Canad. Math. Bull. Vol. **56** (3), 2013 pp. 584–592
http://dx.doi.org/10.4153/CMB-2011-185-5

On Automorphisms and Commutativity in Semiprime Rings

Pao-Kuei Liau and Cheng-Kai Liu

Abstract. Let R be a semiprime ring with center $Z(R)$. For $x, y \in R$, we denote by $[x, y] = xy - yx$ the commutator of x and y. If σ is a non-identity automorphism of R such that

$$\Big[\Big[\cdots\Big[[\sigma(x^{n_0}), x^{n_1}], x^{n_2}\Big], \cdots\Big], x^{n_k}\Big] = 0$$

for all $x \in R$, where $n_0, n_1, n_2, \ldots, n_k$ are fixed positive integers, then there exists a map $\mu\colon R \to Z(R)$ such that $\sigma(x) = x + \mu(x)$ for all $x \in R$. In particular, when R is a prime ring, R is commutative.

1 Introduction and Results

Let R be a ring with center $Z(R)$. R is said to be semiprime if for $x \in R$, $xRx = 0$ implies $x = 0$ and R is said to be prime if for $x, y \in R$, $xRy = 0$ implies $x = 0$ or $y = 0$. For $x, y \in R$, set

$$[x, y]_1 = [x, y] = xy - yx \quad \text{and} \quad [x, y]_k = \big[[x, y]_{k-1}, y\big]$$

for $k > 1$. An Engel condition is a polynomial $[x, y]_k = \sum_{i=0}^{k}(-1)^i \binom{k}{i} y^i x y^{k-i}$ in noncommutative indeterminates x, y. The question of whether a ring is commutative or nilpotent if it satisfies an Engel condition goes back to the well-known result of Engel on Lie algebras [15].

A mapping $f\colon R \to R$ is called commuting (centralizing) if $[f(x), x] = 0$ (resp. $[f(x), x] \in Z(R)$) for all $x \in R$. The study of commuting and centralizing mappings began in 1955 when Divinsky [11] proved that a simple artinian ring is commutative if it has a commuting non-identity automorphism. In 1970 Luh [27] generalized Divinsky's result to prime rings. In 1976 Mayne [29] showed that a prime ring must be commutative if it possesses a non-identity centralizing automorphism. These results have been now generalized in various directions (see, for instance, [3, 4, 9, 20, 22, 30, 32, 33, 35]). In 1990 Vukman [31] studied the Engel type identities with derivations and proved that a prime ring R of char $R \neq 2$ is commutative if there is a nonzero derivation d of R such that $[d(x), x]_2 = 0$ for all $x \in R$. On the other hand, Deng and Bell [10] proved that a semiprime ring R contains a nonzero central ideal if either R is 6-torsion free and $[d(x), x]_2 \in Z(R)$ for all $x \in R$ or if R is $n!$-torsion free and $[d(x), x^n] \in Z(R)$ for all $x \in R$, where d is a nonzero derivation

Received by the editors March 31, 2011; revised June 1, 2011.
Published electronically January 27, 2012.
Corresponding author: Cheng-Kai Liu
AMS subject classification: **16N60**, 16W20, 16R50.
Keywords: semiprime ring, automorphism, generalized polynomial identity (GPI).

of R. Later Lee [21] and Lanski [18] independently extended these two results in full generality and studied the situation where $[[\cdots[[d(x^{n_0}),x^{n_1}],x^{n_2}],\cdots],x^{n_k}]=0$ for all $x\in R$. Several related generalizations can be found in [1, 6, 13, 14, 24, 25, 34]. The goal of this paper is to investigate the analogous result for automorphisms. Precisely, we prove the following theorem.

Theorem 1.1 *Let R be a semiprime ring with center $Z(R)$. If σ is an automorphism of R such that $\big[[\cdots[[\sigma(x^{n_0}),x^{n_1}],x^{n_2}],\cdots],x^{n_k}\big]=0$ for all $x\in R$, where $k,n_0,n_1,n_2,\dots,n_k$ are fixed positive integer (and independent of x), then there is a map $\mu\colon R\to Z(R)$ such that $\sigma(x)=x+\mu(x)$ for all $x\in R$ and $\mu(R)$ is contained in a central ideal of R.*

For prime rings, we have the following theorem.

Theorem 1.2 *Let R be a prime ring, let I be a nonzero ideal of R, and let σ be a non-identity automorphism of R. Suppose that $\big[[\cdots[[\sigma(x^{n_0}),x^{n_1}],x^{n_2}],\cdots],x^{n_k}\big]=0$ for all $x\in I$, where $k,n_0,n_1,n_2,\dots,n_k$ are fixed positive integers (and independent of x). Then R is commutative.*

2 The Prime Case

Let V_D be a right vector space over a division ring D. We denote $\mathrm{End}(V_D)$ the ring of D-linear transformations on V_D. A map $T\colon V\to V$ is called a semi-linear transformation if $T(u+v)=Tu+Tv$ for all $u,v\in V$ and there is an automorphism τ of D such that $T(v\alpha)=(Tv)\tau(\alpha)$ for all $v\in V$ and $\alpha\in D$.

Lemma 2.1 *Let σ be an automorphism of $\mathrm{End}(V_D)$. Assume that $\big[\sigma(x^m),x^n\big]_k=0$ for all $x\in\mathrm{End}(V_D)$, where m,n,k are fixed positive integers. If $\dim V_D\geq 2$, then σ is the identity map of $\mathrm{End}(V_D)$.*

Proof By [16, Isomorphism Theorem, p. 79], there exists an invertible semi-linear transformation $T\colon V\to V$ such that $\sigma(x)=TxT^{-1}$ for all $x\in\mathrm{End}(V_D)$. In particular, there exists an automorphism τ of D such that $T(v\alpha)=(Tv)\tau(\alpha)$ for all $v\in V$ and $\alpha\in D$. Hence by assumption, we have

$$0=\big[\sigma(x^m),x^n\big]_k=\big[Tx^mT^{-1},x^n\big]_k=\sum_{i=0}^{k}(-1)^i\binom{k}{i}x^{ni}(Tx^mT^{-1})x^{n(k-i)}$$

for all $x\in R$. We divide the proof into two cases.

Case 1 There exists $v_0\in V$ such that v_0 and $T^{-1}v_0$ are D-independent.

Suppose first that $v_0,T^{-1}v_0,T^{-2}v_0$ are D-independent. Let $x\in\mathrm{End}(V_D)$ such that $xv_0=0$, $xT^{-1}v_0=T^{-1}v_0+T^{-2}v_0$, and $xT^{-2}v_0=0$. Then $x^{\ell}T^{-1}v_0=T^{-1}v_0+T^{-2}v_0\neq 0$ for all $\ell\geq 1$, and hence

$$\begin{aligned}0=\big[\sigma(x^m),x^n\big]_k v_0&=\Big(\sum_{i=0}^{k}(-1)^i\binom{k}{i}x^{ni}(Tx^mT^{-1})x^{n(k-i)}\Big)v_0\\&=(-1)^kx^{nk}Tx^mT^{-1}v_0=(-1)^k(T^{-1}v_0+T^{-2}v_0),\end{aligned}$$

https://doi.org/10.4153/CMB-2011-185-5 Published online by Cambridge University Press

a contradiction.

Suppose next that $v_0, T^{-1}v_0, T^{-2}v_0$ are D-dependent. Then there exist $\alpha, \beta \in D$ such that $T^{-2}v_0 = v_0\alpha + (T^{-1}v_0)\beta$. In particular,

$$T^{-1}v_0 = T(T^{-2}v_0) = T\big(v_0\alpha + (T^{-1}v_0)\beta\big) = (Tv_0)\alpha_1 + v_0\beta_1,$$

where $\alpha_1 = \tau(\alpha)$ and $\beta_1 = \tau(\beta)$. Clearly, $\alpha_1 \neq 0$. Thus $Tv_0 = (T^{-1}v_0)\alpha_1^{-1} - v_0\beta_1\alpha_1^{-1}$. Let $x \in \mathrm{End}(V_D)$ such that $xv_0 = 0$ and $xT^{-1}v_0 = T^{-1}v_0 + v_0$. Then $x^\ell T^{-1}v_0 = T^{-1}v_0 + v_0$, $x^\ell Tv_0 = (T^{-1}v_0 + v_0)\alpha_1^{-1} \neq 0$ for all $\ell \geq 1$ and hence

$$\begin{aligned} 0 = \big[\sigma(x^m), x^n\big]_k v_0 &= \Big(\sum_{i=0}^{k}(-1)^i\binom{k}{i}x^{ni}(Tx^mT^{-1})x^{n(k-i)}\Big)v_0 \\ &= (-1)^k x^{nk}Tx^mT^{-1}v_0 = (-1)^k x^{nk}T(T^{-1}v_0 + v_0) = (-1)^k x^{nk}Tv_0, \end{aligned}$$

a contradiction.

Case 2 We have that v and $T^{-1}v$ are D-dependent for every $v \in V$. For each $v \in V$, we write $T^{-1}v = v\alpha_v$, where $\alpha_v \in D$. Fix $0 \neq u \in V$. Let $0 \neq v \in V$ and write $T^{-1}v = v\alpha_v$ where $\alpha_v \in D$. Suppose first that v and u are D-independent. Then

$$(u + v)\alpha_{u+v} = T^{-1}(u + v) = T^{-1}u + T^{-1}v = u\alpha_u + v\alpha_v.$$

So $u(\alpha_{u+v} - \alpha_u) = v(\alpha_v - \alpha_{u+v})$, and hence $\alpha_{u+v} = \alpha_u = \alpha_v$. Suppose next that v and u are D-dependent. Since $\dim V_D \geq 2$, there exists $w \in V$ such that w and u are D-independent, and then, by the proof above, we have $\alpha_w = \alpha_u$. Clearly, w and v are D-independent. So $\alpha_w = \alpha_v$, implying that $\alpha_u = \alpha_v$. Consequently, $T^{-1}v = v\alpha$ for all $v \in V$, where $\alpha = \alpha_u$. Now we have $\sigma(x)v = TxT^{-1}v = T(x(v\alpha)) = T((xv)\alpha) = xv$ for all $x \in \mathrm{End}(V_D)$ and $v \in V$. In particular, $(\sigma(x) - x)V = 0$ for all $x \in \mathrm{End}(V_D)$. Thus $\sigma(x) = x$ for all $x \in \mathrm{End}(V_D)$. This implies σ is the identity map of $\mathrm{End}(V_D)$, proving the lemma. ■

Throughout the rest in this section, R is always a prime ring with the maximal right ring of quotients $Q = Q_{mr}(R)$. Note that Q is also a prime ring, and the center C of Q, which is called the extended centroid of R, is a field. Moreover, $Z(R) \subseteq C$ (see [2] for details). It is well known that any automorphism of R can be uniquely extended to an automorphism of Q. An automorphism σ of R is called Q-inner if there exists an invertible element $g \in Q$ such that $\sigma(x) = gxg^{-1}$ for all $x \in R$. Otherwise, σ is called Q-outer. An automorphism σ of Q is called Frobenius if, in the case of $\mathrm{char}R = 0$, $\sigma(\alpha) = \alpha$ for all $\alpha \in C$ and if, in the case of $\mathrm{char}R = p \geq 2$, $\sigma(\alpha) = \alpha^{p^t}$ for all $\alpha \in C$, where t is a fixed integer, positive, zero, or negative.

Let $Q *_C C\{X\}$ be the free product of Q and the free algebra $C\{X\}$ over C on an infinite set X, of indeterminates. A typical element in $Q *_C C\{X\}$ is a finite sum of monomials of the form $\alpha a_{i_0}x_{j_1}a_{i_1}x_{j_2}\cdots x_{j_n}a_{i_n}$, where $\alpha \in C$, $a_{i_k} \in Q$, and $x_{j_k} \in X$. We say that R satisfies a nontrivial generalized polynomial identity (GPI) if there exists a nonzero polynomial $\phi(x_i) \in Q *_C C\{X\}$ such that $\phi(r_i) = 0$ for all $r_i \in R$.

Lemma 2.2 *Let R be a prime ring and let σ be a non-identity automorphism of R. If σ is Q-inner such that $\left[\sigma(x^m), x^n\right]_k = 0$ for all $x \in R$, where m, n, k are fixed positive integers, then R is commutative.*

Proof By assumption, $\sigma(x) = gxg^{-1}$ for all $x \in R$, where g is an invertible element in Q. Note that $g \notin C$; otherwise σ becomes the identity map of R, contrary to our assumption. Since $g \notin C$, it is easy to see that

$$\phi(x) = [\sigma(x^m), x^n]_k = gx^m g^{-1} x^{nk} + \sum_{i=1}^{k} (-1)^i \binom{k}{i} x^{ni} (gx^m g^{-1}) x^{n(k-i)}$$

is a nontrivial GPI of R. By [2, Theorem 6.4.4], R and Q satisfy the same GPIs. So we have $\phi(x) = 0$ for all $x \in Q$. Denote by F the algebraic closure of C if C is infinite and set $F = C$ for C finite. Then $Q \otimes_C F$ is a prime ring with the extended centroid F [12, Theorem 3.5]. Clearly, $Q \cong Q \otimes_C C \subseteq Q \otimes_C F$. So we may regard Q as a subring of $Q \otimes_C F$. By a standard argument [19, Proposition] (or see the proof of [17, Lemma 2]), $\phi(x)$ is also a nontrivial GPI of $Q \otimes_C F$. Let $\widetilde{Q} = Q_{mr}(Q \otimes_C F)$, the maximal right rings of quotients of $Q \otimes_C F$. By [2, Theorem 6.4.4], $\phi(x)$ is also a nontrivial GPI of $\widetilde{Q}$. By Martindale's theorem [28], $\widetilde{Q} \cong \mathrm{End}(V_D)$, where V is a vector space over a division ring D and D is finite-dimensional over its center F. Recall that F is either algebraically closed or finite. From the finite dimensionality of D over F, it follows that $D = F$. Hence $\widetilde{Q} \cong \mathrm{End}(V_F)$. By Lemma 2.1, $\dim V_F = 1$, implying $\widetilde{Q} = F$. Consequently, $\widetilde{Q}$ is commutative and hence R is commutative, as desired. ■

The following two lemmas are essential to our proof.

Lemma 2.3 ([5, p. 239, Theorem A7]) *Let R be a prime ring and $a_i, b_i, c_j, d_j \in Q$. Suppose that $\sum_{i=1}^{m} a_i x b_i + \sum_{j=1}^{n} c_j x d_j = 0$ for all $x \in R$. If $b_1, \dots, b_m$ are C-independent, then each a_i is a C-linear combination of $c_1, \dots, c_n$.*

Lemma 2.4 ([18, Theorem 2]) *Let R be a prime ring. If $a \in R$ such that $\left[a, x^n\right]_k = 0$ for all $x \in R$, where n, k are fixed positive integers, then $a \in Z(R)$.*

Theorem 2.5 *Let R be a prime ring and let σ be a non-identity automorphism of R. Suppose that $\left[[\cdots[[\sigma(x^{n_0}), x^{n_1}], x^{n_2}], \cdots], x^{n_k}\right] = 0$ for all $x \in R$, where $n_0, n_1, n_2, \dots, n_k$ are fixed positive integers. Then R is commutative.*

Proof Using the identities

$$\sum_{i=0}^{\ell} (x^t)^i [y, x^s] (x^t)^{\ell-i} = \left[\sum_{i=0}^{\ell} (x^t)^i y (x^t)^{\ell-i}, x^s\right],$$

$$\sum_{i=0}^{\ell-1} (x^t)^i [y, x^t] (x^t)^{\ell-1-i} = [y, x^{\ell t}]$$

and letting $m = n_0$ and $n = n_1 n_2 \cdots n_k$, by assumption we have

$$\left[\sigma(x^m), x^n\right]_k = 0 \qquad (2.1)$$

https://doi.org/10.4153/CMB-2011-185-5 Published online by Cambridge University Press

for all $x \in R$. If σ is Q-inner, then by Lemma 2.2, we are done. So from now on we assume that σ is Q-outer. In this case, $\phi(x) = [\sigma(x^m), x^n]_k = [\sigma(x)^m, x^n]_k$ is a nontrivial GPI of R with automorphisms. By [7, Main Theorem], R must satisfy a nontrivial GPI. By Martindale's theorem [28], $Q \cong \mathrm{End}(V_D)$, where V is a vector space over a division ring D and D is finite-dimensional over its center $C = Z(D)$. Since R and Q satisfy the same GPIs with automorphisms [8, Theorem 1], we have $\left[\sigma(x^m), x^n\right]_k = 0$ for all $x \in Q$. By Lemma 2.1, $\dim V_D = 1$ and hence $Q \cong D$. If C is finite, then from the finite dimensionality of D over C it follows that $D = C$. Thus $Q = C$ is a field, implying that R is commutative. Hence from now on we may assume that C is infinite. We divide the proof into two cases.

Case 1: σ is not Frobenius. By [8, Main Theorem], replacing $\sigma(x)$ with y, we obtain $\left[y, x^n\right]_k = 0$ for all $x, y \in R$. By Lemma 2.4, R is commutative, as desired.

Case 2: σ is Frobenius. If $\mathrm{char}\, R = 0$, then the Frobenius automorphism σ fixes C, that is, $\sigma(\alpha) = \alpha$ for all $\alpha \in C$. By Skolem–Noether theorem [23, Theorem 1.1], σ must be Q-inner, a contradiction. So we may assume that $\mathrm{char}\, R = p \geq 2$. Then there exists an integer t such that $\sigma(\alpha) = \alpha^{p^t}$ for all $\alpha \in C$. Clearly $t \neq 0$; otherwise, $\sigma(\alpha) = \alpha$ for all $\alpha \in C$. By [23, Theorem 1.1], σ is Q-inner, a contradiction. Choose an integer ℓ such that $p^\ell > k$. By (2.1) we have

$$0 = \left[[\sigma(x^m), x^n]_k, x^n\right]_{p^\ell - k} = [\sigma(x^m), x^n]_{p^\ell}$$
$$= \sum_{i=0}^{p^\ell} (-1)^i \binom{p^\ell}{i} x^{ni} \sigma(x^m) x^{n(p^\ell - i)} = \left[\sigma(x^m), x^{np^\ell}\right],$$

since $\binom{p^\ell}{i} = 0$ for $0 < i < p^\ell$. Let $s = np^\ell$. Then

$$0 = [\sigma(x^m), x^s] = [\sigma(x)^m, x^s] \quad \text{for all} \quad x \in Q. \tag{2.2}$$

Suppose first that $t \geq 1$. Let $x, y \in Q$ and $\alpha \in C$. Then

$$(x + \alpha y)^s = x^s + \sum_{i=1}^{s} \alpha^i \phi_i(x, y),$$

where $\phi_i(x, y)$ denotes the sum of all monic monomials with x-degree $s - i$ and y-degree i for $0 \leq i \leq s$. In particular,

$$\phi_1(x, y) = \sum_{i=0}^{s-1} x^{s-1-i} y x^i = x^{s-1} y + x^{s-2} y x + \cdots + y x^{s-1}.$$

For $\alpha \in C$ and $x, y \in Q$, replacing x by $x + \alpha y$ in (2.2) and using the identity

https://doi.org/10.4153/CMB-2011-185-5 Published online by Cambridge University Press

$[x, y+z] = [x, y] + [x, z]$, we have

$$\begin{aligned}
0 &= \big[\sigma(x+\alpha y)^m, (x+\alpha y)^s\big] = \big[(\sigma(x)+\sigma(\alpha)\sigma(y))^m, (x+\alpha y)^s\big] \\
&= \big[(\sigma(x)+\alpha^{p^t}\sigma(y))^m, (x+\alpha y)^s\big] \\
&= \Big[\sigma(x)^m + \sum_{j=1}^{m} \alpha^{jp^t}\varphi_j(\sigma(x),\sigma(y)), x^s + \sum_{i=1}^{s}\alpha^i\phi_i(x,y)\Big] \\
&= \alpha\big[\sigma(x)^m, \phi_1(x,y)\big] + \sum_{i=2}^{s}\alpha^i\big[\sigma(x)^m, \phi_i(x,y)\big] \\
&\quad + \sum_{j=1}^{m}\alpha^{jp^t}\big[\varphi_j(\sigma(x),\sigma(y)), x^s\big] + \sum_{j=1}^{m}\sum_{i=1}^{s}\alpha^{i+jp^t}\big[\varphi_j(\sigma(x),\sigma(y)), \phi_i(x,y)\big],
\end{aligned}$$

where $\varphi_j(x, y)$ denotes the sum of all monic monomials with x-degree $m-j$ and y-degree j for $0 \le j \le m$. Since C is infinite, it follows from the Vandermonde determinant argument that

$$\big[\sigma(x)^m, \phi_1(x,y)\big] = 0 \tag{2.3}$$

for all $x, y \in Q$. If $x^{ms} \in C$ for all $x \in Q$, then $[y, x^{ms}] = 0$ for all $x, y \in Q$, and hence Q is commutative by Lemma 2.4. This implies that R is commutative, proving the theorem. Thus we may assume that $x^{ms} \notin C$ for some $x \in Q$. Let $1 \le \ell \le s-1$ be the largest integer such that $1, x, \dots, x^\ell$ are C-independent and write $\phi_1(x, y) = \sum_{i=0}^{\ell} g_i(x)yx^i$, where $g_0(x), \dots, g_\ell(x)$ are C-linear combinations of $1, x, \dots, x^\ell$. Note that $g_w(x) \ne 0$ for some $0 \le w \le \ell$; otherwise, $\phi_1(x, y) = 0$ for all $y \in Q$ and then $0 = [x, \phi_1(x, y)] = [x^s, y]$ for all $y \in Q$, implying that $x^s \in C$ by Lemma 2.4 and hence $x^{ms} \in C$, a contradiction. By (2.3), we have

$$\begin{aligned}
0 &= \big[\sigma(x)^m, \phi_1(x,y)\big] = \sigma(x)^m\phi_1(x,y) - \phi_1(x,y)\sigma(x)^m \\
&= \sigma(x)^m\sum_{i=0}^{\ell} g_i(x)yx^i - \sum_{i=0}^{s-1} x^{s-1-i}yx^i\sigma(x)^m
\end{aligned} \tag{2.4}$$

for all $y \in Q$. Applying Lemma 2.3 to (2.4), $\sigma(x)^m g_w(x)$ can be expressed as a C-linear combination of $1, x, \dots, x^{s-1}$. Recall that $Q \cong D$ is a division ring and $g_w(x) \ne 0$. So $\sigma(x)^m$ is a C-linear combination of $g_w(x)^{-1}, g_w(x)^{-1}x, \dots, g_w(x)^{-1}x^{s-1}$. Hence $[\sigma(x)^m, x] = 0$. For any $z \in Q$, there exist infinite many $\beta \in C$ such that $(x+\beta z)^s \notin C$; otherwise, from $(x+\beta z)^s = x^s + \sum_{i=1}^{s}\beta^i\phi_i(x, z) \in C$, it follows that $x^s \in C$ by the Vandermonde determinant argument, a contradiction. For such $\beta \in C$, by the same proof as above, we obtain $[\sigma(x+\beta z)^m, x+\beta z] = 0$. Thus

$$\begin{aligned}
0 &= \big[\sigma(x+\beta z)^m, x+\beta z\big] = \big[(\sigma(x)+\beta^{p^t}\sigma(z))^m, x+\beta z\big] \\
&= \beta\big[\sigma(x)^m, z\big] + \sum_{j=1}^{m}\beta^{jp^t}\big[\varphi_j(\sigma(x),\sigma(z)), x+\beta z\big].
\end{aligned}$$

https://doi.org/10.4153/CMB-2011-185-5 Published online by Cambridge University Press

By the Vandermonde determinant argument again, $[\sigma(x)^m, z] = 0$ for all $z \in Q$. This implies that $\sigma(x)^m = \sigma(x^m) \in C$. Thus $x^m \in C$. In particular, $x^{ms} \in C$, a contradiction.

Suppose next that $t \leq -1$. By assumption $\sigma(\alpha) = \alpha^{p^t}$ for all $\alpha \in C$. Let $t' = -t \geq 1$. Then $\sigma(\alpha^{p^{t'}}) = \alpha$ and hence $\sigma^{-1}(\alpha) = \alpha^{p^{t'}}$ for all $\alpha \in C$. This implies that σ^{-1} is a Frobenius automorphism of R. By (2.2), $[\sigma^{-1}(x^s), x^m] = 0$ for all $x \in Q$. Proceeding in the same way as above, we obtain that R is commutative. The proof is now complete. ■

We are now ready to prove Theorem 1.2.

Proof of Theorem 1.2 Since a prime ring R and its nonzero ideal I satisfy the same GPIs with automorphisms [7, Theorem 1], we have $[[\cdots[\sigma(x^{n_0}), x^{n_1}], \cdots], x^{n_k}] = 0$ for all $x \in R$. By Theorem 2.5 we are done. ■

3 The Semiprime Case

Theorem 3.1 *Let R be a prime ring and let σ be an epimorphism of R but not a monomorphism. Suppose that $\big[[\cdots[[\sigma(x^{n_0}), x^{n_1}], x^{n_2}], \cdots], x^{n_k}\big] = 0$ for all $x \in R$, where $n_0, n_1, n_2, \ldots, n_k$ are fixed positive integers. Then R is commutative.*

Proof Let $I = \operatorname{Ker}\sigma$. Then I is a nonzero ideal of R. In view of the proof of Theorem 2.5, we have $[\sigma(x^m), x^n]_k = 0$ for all $x \in R$, where $m = n_0$ and $n = n_1 n_2 \cdots n_k$. For $x \in R$ and $y \in I$, $0 = [\sigma((x+y)^m), (x+y)^n]_k = [\sigma(x^m), (x+y)^n]_k$. Since I and R satisfy the same GPIs [2, Theorem 6.4.4], we have $[\sigma(x^m), (x+y)^n]_k = 0$ for all $x, y \in R$. Next replacing y with $y - x$, we obtain $[\sigma(x^m), y^n]_k = 0$ for all $x, y \in R$. Hence by Lemma 2.4 $\sigma(x^m) = \sigma(x)^m \in Z(R)$ for all $x \in R$. In particular, $x^m \in Z(R)$ for all $x \in R$. So $[y, x^m] = 0$ for all $x, y \in R$. By Lemma 2.4, R is commutative, proving the theorem. ■

We are now ready to prove Theorem 1.1

Proof of Theorem 1.1 In view of the proof of Theorem 2.5, we have $[\sigma(x^m), x^n]_k = 0$ for all $x \in R$, where $m = n_0$ and $n = n_1 n_2 \cdots n_k$. Let P be a prime ideal of R and set $\overline{R} = R/P$. For $x \in R$, we write $\overline{x} = x + P \in \overline{R}$.

Assume first that $\sigma(P) \nsubseteq P$. For $x \in R$ and $p \in P$,

$$\overline{0} = \overline{[\sigma((x+p)^m), (x+p)^n]_k} = [(\overline{\sigma(x)} + \overline{\sigma(p)})^m, \overline{x}^n]_k.$$

Thus $[(\overline{\sigma(x)} + \overline{y})^m, \overline{x}^n]_k = \overline{0}$ for all $x \in R$ and $y \in \sigma(P)$. Since $\sigma(P) \nsubseteq P$, $\overline{\sigma(P)} = \big(\sigma(P) + P\big)/P$ is a nonzero ideal of the prime ring $\overline{R}$. By [2, Theorem 6.4.4], $[(\overline{\sigma(x)} + \overline{y})^m, \overline{x}^n]_k = \overline{0}$ for all $x, y \in R$. Replacing y with $y - \sigma(x)$, we obtain $[\overline{y}^m, \overline{x}^n]_k = \overline{0}$ for all $x, y \in R$. This implies that $\overline{y}^m \in Z(\overline{R})$ for all $y \in R$ by Lemma 2.4. Hence $[\overline{x}, \overline{y}^m] = 0$ for all $x, y \in R$, implying that $\overline{R}$ is commutative by Lemma 2.4. So $[\overline{R}, \overline{R}] = \overline{0}$. Equivalently, $[R, R] \subseteq P$. In particular, $[\sigma(x) - x, y] \in P$ and $[(\sigma(x) - x)z, y] \in P$ for all $x, y, z \in R$.

Assume next that $\sigma(P) \subseteq P$. Define $\overline{\sigma}\colon \overline{R} \to \overline{R}$ by $\overline{\sigma}(\overline{x}) = \overline{\sigma(x)}$ for $x \in R$. Then $\overline{\sigma}$ is an epimorphism of $\overline{R}$. Then $\overline{0} = \overline{[\sigma(x^m), x^n]_k} = [\overline{\sigma}(\overline{x}^m), \overline{x}^n]_k$ for all $x \in R$.

https://doi.org/10.4153/CMB-2011-185-5 Published online by Cambridge University Press

By Theorems 3.1 and 2.5, $\overline{\sigma}$ is the identity automorphism of $\overline{R}$ or $\overline{R}$ is commutative. Hence $\sigma(x)-x \in P$ for all $x \in R$ or $[R,R] \subseteq P$. In both cases, we have $[\sigma(x)-x, y] \in P$ and $[(\sigma(x)-x)z, y] \in P$ for all $x, y, z \in R$.

Since R is semiprime, $\cap P = 0$, where P runs over all prime ideals of R. So we conclude that $[\sigma(x)-x, y] = 0$ and $[(\sigma(x)-x)z, y] = 0$ for all $x, y, z \in R$. Hence $\sigma(x)-x \in Z(R)$ and $(\sigma(x)-x)R \subseteq Z(R)$ for all $x \in R$. Let $\mu(x) = \sigma(x)-x$ for $x \in R$. Then $\mu(R) \subseteq Z(R)$ and $\mu(R)R \subseteq Z(R)$. So $\mu(R) + \mu(R)R$ is a central ideal of R. This proves the theorem. ■

Finally, we construct a noncommutative semiprime ring that admits a commuting non-identity automorphism.

Example Let F be a field, let $M_2(F)$ be the 2×2 matrix ring over F, and let $R = M_2(F) \times F \times F$. Let σ be the automorphism of R defined by $\sigma((x_1, x_2, x_3)) = (x_1, x_3, x_2)$ for $x_1 \in M_2(F)$ and $x_2, x_3 \in F$. Then $[\sigma(x), x] = 0$ and $\mu(x) = \sigma(x) - x$ for all $x \in R$, where $\mu((x_1, x_2, x_3)) = (0, x_3 - x_2, x_2 - x_3)$ for $x_1 \in M_2(F)$ and $x_2, x_3 \in F$. Clearly, $\mu(R)$ is contained in the central ideal $\{0\} \times F \times F$ of R.

Acknowledgement The authors are thankful to the referee for the very thorough reading of the paper and for valuable suggestions.

References

[1] E. Albas, N. Argac, and V. De Filippis, *Generalized derivations with Engel conditions on one-sided ideals.* Comm. Algebra **36**(2008), no. 6, 2063–2071. http://dx.doi.org/10.1080/00927870801949328

[2] K. I. Beidar, W. S. Martindale III, and A. V. Mikhalev, *Rings with generalized identities.* Monographs and Textbooks in Pure and Applied Mathematics, 196, Marcel Dekker, Inc., New York, 1996.

[3] H. E. Bell and W. S. Martindale III, *Centralizing mappings of semiprime rings.* Canad. Math. Bull. **30**(1987), no. 1, 92–101. http://dx.doi.org/10.4153/CMB-1987-014-x

[4] M. Brešar, *Centralizing mappings and derivations in prime rings.* J. Algebra **156**(1993), no. 2, 385–394. http://dx.doi.org/10.1006/jabr.1993.1080

[5] M. Brešar, M. A. Chebotar, and W. S. Martindale III, *Functional Identities. Frontiers in mathematics.* Birkhäuser Verlag, Basel, 2007.

[6] M.-C. Chou and C.-K. Liu, *An Engel condition with skew derivations.* Monatsh. Math. **158**(2009), 259-270. http://dx.doi.org/10.1007/s00605-008-0043-5

[7] C.-L. Chuang, *Differential identities with automorphisms and antiautomorphisms. I.* J. Algebra **149**(1992), no. 2, 371–404. http://dx.doi.org/10.1016/0021-8693(92)90023-F

[8] ———, *Differential identities with automorphisms and antiautomorphisms. II.* J. Algebra **160**(1993), no. 1, 130–171. http://dx.doi.org/10.1006/jabr.1993.1181

[9] C.-L. Chuang and C.-K. Liu, *Extended Jacobson density theorem for rings with skew derivations.* Comm. Algebra **35**(2007), no. 4, 1391–1413. http://dx.doi.org/10.1080/00927870601142207

[10] Q. Deng and H. E. Bell, *On derivations and commutativity in semiprime rings.* Comm. Algebra **23**(1995), no. 10, 3705–3713. http://dx.doi.org/10.1080/00927879508825427

[11] N. Divinsky, *On commuting automorphisms of rings.* Trans. Roy. Soc. Canada. Sect. III. **49**(1955), 19–22.

[12] T. S. Erickson, W. S. Martindale III, and J. M. Osborn, *Prime nonassociative algebras.* Pacific J. Math. **60**(1975), 49–63.

[13] V. De Filippis, *An Engel condition with generalized derivations on multilinear polynomials.* Israel J. Math. **162**(2007), 93–108. http://dx.doi.org/10.1007/s11856-007-0090-y

[14] ———, *Generalized derivations with Engel condition on multilinear polynomials*. Israel J. Math. **171**(2009), 325–348. http://dx.doi.org/10.1007/s11856-009-0052-7

[15] N. Jacobson, *Lie algebras.* Interscience Tracts in Pure and Applied Mathematics, 10, Interscience Publishers, New York, 1962.

https://doi.org/10.4153/CMB-2011-185-5 Published online by Cambridge University Press

[16] ______, *Structure of rings.* American Mathematical Society Colloquium Publications, 37, American Mathematical Society, Providence, RI, 1964.
[17] C. Lanski, *An Engel condition with derivation.* Proc. Amer. Math. Soc. **118**(1993), no. 3, 731–734. http://dx.doi.org/10.1090/S0002-9939-1993-1132851-9
[18] ______, *An Engel condition with derivation for left ideals.* Proc. Amer. Math. Soc. **125**(1997), no. 2, 339–345. http://dx.doi.org/10.1090/S0002-9939-97-03673-3
[19] P.-H. Lee and T.-L. Wong, *Derivations cocentralizing Lie ideals.* Bull. Inst. Math. Acad. Sinica **23**(1995), no. 1, 1–5.
[20] P.-H. Lee and Yu Wang, *Supercentralizing maps in prime superalgebras.* Comm. Algebra **37**(2009), 840–854. http://dx.doi.org/10.1080/00927870802271672
[21] T.-K. Lee, *Semiprime rings with hypercentral derivations.* Canad. Math. Bull. **38**(1995), no. 4, 445–449. http://dx.doi.org/10.4153/CMB-1995-065-2
[22] T.-K. Lee and T.-L. Wong, *On certain subgroups of prime rings with automorphisms.* Comm. Algebra **30**(2002), no. 10, 4997–5009. http://dx.doi.org/10.1081/AGB-120014681
[23] T.-K. Lee and K.-S. Liu, *The Skolem-Noether theorem for semiprime rings satisfying a strict identity.* Comm. Algebra **35**(2007), no. 6, 1949–1955. http://dx.doi.org/10.1080/00927870701247062
[24] T.-K. Lee and Y. Zhou, *An identity with generalized derivations.* J. Algebra Appl. **9**(2009), no. 3, 307–317. http://dx.doi.org/10.1142/S021949880900331X
[25] C.-K. Liu, *Derivations with Engel and annihilator conditions on multilinear polynomials.* Comm. Algebra **33**(2005), no. 3, 719–725. http://dx.doi.org/10.1081/AGB-200049880
[26] ______, *Derivations cocentralizing multilinear polynomials on left ideal.* Monatsh. Math. **162**(2011), no. 3, 297–311. http://dx.doi.org/10.1007/s00605-009-0179-y
[27] J. Luh, *A note on commuting automorphisms of rings.* Amer. Math. Monthly **77**(1970), 61–62. http://dx.doi.org/10.2307/2316858
[28] W. S. Martindale III, *Prime rings satisfying a generalized polynomial identity.* J. Algebra **12**(1969), 576–584. http://dx.doi.org/10.1016/0021-8693(69)90029-5
[29] J. H. Mayne, *Centralizing automorphisms of prime rings.* Canad. Math. Bull. **19**(1976), no. 1, 113–115. http://dx.doi.org/10.4153/CMB-1976-017-1
[30] ______, *Centralizing automorphisms of Lie ideals in prime rings.* Canad. Math. Bull. **35**(1992), no. 4, 510–514. http://dx.doi.org/10.4153/CMB-1992-067-0
[31] J. Vukman, *Commuting and centralizing mappings in prime rings.* Proc. Amer. Math. Soc. **109**(1990), no. 1, 47–52. http://dx.doi.org/10.1090/S0002-9939-1990-1007517-3
[32] Yu Wang, *A note on Lie automorphisms, subrings, and Lie ideals of prime rings.* Comm. Algebra **33**(2005), no. 11, 4057–4062. http://dx.doi.org/10.1080/00927870500261363
[33] ______, *Power-centralizing automorphisms of Lie ideals in prime rings.* Comm. Algebra **34**(2006), no. 2, 609–615. http://dx.doi.org/10.1080/00927870500387812
[34] ______, *Annihilator conditions of derivations on multilinear polynomial.* Comm. Algebra **39**(2011), no. 1, 237–246. http://dx.doi.org/10.1080/00927870903337992
[35] T.-L. Wong, *On Lie automorphisms, additive subgroups, and Lie ideals of prime rings.* Comm. Algebra **31**(2003), 969–979. http://dx.doi.org/10.1081/AGB-120017353

Department of Mathematics, National Changhua University of Education, Changhua 500, Taiwan
e-mail: d96211001@mail.ncue.edu.tw ckliu@cc.ncue.edu.tw