BULLETIN OF THE
INSTITUTE OF MATHEMATICS
ACADEMIA SINICA
Volume 18, Number 4, December 1990

POWERS OF SKEW AND SYMMETRIC ELEMENTS UNDER A DERIVATION

BY

TSIU-KWEN LEE (李秋坤)

Abstract. Let R be a prime ring with involution $*$ and d a nonzero derivation of R such that $d(x^n) \in Z$, the center of R, for all symmetric (skew resp.) elements x in R, where n is a fixed positive integer. Then R satisfies $S_4(x_1, x_2, x_3, x_4)$, the standard identity of degree 4.

0. Introduction and notation. Let R be an associative ring. By a derivation d on R we mean that d is an additive mapping of R into itself such that $d(xy) = xd(y) + d(x)y$ for all $x, y \in R$. In [5] Felzenszwalb showed that if R is a prime ring and d is a derivation of R such that $d(x^n) = 0$ for all $x \in R$, where n is a fixed positive integer, then either $d = 0$ or R is commutative. In [17], Misso gave a parallel result for the case when R is equipped with involution. Explicitly speaking, she proved:

Let R be a prime ring with involution $*$, char $R \neq 2, 3$, and d an inner derivation of R induced by a symmetric element. Suppose that $d(s^n) = 0$ for all symmetric elements $s \in R$, where n is a fixed positive integer. Then $d = 0$.

In this paper we shall handle both the symmetric and the skew case for general derivations. Recall that a ring R is called an S_n-ring if it satisfies $S_n(X_1, \dots, X_n) = \sum_{\sigma \in \mathrm{Sym}(n)} (-1)^\sigma X_{\sigma(1)} \cdots X_{\sigma(n)}$, the standard identity of degree n. Since the structure of prime S_4-rings is completely determined,

Received by the editors March 12, 1990 and in revised form October 26, 1990.

1980 Mathematics Subject Classifications (1985 Revision): Primary 16A72.

Key words and phrases: Prime rings, involutions, derivations, generalized polynomial identities, generalized $*$-identities.

removing the assumption on the characteristic of R we shall prove the following

Theorem. *Let R be a prime ring with involution $*$ and d a nonzero derivation of R such that $d(x^n) \in Z$, the center of R, for all symmetric (skew resp.) elements x in R, where n is a fixed positive integer. Then R is an S_4-ring.*

Throughout this paper, unless otherwise stated, R will always denote a prime ring with *involution* $*$ and center Z. S will stand for the set of symmetric elements of R and K for the set of skew elements of R. For two subsets A and B of R, $[A, B]$ will be the additive subgroup of R generated by all elements of the form $[a, b] = ab - ba$ with $a \in A$, $b \in B$. For convenience, a ring is called S_n-free if it does not satisfy $S_n(X_1, \ldots, X_n)$. Finally, for a derivation d of R, d^* is defined by $d^*(x) = d(x^*)^*$ for all $x \in R$. Notice that d^* is also a derivation. Also, d is called a $*$-derivation (skew $*$-derivation resp.) if $d^* = d$ ($d^* = -d$ resp.). We also remark that, for a derivation d of R, $d + d^*$ is a $*$-derivation and $d - d^*$ is then a skew $*$-derivation.

1. The symmetric case. We begin with

Theorem 1.1. *Let R be a prime S_4-free ring and d a derivation of R such that $d(s^n) = 0$ for all $s \in S$, where n is a fixed positive integer. Then $d = 0$.*

We shall proceed with a series of lemmas to complete the proof of the above theorem. Until the completion of this proof we assume that R always satisfies the assumptions stated in the above theorem. Also, by a simple observation it is sufficient to assume that d is either a $*$-derivation or a skew $*$-derivation.

Let C be the extended centroid of R and $T = RC + C$ the central closure of R. Then the involution $*$ can be extended to an involution, denoted also by $*$, on T satisfying $(\sum x_i\alpha_i + \beta)^* = \sum x_i^*\alpha_i^* + \beta^*$ for $x_i \in R$ and $\alpha_i, \beta \in C$ and d can be also extended in a natural way to a derivation, denoted also by d, on T such that $d(x\alpha) = xd(\alpha) + d(x)\alpha$ for all $x \in R$, $\alpha \in C$ [7; Lemma 2.4.1 and 5; Lemma 4]. We first prove

Lemma 1.1 *If $d \neq 0$, then T is a primitive ring with a minimal right ideal eT, where $e^2 = e$, and eTe is a finite dimensional central division algebra over C.*

Proof. Since $d(s^n) = 0$ for all $s \in S$, by a standard linearization process we have $d(\sum_{\sigma \in \mathrm{Sym}(n)} s_{\sigma(1)} s_{\sigma(2)} \cdots s_{\sigma(n)}) = 0$ for all $s_1, \ldots, s_n$ in S. Replacing s_i by s_i^n for $i = 2, \ldots, n$ and using the hypothesis, we yield

$$(1) \qquad \sum_{\sigma \in \mathrm{Sym}(n), \sigma(k)=1} s_{\sigma(1)}^n \cdots s_{\sigma(k-1)}^n d(s_{\sigma(k)}) s_{\sigma(k+1)}^n \cdots s_{\sigma(n)}^n = 0.$$

Suppose first that $d(S) \subseteq Z$. If char $R \neq 2$, then, by [8; Corollary, p.358], R is an S_4-ring, which is absurd. On the other hand, if char $R = 2$, then $s^8 \in Z$ for all $s \in S$ by [13; Lemma 4] and hence R also satisfies S_4 by [13; Theorem 3], a contradiction. Thus $d(S) \not\subseteq Z$.

Choose an element s_1 in S such that $d(s_1) \notin Z$. Let $X_2, \ldots, X_n$ be noncommuting indeterminates; then by (1)

$$f(X_2, \ldots, X_n; X_2^*, \ldots, X_n^*)$$
$$= \sum_{\sigma \in \mathrm{Sym}(n), \sigma(k)=1} (X_{\sigma(1)} X_{\sigma(1)}^*)^n \cdots (X_{\sigma(k-1)} X_{\sigma(k-1)}^*)^n d(s_{\sigma(k)}) \cdots (X_{\sigma(n)} X_{\sigma(n)}^*)^n$$

is a nontrivial $*$-GPI satisfied by R. Combining [4; Lemma 8] with the main result of [16], we have that $T = RC + C$ is a primitive ring with a minimal right ideal eT, where $e^2 = e \in T$, such that eTe is a finite dimensional central division algebra over C. This completes the proof.

We now dispose of the case when C is an infinite field.

Lemma 1.2. *If C is an infinite field, then $d = 0$.*

Proof. Assume on the contrary that $d \neq 0$. Let $C^+ = \{\alpha \in C | \alpha^* = \alpha\}$. Suppose first that $d(\alpha^n) \neq 0$ for some $\alpha \in C^+$. Choose a nonzero $*$-ideal I of R such that $\alpha I \subseteq R$. Let $s \in I \cap S$; then $d((\alpha s)^n) = 0$ and hence $0 = d(\alpha^n)s^n + \alpha^n d(s^n) = d(\alpha^n)s^n$. So $s^n = 0$ for all $s \in I \cap S$. If $n > 1$, then, for $s \in I \cap S$, $x \in R$, we get that $s^{n-1}x + x^* s^{n-1} \in I \cap S$ and hence $0 = x(s^{n-1}x + x^* s^{n-1})^n s^{n-1} = (xs^{n-1})^{n+1}$. By Levitzki's lemma, $s^{n-1} = 0$

for all $s \in I \cap S$. By induction on n, $I \cap S = 0$ follows; this implies that $x^2 = 0$ for all $x \in I$, which is absurd. Therefore $d(\alpha^n) = 0$ for all $\alpha \in C^+$.

Since C is an infinite field, so is C^+. Pick $n-1$ nonzero elements $\alpha_1, \ldots, \alpha_{n-1}$ in C^+ such that if $i \neq j$, then $\alpha_i^n \neq \alpha_j^n$. Choose a nonzero $*$-ideal U of R such that $\alpha_i^n U \subseteq R$ for all $i = 1, 2, \ldots, n-1$. Let $\delta(U) = \{x \in U | d^i(x) \in U$ for all $i \geq 1\}$. Since d is assumed to be either a $*$-derivation or a skew $*$-derivation, $\delta(U)$ is a $*$-ideal of R which is invariant under d. Moreover, by hypothesis, $s^n \in \delta(U)$ for all $s \in U \cap S$. Hence $\delta(U) \neq 0$.

Now $\delta(U)$ is a prime ring with involution $*$ and d is a nonzero derivation on $\delta(U)$, for otherwise $d = 0$ on R as desired. Let $s, t \in \delta(U) \cap S$, $\lambda \in \{\alpha_1^n, \alpha_2^n, \ldots, \alpha_{n-1}^n\}$; then $d((s+\lambda t)^n) = 0$. Expanding this and using $d(\lambda) = 0$, we yield

$$\lambda d\left(\left\{\begin{matrix} s & t \\ n-1 & 1 \end{matrix}\right\}\right) + \lambda^2 d\left(\left\{\begin{matrix} s & t \\ n-2 & 2 \end{matrix}\right\}\right) + \cdots + \lambda^{n-1} d\left(\left\{\begin{matrix} s & t \\ 1 & n-1 \end{matrix}\right\}\right) = 0,$$

where $\left\{\begin{matrix} s & t \\ n-r & r \end{matrix}\right\}$ is the sum of terms with $\deg(s) = n-r$, $\deg(t) = r$ in the expansion of $(s+t)^n$. Since $\alpha_i^n \neq \alpha_j^n$ if $i \neq j$, $d\left(\left\{\begin{matrix} s & t \\ n-r & r \end{matrix}\right\}\right) = 0$ for every r. In particular, $d\left(\left\{\begin{matrix} s & t \\ n-1 & 1 \end{matrix}\right\}\right) = 0$. Suppose first that $d(s) = 0$. Then

$$[d(t), s^n] = d([t, s^n]) = d\left(\left[\left\{\begin{matrix} s & t \\ n-1 & 1 \end{matrix}\right\}, s\right]\right) = 0$$

for all $t \in \delta(U) \cap S$. By [14; Theorem 1] for char $R \neq 2$ and [13; Lemma 4] for char $R = 2$, $s^{8n} \in Z(\delta(U)) \subseteq Z$, where $Z(\delta(U))$ denotes the center of $\delta(U)$.

Now for any $s \in U \cap S$, then $s^n \in \delta(U)$ and by hypothesis $d(s^n) = 0$. Thus the above implies $s^{8n^2} \in Z$. So U is an S_4-ring and hence so is R, a contradiction. This completes the proof.

With Lemma 1.2 in hand we shall reduce our problem to the case when $R = M_m(F)$, the m by m matrix ring over a finite field F. To arrive at this aim we need another lemma. Recall that a projection is a symmetric idempotent element.

Lemma 1.3. *Let F be a field and $*$ an involution on $M_m(F)$. Then, if $m \geq 3$, $M_m(F)$ is generated by projections as an algebra over F.*

Proof. As in [12], let $E^*(M_m(F))$ be the subspace of $M_m(F)$ spanned by all projections of $M_m(F)$ over F. Denote by $A^*(M_m(F))$ the subalgebra of $M_m(F)$ generated by all projections of $M_m(F)$ over F. Of course, $E^*(M_m(F)) \subseteq A^*(M_m(F))$ holds always. If $*$ is of the second kind, then, by [12; Theorem 1], $E^*(M_m(F)) = M_m(F)$ and hence $A^*(M_m(F)) = M_m(F)$.

Assume from now on that $*$ is of the first kind. Our argument will depend on the type of the involution $*$. Note that, by a simple observation as in [12; Lemma 1], if $A^*(M_k(F)) = M_k(F)$ for some $k \geq 2$, then $A^*(M_n(F)) = M_n(F)$ for all $n \geq k$. Thus for the equality $A^*(M_m(F)) = M_m(F)$ to be true, it is sufficient that the equality $A^*(M_k(F)) = M_k(F)$ hold only for some $k \leq m$, such as $k = 2$ or 3.

Case 1. *Suppose that $*$ is of the transpose type.*

Since $*$ is of the first kind, we may assume, without loss of generality, that $*$ is given by

$$(\alpha_{ij})^* = (\pi_i^{-1}\delta_{ij})(\alpha_{ji})(\pi_i\delta_{ij}),$$

where $\pi_1, \ldots, \pi_m$ are m fixed nonzero elements in F, $\delta_{ij} = 1$ if $i = j$ and 0 otherwise.

Assume $|F| > 3$. In this case we claim that $A^*(M_2(F)) = M_2(F)$. The involution $*$ is now given by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & \pi^{-1}\gamma \\ \pi\beta & \delta \end{pmatrix}, \quad \text{where } \pi = \pi_1\pi_2^{-1}.$$

Choose an element $0 \neq \mu \in F$ such that $\mu^2 \neq -\pi$. Then $A^*(M_2(F))$ contains the following projections

$$e_{11}, \quad e_{22}, \quad \text{and} \quad \frac{1}{\pi + \mu^2}\begin{pmatrix} \mu^2 & \mu \\ \pi\mu & \pi \end{pmatrix}$$

Since $A^*(M_2(F))$ is a subalgebra of $M_2(F)$, $A^*(M_2(F)) = M_2(F)$ follows and hence $A^*(M_m(F)) = M_m(F)$ for all $m \geq 3$.

Assume $|F| = 2$. In this case $*$ is just the usual matrix transpose and note that $A^*(M_2(F)) \neq M_2(F)$. So we have to check the equality $A^*(M_3(F)) = M_3(F)$. An elementary calculation gives the following four projections in $A^*(M_3(F))$, that is

$$e_{11}, \quad e_{22}, \quad e_{33} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

From these, it is easy to check that $e_{ij} \in A^*(M_3(F))$ for all $i, j, 1 \leq i, j \leq 3$ and hence $A^*(M_3(F)) = M_3(F)$.

Finally assume $|F| = 3$. We claim that $A^*(M_3(F)) = M_3(F)$. Note that whether this equality holds is independent of the permutation on the π_i's and furthermore (π_1, π_2, π_3) and $(-\pi_1, -\pi_2, -\pi_3)$ induce the same involution. Thus it suffices to check only for $(\pi_1, \pi_2, \pi_3) = (1,1,1)$ or $(1,1,2)$. For $(\pi_1, \pi_2, \pi_3) = (1,1,1)$, $A^*(M_3(F))$ contains the following projections:

$$e_{11}, \quad e_{22}, \quad e_{33}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

But if $(\pi_1, \pi_2, \pi_3) = (1,1,2)$, $A^*(M_3(F))$ contains the following projections:

$$e_{11}, \quad e_{22}, \quad e_{33}, \quad \text{and} \quad \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{pmatrix}.$$

In either case, it is easy to check that the equality $A^*(M_3(F)) = M_3(F)$ holds.

Case 2. *Suppose that $*$ is of the symplectic type.*

In this case m must be even and the involution $*$ is given by $(A_{ij})^* = (A_{ji}^{\sigma})$, where the A_{ij} are 2 by 2 matrices and σ is the mapping

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \longmapsto \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}.$$

It suffices to prove the equality $A^*(M_4(F)) = M_4(F)$. An elementary calculation gives the following projections in $A^*(M_4(F))$:

$$e_{11} + e_{22}, \quad e_{33} + e_{44}, \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & \omega \\ \omega & -1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & \omega & 0 \\ 0 & 0 & 1 & 0 \\ -\omega & 1 & 0 & 1 \end{pmatrix},$$

where $\omega \in F$. Hence $A^*(M_4(F)) = M_4(F)$, which completes the proof.

With the lemma above, we are in a position to give the proof of Theorem 1.1. We first make a well-known

Remark. Let D be a division ring with involution and V a left vector space over D. Suppose that $(\, , \,)$ is a non-degenerate Hermitian or alternate form on the self-dual space V over D. Then every finite-dimensional subspace of V is contained in some finite-dimensional non-degenerate subspace of V.

Proof of Theorem 1.1. Assume on the contrary that $d \neq 0$. By Lemma 1.1, T is a primitive ring with a minimal right ideal eT, where $e^2 = e$, and eTe is a finite dimensional central division algebra over C. From Lemma 1.2, we may assume that C is a finite field. Thus $eTe = Ce$. Suppose first that $\dim_{eTe} eT = k < \infty$. Then the density theorem implies $T = M_k(eTe)$. From [7; Theorem 1.4.3] R is an order in T; furthermore, C is exactly the quotient field of Z. Since C is a finite field, $Z = C$ follows and hence $R = T = M_k(C)$. Note that $d(C) = 0$. Also, by hypothesis, $d(f) = 0$ for every projection $f \in R$. Thus $d(A^*(M_k(C))) = 0$. Since R is S_4-free, $k \geq 3$ and hence applying Lemma 1.3 we get $d(R) = 0$. Thus $d = 0$ for the case when $\dim_{eTe} eT < \infty$.

Assume, henceforth, that $\dim_{eTe} eT = \infty$. From [7; Theorem 1.2.2], for some suitable choice of eT, T becomes a ring of linear transformations on the left vector space $V = eT$ over $\Delta = eTe$; furthermore, V can be equipped with a non-alternate Hermitian or an alternate form, denoted by $(\, , \,)$, such that the elements of T are continuous with respect to this form $(\, , \,)$; T contains all continuous linear transformations of finite rank and the $*$ of T (extended from that on R) is just the adjoint relative to this form. Denote by $S_V(V)$ the set of all elements of finite rank in T. Note that $S_V(V)$ is just the socle of T. Then $R \cap S_V(V) \neq 0$. Thus, to get $d = 0$, it suffices to show that $d(R \cap S_V(V)) = 0$.

Let $r \in R \cap S_V(V)$; then $r^* \in R \cap S_V(V)$ also. Suppose that this form $(\, , \,)$ is both Hermitian and non-alternate. By the above remark, there exists a finite dimensional non-degenerate subspace W of V containing both Vr and Vr^* such that $\dim_\Delta W \geq 3$ and W is also Hermitian, non-alternate relative to this form $(\, , \,)$. Let $W^\perp$ denote the orthogonal complement of W; then $V = W \oplus W^\perp$ and $\{x \in S_V(V) | Wx \subseteq W \text{ and } W^\perp x = 0\} \cong M_m(\Delta)$, where $m = \dim_\Delta W \geq 3$, is a $*$-invariant subring contained in T. Since Δ is a finite field, by [18; Theorem 1] we get that $M_m(\Delta) \subseteq R$ and the adjoint is an involution on $M_m(\Delta)$ which is of the transpose type. Note that $Wr \subseteq Vr \subseteq W$. Also, for any $v \in V$, $z \in W^\perp$ we have $(v, zr) = (vr^*, z) \in (W, W^\perp) = 0$. Thus $(V, W^\perp r) = 0$ and hence $W^\perp r = 0$. So $r \in M_m(\Delta)$. But $d(\Delta) = 0$ and $d(f) = 0$ for every projection $f \in M_m(\Delta)$, Lemma 1.3 implies $d(M_m(\Delta)) = 0$. In particular, $d(r) = 0$. That is, $d(R \cap S_V(V)) = 0$ and hence $d = 0$, which is absurd. Of course, a similar argument can be applied to the alternate case. This completes the proof.

As a consequence of Theorem 1.1, we give a slight generalization.

Theorem 1.2. *Let R be a prime S_4-free ring, d a derivation of R, and I a nonzero ideal of R. Suppose that $d(s^n) \in Z$ for all $s \in I \cap S$, where n is a fixed positive integer. Then $d = 0$.*

Proof. As in the course of the proof of Theorem 1.1, we may assume that d is either a $*$-derivation or a skew $*$-derivation. Replacing I by $I \cap I^* \neq 0$, we may assume that I is a nonzero $*$-ideal of R. Suppose that there exists $\alpha \in Z \cap S$ such that $d(\alpha^n) \neq 0$. Then, for $s \in I \cap S$, we have $\alpha s \in I \cap S$ and hence $d((\alpha s)^n) = \alpha^n d(s^n) + d(\alpha^n)s^n \in Z$. Thus $s^n \in Z$ for all $s \in I \cap S$. From [13; Theorem 3], I is an S_4-ring and hence so is R. This is a contradiction. In other words, $d(\alpha^n) = 0$ for all $\alpha \in Z \cap S$. Let $s \in I \cap S$. Then $d(s^{2n}) = 2s^n d(s^n) \in Z$. If char $R = 2$, then $d(s^{2n}) = 0$; while if char $R \neq 2$, then either $d(s^n) = 0$ or $s^n \in Z$. However, if $s^n \in Z$, then $d(s^{n^2}) = 0$. At any rate, $d(s^{n^2}) = 0$ for all $s \in I \cap S$ in case char $R \neq 2$.

Thus in either case this problem can be reduced to assuming that $d(s^k) = 0$ for all $s \in I \cap S$, where k is a fixed positive integer. As in the proof of Lemma 1.2, we may define $\delta(I)$, which is a nonzero $*$-ideal of R invariant under d such that $d(s^k) = 0$ for all $s \in \delta(I) \cap S$. Applying

Theorem 1.1, we get $d(\delta(I)) = 0$ and hence $d = 0$.

Recall that a ring R is called a $*$-prime ring if the product of any two nonzero $*$-ideals of R is nonzero; equivalently, there exists a prime ideal P of R such that $P \cap P^* = 0$. We conclude this section by extending Theorem 1.1 to the $*$-prime case.

Theorem 1.3. *Let R be a $*$-prime S_4-free ring and d a derivation of R such that $d(s^n) \in Z$ for all $s \in S$, where n is a fixed positive integer. Then $d = 0$.*

Proof. By Theorem 1.2, we assume that R is not a prime ring. Thus there exists a nonzero prime ideal P of R such that $P \cap P^* = 0$. Applying d to $PP^* = 0$, we get $d(P)P^* \subseteq P$. Since $P^* \not\subseteq P$ and P is a prime ideal of R, we get $d(P) \subseteq P$. Similarly, $d(P^*) \subseteq P^*$. Thus, if $d(R) \not\subseteq P$, d induces a nonzero derivation $\overline{d}$ on $\overline{R} = R/P$ by $\overline{d}(\overline{x}) = \overline{d(x)}$ for all $x \in R$, where $\overline{x}$ denotes the image of x in $\overline{R}$. Let $y \in P^*$. Then $\overline{y} = \overline{y + y^*} \in P{+}P^*/P = \overline{P^*}$, a nonzero ideal of $\overline{R}$. Thus $\overline{d}(\overline{y}^n) = \overline{d((y + y^*)^n)} \in Z(\overline{R})$ by hypothesis. By [5; Theorem 4] and the proof of Theorem 1.2 these imply that $\overline{R}$ is commutative. Since R/P^* is anti-isomorphic to R/P and R is a subdirect product of R/P and R/P^*, R must be commutative. Of course, R is an S_4-ring, a contradiction. Therefore we have seen $d(R) \subseteq P$. Similarly $d(R) \subseteq P^*$. So $d(R) = 0$ as desired.

2. The skew case. To handle the skew case we first need a result about rings with power-central skew elements of bounded index. That is

Lemma 2.1. *Let n be a fixed positive integer such that $k^n \in Z$ for all $k \in K$. Then R is an S_4-ring.*

Proof. If $Z = 0$, then $k^n = 0$ for all $k \in K$, which leads to $K = 0$ and so R is commutative. Thus assume $Z \neq 0$ and hence $Z^+ = Z \cap S \neq 0$. Localize R at $Z^+ - \{0\}$ to obtain a simple ring R_{Z^+}, which has an involution, denoted by $*$ also, defined by $(x\alpha^{-1})^* = x^*\alpha^{-1}$, for $x \in R$, $\alpha \in Z^+ - \{0\}$. Thus R_{Z^+} also has power-central skew elements with the same bounded index n.

In light of [10; Theorem 10] R_{Z^+} satisfies S_4 and, a fortiori, R satisfies S_4 too. This completes the proof.

The main result in this section is the following

Theorem 2.1. *Let R be a prime S_4-free ring and d a derivation of R such that $d(k^n) = 0$ for all $k \in K$, where n is a fixed positive integer. Then $d = 0$.*

We first dispose of the case when R is not a PI-ring.

Lemma 2.2. *Under the assumptions of Theorem 2.1, if R is not a PI-ring, then $d = 0$.*

Proof. If char $R = 2$, K coincides with S and hence it is just Theorem 1.1. So we assume from now on that char $R \neq 2$. Also, n may be assumed to be even. Let A be the additive subgroup of R generated by the set $\{p(k_1, \dots, k_n) | k_i \in K, 1 \leq i \leq n\}$, where $p(x_1, \dots, x_n) = \sum_{\sigma \in \mathrm{Sym}(n)} x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}$. Since n is even, we have that both $A^* = A$ and $A \subseteq S$. Moreover, if $k, k_1, \dots, k_n \in K$, then $[k, p(k_1, \dots, k_n)] = \sum_{i=1}^{n} p(k_1, \dots, [k, k_i], \dots, k_n) \in A$. That is, $[A, K] \subseteq A$. Since R is not a PI-ring, it follows from [1; Theorem 1] that $A \not\subseteq Z$. Hence by [9; Theorem 1] there exists a nonzero $*$-ideal I of R such that $[I \cap S, K] + [S, I \cap K] \subseteq A$. Note that $d(A) = 0$, because $p(x_1, \dots, x_n)$ is obtained from the polynomial x^n by a series of standard linearization processes. So $d([I \cap S, K]) = 0 = d([S, I \cap K])$.

Let $k \in I \cap K$, $l \in I^2 \cap K$, and $s \in I \cap S$; then $[k, s] \in I \cap S$. Hence $d([[k, s], l]) = 0$. Expanding it and using $d([k, s]) = 0$, we get $[d(l), [k, s]] = 0$ and hence $[d(l)^*, [k, s]] = 0$. These imply that $[d(l) \pm d(l)^*, [k, s]] = 0$. Note that $d(l) \in I$ and that I is not a PI-ring; it follows from [14; Theorem 1] and [15; Main Theorem] that $d(l) \pm d(l)^* \in Z$ for all $l \in I^2 \cap K$. So $d(I^2 \cap K) \subseteq Z$, which implies that either I^2 is an S_4-ring or $d = 0$. But I^2 is not a PI-ring, $d = 0$ follows.

Having handled the non-PI case, we next turn our attention to the case when R is a PI-ring. For this purpose we need one more lemma.

Lemma 2.3. *Let F be a field with $|F| = 3$ or 5 and $*$ an involution on $M_m(F)$, where $m \geq 3$. If $a \in M_m(F)$, $[a, k^n] = 0$ for all $k \in K$, where n is a fixed positive integer, then $a \in F$.*

Proof. **Case 1.** *Assume that $*$ is of the symmetric type.*

Let W be the subalgebra of $M_m(F)$ over F generated by all k^n, where $k \in K$. Then $uWu^{-1} \subseteq W$ for every unitary element u in $M_m(F)$ (that is, $u^*u = 1 = uu^*$). Note that in this case $K = K_1 + [K_1, K_1]$, where K_1 is the additive subgroup of K generated by skew elements of square zero. Therefore $[K, W] \subset W$ [3;p.555]. It follows from [11; Theorem 5] and Lemma 2.1 that $W = M_m(F)$. Since $[a, W] = 0$, we get $a \in F$.

Case 2. *Assume that $*$ is of the transpose type.*

Since $|F| = 3$ or 5, $*$ is given by $(\alpha_{ij})^* = p(\alpha_{ji})p^{-1}$, where $p = \operatorname{diag}\{\pi_1, \ldots, \pi_m\}$, $\pi_i \neq 0$ for each i. Let $Y = \{x \in M_m(F) | [x, k^n] = 0$ for all $k \in K\}$. Since $e_{ij} - \pi_j\pi_i^{-1}e_{ji} \in K$ if $i \neq j$, by the fact that $(e_{ij} - \pi_j\pi_i^{-1}e_{ji})^2 = -\pi_j\pi_i^{-1}(e_{ii} + e_{jj})$ we have that every element in Y assumes a diagonal form. So to prove the fact that $Y \subseteq F$, it suffices to consider only the case $m = 3$. In this situation, every skew element assumes the form

$$\begin{pmatrix} 0 & x & y \\ -\alpha x & 0 & z \\ -\beta y & -\gamma z & 0 \end{pmatrix},$$

where $\alpha = \pi_2\pi_1^{-1}$, $\beta = \pi_3\pi_2^{-1}$ and $\gamma = \alpha^{-1}\beta$. Also, if

$$k = \begin{pmatrix} 0 & x & y \\ -\alpha x & 0 & z \\ -\beta y & -\gamma z & 0 \end{pmatrix},$$

then $k^3 = \lambda k$, where $\lambda = -(\alpha x^2 + \beta y^2 + \gamma z^2)$. Thus $k^{2l} = \lambda^{l-1}k^2$ and $k^{2l+1} = \lambda^l k$ for every positive integer l. Since $|F| = 3$ or 5, it is not hard to check the fact that $Y \subseteq F$. We omit its detail.

Now we set about proving Theorem 2.1.

Proof of Theorem 2.1. Assume on the contrary that $d \neq 0$. From Theorem 1.1 and Lemma 2.2 we may assume that R is a prime PI-ring with char $R \neq 2$. Thus $Z \neq 0$. Suppose first that $*$ is of the second kind. Pick a $\lambda \in Z$ such that $\lambda^* = -\lambda \neq 0$. Thus for $s \in S$, we have that $d((\lambda s)^n) = 0 = d(\lambda^n)$. Therefore $d(s^n) = 0$ for every $s \in S$. Theorem 1.1 implies $d = 0$. So assume, henceforth, that $*$ is of the first kind.

For $\lambda \in Z$, $k \in K$, we have that $\lambda k \in K$ and hence $d(\lambda^n k^n) = 0$ Thus $d(\lambda^n)k^n = 0$. By Lemma 2.1, pick a skew element k such that $k^n \neq 0$. So $d(\lambda^n) = 0$ for all $\lambda \in Z$. Consider R_Z, the localization of R at $Z - \{0\}$. R_Z is then a finite-dimensional simple algebra with an involution, denoted by $*$ also, defined by $(x\alpha^{-1})^* = x^*\alpha^{-1}$ for $x \in R$, $\alpha \in Z - \{0\}$. Moreover, d can be uniquely extended to R_Z. Since $d(\lambda^n) = 0$ for all $\lambda \in Z$, R_Z satisfies the same assumption. In other words, R may be assumed to be a finite-dimensional central simple algebra. Since $d(k^{2n}) = 0$ for all $k \in K$, we assume that n is even.

Case 1. Suppose that $d(Z) = 0$. By a classical result [6; Proposition, p.100], d is an inner derivation of R. Write $R = M_m(D)$ for some division algebra D and some positive integer m. Denote by W the subalgebra over Z of R generated by all k^n, where $k \in K$. Note that $d(W) = 0$. In case $m = 1$, by [2; Theorem 3] $W = R$ and hence $d = 0$. If $|D| \leq 5$, then D is a field and $m \geq 3$, since R is S_4-free. It follows from Lemma 2.3 that $d = 0$. Finally, assume both $m > 1$ and $|D| > 5$. If the involution $*$ is of the symplectic type, by [11; Theorem 5] the only unitary invariant subalgebra of R are 0, Z and R. By Lemma 2.1 we have $W = R$ and so $d = 0$. Assume next that $*$ is of the transpose type. If $m \geq 3$, by [11; Main Theorem] and Lemma 2.1 again we have $W = R$. Suppose now that $m = 2$. In this situation, we may assume that

$$\text{for } \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in R, \quad \begin{pmatrix} x & y \\ z & t \end{pmatrix}^* = \begin{pmatrix} \bar{x} & \bar{z}q^{-1} \\ q\bar{y} & q\bar{t}q^{-1} \end{pmatrix},$$

where $^-$ is the induced first kind involution on D and $\bar{q} = q \neq 0$ in D. From [11; Main Theorem] we have $W = R$ unless R is one of the only possible two cases given as follows:

$$\text{(i) } W = \left\{ \begin{pmatrix} x & y \\ -qy & x \end{pmatrix} \middle| x \in Z + K_1, y \in \mathring{S}_1 \right\},$$

where $\dim_Z D = 4$, $K_1 = \{x \in D|\overline{x} = -x\}$ 1-dimensional, $\overset{\circ}{S_1} = \{x \in D|xk + kx = 0 \text{ for all } k \in K_1\}$ and q is a fixed nonzero central element.

$$\text{(ii) } W = \left\{ \begin{pmatrix} u & v \\ -q\overline{v} & \dot{u} \end{pmatrix} \middle| u \in Z + K_1, v \in (Z + K_1)(a - b) \right\},$$

where $\dim_Z D = 4$, $K_1 = \{x \in D|\overline{x} = -x\}$, $[K_1, K_1] = 0$ and $0 \neq a \in K_1$, $0 \neq b \in K_2 = \{x \in D|q\overline{x}q^{-1} = -x\}$ such that $u = \alpha + \beta a \mapsto \dot{u} = \alpha + \beta b$ is an isomorphism of $Z + K_1$ onto $Z + K_2$.

By a simple observation, in the above cases (i) and (ii) $W \cap S \subseteq Z$ always holds. In particular, $k^n \in W \cap S \subseteq Z$, for all $k \in K$. Thus Lemma 2.1 implies that R is an S_4-ring, contrary to our hypothesis. So (i) or (ii) cannot occur, which completes the proof of Case 1.

Case 2. Suppose that $d(Z) \neq 0$. So Z must be an infinite field. For any unitary element $u \in R$ and $k \in K$, we have $uku^{-1} \in K$ and hence $d(k^n) = 0 = d(uk^nu^{-1})$. Since $d(u^{-1}) = -u^{-1}d(u)u^{-1}$, expanding $d(uk^nu^{-1}) = 0$ we get $[u^{-1}d(u), k^n] = 0$. By Case 1, $u^{-1}d(u) \in Z$ follows. For any $k \in K$, by Z being infinite and $\dim_Z R < \infty$, there exists an element $\alpha \in Z - \{0\}$ such that $1 + \alpha k$ is invertible in R. Thus $(1 - \alpha k)(1 + \alpha k)^{-1}$ is a unitary element and so $(1 + \alpha k)(1 - \alpha k)^{-1}d((1 - \alpha k)(1 + \alpha k)^{-1}) \in Z$. An elementary calculation shows that $[k, d(k)] = 0$. Up to now we have proved that $[k, d(k)] = 0$ for all $k \in K$. By [13; Theorem 2] we yield $d = 0$ since R is S_4-free, which completes the proof of Theorem 2.1.

As in the proof given in Section 1, we can extend Theorem 2.1 to the central case and the $*$-prime case. The argument is almost the same as those of Section 1. Thus we only give these statements.

Theorem 2.2. *Let R be a prime S_4-free ring, d a derivation of R and I a nonzero ideal of R. Suppose that $d(k^n) \in Z$ for all $k \in K \cap I$, where n is a fixed positive integer. Then $d = 0$.*

Theorem 2.3. *Let R be a $*$-prime S_4-free ring and d a derivation of R such that $d(k^n) \in Z$ for all $k \in K$, where n is a fixed positive integer. Then $d = 0$.*

References

1. S. A. Amitsur, *Indentities in rings with involution*, Israel J. Math., **7**(1969), 63–68.

2. M. Chacron and I. N. Herstein, *Powers of skew and symmetric elements*, Houston J. Math., **1**(1975), 15–27.

3. M. Chacron, *Unitaries in simple Artinian rings*, Canad. J. Math., **31**(1979), 542–557.

4. C. L. Chuang, **-differential identities of prime rings with involution*, Trans. A.M.S., **316**(1989), 251–279.

5. B. Felzenszwalb, *Derivations in prime rings*, Proc. A.M.S., **84**(1982), 16–20.

6. I. N. Herstein, *Noncommutative Rings*, Carus Monograph, **15**(1968).

7. I. N. Herstein, *Rings with Involution*, Univ. of Chicago Press, Chicago (1976).

8. I. N. Herstein, *A theorem on derivations of prime rings with involution*, Canad. J. Math., **34**(1982), 356–369.

9. C. Lanski, *Invariant submodules in semiprime rings with involution*, Comm. in Algebra, **6**(1978), 75–96.

10. P. H. Lee, *Power-central traces and skew traces*, Bull. Inst. Math. Acad. Sinica, **3**(1975), 171–176.

11. P. H. Lee, *On unitary invariant subalgebra*, Chinese J. Math., **17**(1989), 87–108.

12. P. H. Lee and T. K. Lee, *Projections in simple Artinian rings*, Chinese J. Math., **13**(1985), 15–21.

13. P. H. Lee and T. K. Lee, *Derivations centralizing symmetric or skew elements*, Bull. Inst. Math. Acad. Sinica, **14**(1986), 249–256.

14. T. K. Lee, *On derivations of prime rings with involution* (I), Chinese J. Math., **13**(1985), 179–186.

15. T. K. Lee, *On derivations of prime rings with involution* (II), Bull. Inst. Math. Acad. Sinica, **14**(1986), 365–375.

16. W. Martindale, *Prime rings satisfying a generalized polynomial identity*, J. Algebra, **12**(1969), 576–584.

17. P. Misso, *Commutativity conditions on rings with involution*, Canad. J. Math., **34**(1982), 17–22.

18. S. Montgomery, *A structure theorem and a positive definiteness condition in rings with involution*, J. Algebra, **34**(1976), 181–192.

19. L. Rowen, *Polynomial Identities in Ring Theory*, Academic Press, New York/ London (1980).

Department of Mathematics, National Taiwan University, Taipei, Taiwan 10764, R.O.C.