mu \in C$, since $b \notin C$ and $C = \mathrm{GF}(2)$. Thus

$(e_{12}, e_{12}) \in H$. By Theorem L, this proves that $f(X_1, \ldots, X_t)^2$ is central-valued on R.

Now $f(X_1, \ldots, X_t)^2$ is central-valued on R, so $[p, f(x_1, \ldots, x_t)]f(x_1, \ldots, x_t) + f(x_1, \ldots, x_t)[p, f(x_1, \ldots, x_t)] = [p, f(x_1, \ldots, x_t)^2] = 0$ for all $x_i \in R$. Thus $(p, p) \in H$. On the other hand, $(p, q) \in H$, so $(0, p - q) \in H$. By Theorem 2, we have $p + q = p - q \in C$, that is, $\delta = -d$, a contradiction. This completes the proof of the Main Theorem. ■

Acknowledgement

The authors are grateful to Professor P.-H. Lee for pointing out some errors and for useful comments to simplify the proof of the Main Theorem.

References

1. S. Asano, On invariant subspaces of division algebras, *Kodai Math. J.* **18** (1966), 322-334.
2. C. L. Chuang, On invariant additive subgroups, *Israel J. Math.* **57** (1987), 116-128.
3. C. L. Chuang, GPIs having coefficients in Utumi quotient rings, *Proc. Amer. Math. Soc.* **103** (1988), 723-728.
4. C. Faith and Y. Utumi, On a new proof of Litoff's theorem, *Acta Math. Acad. Sci. Hungar.* **14** (1963), 369-371.
5. W. F. Ke, On derivations of prime rings of characteristic 2, *Chinese J. Math.* **13** (1985), 273-290.
6. V. K. Kharchenko, Differential identities of semiprime rings, *Algebra and Logic* **18** (1979), 86-119.
7. C. Lanski and S. Montgomery, Lie structure of prime rings of characteristic 2, *Pacific J. Math.* **42** (1972), 117-136.
8. C. Lanski, Differential identities of prime rings, Kharchenko's theorem, and applications, *Contemp. Math.* **124** (1992), 111-128.
9. P.-H. Lee and T. K. Lee, Lie ideals of prime rings with derivations, *Bull. Inst. Math. Acad. Sinica* **11** (1983), 75-80.
10. T. K. Lee, Semiprime rings with differential identities, *Bull. Inst. Math. Acad. Sinica* **20** (1992), 27-38.
11. T. K. Lee, Derivations with Engel conditins on polynomials, *Algebra Colloq.* **5** (1998), to appear.
12. W. S. Martindale, III, Prime rings satisfying a generalized polynomial identity, *J. Algebra* **12** (1969), 576-584.

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

14. T. L. Wong, Derivations cocentralizing multilinear polynomials, *Taiwanese J. Math.* **1** (1997), 31-37.

Department of Mathematics, National Taiwan University
Taipei 107, Taiwan
E-mail: tklee@math.ntu.edu.tw
E-mail: wkxue@math.ntu.edu.tw