Can. J. Math. Vol. **43** (5), 1991 pp. 1045–1054

NILPOTENT INNER DERIVATIONS OF THE SKEW ELEMENTS OF PRIME RINGS WITH INVOLUTION

W. S. MARTINDALE, 3RD AND C. ROBERT MIERS

ABSTRACT. Let R be a prime ring with invoution *, of characteristic 0, with skew elements K and extended centroid C. Let $a \in K$ be such that $(\operatorname{ad} a)^n = 0$ on K. It is shown that one of the following possibilities holds: (a) R is an order in a 4-dimensional central simple algebra, (b) there is a skew element λ in C such that $(a-\lambda)^{[\frac{n+1}{2}]} = 0$, (c) * is of the first kind, $n \equiv 0$ or $n \equiv 3 \pmod 4$, and $a^{[\frac{n+1}{2}]+1} = 0$. Examples are given illustrating (c).

1. **Introduction.** Since this paper makes substantial use of the *extended centroid* of a prime ring, we begin by briefly recalling this notion (see [4] for details). It is known that for a prime ring R there exists a ring of "quotients", Q, characterized by the following properties:

(i) $R \subseteq Q$
(ii) for $q \in Q$ there exists a non-zero ideal U of R such that $Uq \subseteq R$,
(iii) for $q \in Q$ if $Uq = 0$ for some non-zero ideal U of R then $q = 0$,
(iv) for any $f\colon {}_RU \longrightarrow {}_RR$, where U is a non-zero ideal of R, there exists $q \in Q$ such that $uq = f(u)$ for all $u \in U$.

The center C of Q is called the *extended centroid* of R and the ring $A = RC + C$ is called the *central closure* of R. It is well known that C is a field (containing the center of R) and that A is again a prime ring.

If R is a prime ring with extended centroid C we note a simple fact: if $a \in R$ and $a = b + \lambda$, $b^m = 0$, $\lambda \in C$ then $(\operatorname{ad} a)^{2m-1}(R) = 0$. One asks if the converse is true:

(1) $$\text{Does } (\operatorname{ad} a)^n(R) = 0 \text{ imply } (a-\lambda)^{[\frac{n+1}{2}]} = 0 \text{ for some } \lambda \in C?$$

(Here $\left[\frac{n+1}{2}\right]$ equals $\frac{n}{2}$ if n is even and $\frac{n+1}{2}$ if n is odd.) With no restriction on the characteristic of R the answer to (1) is no. For example, let $R = M_p\big(\mathbb{Z}_p(t)\big)$ the ring of $p \times p$ matrices over the field of rational functions with coefficients in $\mathbb{Z}_p$. R is simple with identity so that its extended centroid is just its center $Z_R = \mathbb{Z}_p(t)I_p$. Let

$$a = \begin{bmatrix} 0 & \cdots & \cdots & 0 & t \\ 1 & 0 & & & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{bmatrix}.$$

The second author was partially supported by NSERC of Canada

Received by the editors February 15, 1990.
AMS subject classification: 16A12, 16A28, 16A72.

https://doi.org/10.4153/CJM-1991-060-2 Published online by Cambridge University Press

Then

$$a^p = \begin{bmatrix} t & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & t & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & & t \end{bmatrix} \in Z_R$$

so that $(\operatorname{ad} a)^p = \operatorname{ad}(a^p) = 0$. However, if $\lambda \in \mathbb{Z}_p(t)$ were such that $a - \lambda I$ were nilpotent there would exist an integer $n > 1$ such that $\lambda^n = t$. (Of course there does exist an extension field of the extended centroid which does contain such a λ but we do not know if this is always the case.) Therefore it is natural to assume in questions of this sort that the characteristic is 0 and throughout this paper we will make this assumption. In an earlier paper [7] we were able to answer (1) in the affirmative.

THEOREM A ([7], P. 182, COROLLARY 1(B)). *Let R be a prime ring of* char 0 *and let $a \in R$ be such that* $(\operatorname{ad} a)^n(R) = 0$. *Then* $(a - \lambda)^{[\frac{n+1}{2}]} = 0$ *for some* $\lambda \in C$.

In case R is simple we remark that Theorem A had been previously proved by Herstein [1] and that both he [1] and Kovacs [2] had conjectured the generalization to prime rings.

The hypothesis being a Lie condition, it seems natural to investigate the analogue of Theorem A for prime rings with involution. To be specific we now let R be a prime ring of char 0 with involution *, and let K be the Lie ring of skew elements of R under *, and we pose the question

(2) For $a \in K$, does $(\operatorname{ad} a)^n(K) = 0$ imply that $(a - \lambda)^{[\frac{n+1}{2}]} = 0$ for some $\lambda \in C$?

One low-dimensional counterexample presents itself immediately, namely, $R = M_2(F)$, $^* =$transpose, $a = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. This type of example aside, we shall see that (2) nearly has an affirmative answer, the only adjustment being that in certain cases the index of nilpotency of $a - \lambda$ must be increased by 1.

In order to state our main theorem accurately (which we shall do at the end of this first section) we need to review some notions and facts concerned with central closures, generalized polynomial identities, and involutions, etc. (see [8] for details). In Section 2 we collect further lemmas which are needed before we give the proof proper (in Section 3) of the Main Theorem. Examples showing that the "expected" result does not always occur in certain cases are given in Section 4.

Let R be a prime ring with involution *, with skew elements K and symmetric elements S. It is straightforward to extend * to an involution of the central closure $A = RC + C$. We say that * is *of the first kind* if * is the identity on C, otherwise it is *of the second kind*. Since our Main Theorem will follow almost immediately from Theorem A in case * is of the second kind we now assume for the time being that * is of the first kind. Now let F be the algebraic closure of C and form the *superstar closure* $\tilde{R} = A \underset{C}{\otimes} F$; it is a closed prime algebra over F and carries an involution given by $(a \otimes \lambda)^* = a^* \otimes \lambda$, $a \in A$, $\lambda \in F$. If R satisfies a generalized polynomial identity (GPI) over C then $\tilde{R}$ is also GPI over F, in which case it is well known that $\tilde{R}$ is a primitive F-algebra with nonzero socle, acting densely on an F-vector space V. $\tilde{R}$ always contains a symmetric idempotent e of rank 2 (unless it is already commutative). The algebra $e\tilde{R}e \cong M_2(F)$ inherits the involution * and, by choosing matrix units properly, one shows that * is either the *transpose involution* or the *symplectic involution.* In the former case there exist symmetric elements of rank 1 whereas in the latter case this cannot occur. If f is another symmetric idempotent of rank 2 it is well known ([8], p. 20, Corollary 2.10) that the involution on $f\tilde{R}f$ is transpose (resp. symplectic) if and only if the involution on $e\tilde{R}e$ is transpose (resp. symplectic). For R a prime GPI ring with * of the first kind it is therefore a well-defined notion to say that R is of *transpose type* (resp. *symplectic type*) according to whether the involution on $e\tilde{R}e$ is transpose or symplectic, e a rank 2 symmetric idempotent.

We mention in passing that K/Z_K is always a *prime* Lie ring, where $Z_K = \{x \in K \mid [x, K] = 0\}$, unless R is of transpose type with $\tilde{R} = M_4(F)$ ([8], Corollary 5.12).

We are now in a position to state the

MAIN THEOREM. *Let R be a prime ring with involution * of characteristic 0. Let $a \in K$ be a skew element such that*

$$(\operatorname{ad} a)^n(K) = 0, \text{ some } n \geq 1. \tag{3}$$

1. *If * is of the second kind, then there is a skew element $\lambda \in C$ such that $(a-\lambda)^{[\frac{n+1}{2}]} = 0$.*
2. *If * is of the first kind, then $a^{[\frac{n+1}{2}]} = 0$ unless one of the following holds:*
   (a) * is of transpose type and $\tilde{R} \cong M_2(F)$.
   (b) $n \equiv 0 \pmod 4$ or $n \equiv 3 \pmod 4$, * is of transpose type, $a^{[\frac{n+1}{2}]}$ is a rank 1 *symmetric element of $\tilde{R}$, and $a^{[\frac{n+1}{2}]+1} = 0$.*

2. **Preliminary results.** In this section we gather together several useful lemmas and equations in preparation for Section 3. The hypotheses of the Main Theorem are always assumed to hold, whenever they are needed. We begin by citing a well known basic lemma [4]:

LEMMA 1. *For $u, v \in R$, if $urv = vru$ for all $r \in R$, then u, v are C-dependent.*

A corollary to Lemma 1 is

LEMMA 2 ([5], THEOREM 5). *$A^\circ \underset{C}{\otimes} A \cong A_\ell A_r$, where A° is the opposite algebra of A, A_ℓ (resp. A_r) are the left (resp. right) multiplications of A.*

LEMMA 3 ([8], LEMMA 5.5). *If $a \in R$ such that $[a, K] = 0$ then either a lies in the center Z of R or $\tilde{R} \cong M_2(F)$ and * is of transpose type.*

LEMMA 4. *If $a \in K$ and $aKa = 0$ then $a = 0$.*

PROOF. In view of $2R \subseteq S + K$, then condition implies $axaxa = 0$ for all $x \in R$, i.e., $(ax)^3 = 0$. Thus the element a generates a nil right ideal of bounded index, whence it is well known that $a = 0$. ∎

https://doi.org/10.4153/CJM-1991-060-2 Published online by Cambridge University Press

LEMMA 5. *Let * be of the first kind, let $0 \neq b \in S$ be such that $b^2 = 0$ and $bKb = 0$. Then R is* GPI *of transpose type and b is of rank 1 in $\tilde{R}$.*

PROOF. The condition $bKb = 0$ implies that $bxb = bx^*b$ for all $x \in R$. Thus $bxbyb = bx^*by^*b = b(ybx)^*b = b(ybx)b$ for all $x, y \in R$, and hence for all $x, y \in \tilde{R}$. In particular R is GPI. Writing this equation in the form $(bxb)yb = by(bxb)$ we conclude from Lemma 1 that $bxb = \lambda_x b, \lambda_x \in F$, for all $x \in \tilde{R}$. Recalling that $\tilde{R}$ acts densely on an F-space V, we claim that rank $b = 1$. Indeed, suppose rank $b \geq 2$. We may select $v_1, v_2 \in V$ such that $w_1 = v_1 b, w_2 = v_2 b$ are F-independent. By density there exists $r \in \tilde{R}$ such that $w_1 r = v_1$ and $w_2 r = 0$. Thus $v_1 brb = w_1$ whereas $v_2 brb = 0$. In particular $brb \neq 0$ which implies that $\lambda_r \neq 0$. But then we have the contradiction $0 = v_2 brb = \lambda_r v_2 b = \lambda_r w_2$, and so b must be of rank 1 as claimed. Next we claim $b \in e\tilde{R}e$ for some symmetric idempotent of rank 2. Indeed, we first write $b\tilde{R} = f\tilde{R}$, where f is a rank 1 idempotent. Then $f = br$ for some $r \in \tilde{R}, f^* = r^*b$, and we note $f^*f = 0$. Then $e = f + f^* - ff^*$ is the desired symmetric idempotent. Since $e\tilde{R}e$ contains a rank 1 symmetric element, namely b, we have earlier noted that * must be of transpose type, and the proof of Lemma 5 is now complete. ∎

We now turn our attention to the basic condition (3) and first remark that in expanded form it may be rewritten as

$$\sum_{j=0}^{n}(-1)^j \binom{n}{j} a^{n-j}ka^j = 0 \text{ for all } k \in K. \tag{4}$$

Adopting the notation a_ℓ (resp. a_r) to stand for the left (resp. right) multiplication determined by a, we note that $(a_\ell + a_r)(s) = as + sa \in K$ for all $s \in S$, and as a consequence we see from (3) that

$$(a_\ell - a_r)^n(a_\ell + a_r)(s) = 0 \text{ for all } s \in S. \tag{5}$$

(5) together with (3) yields

$$(a_\ell - a_r)^n(a_\ell + a_r)(R) = 0. \tag{6}$$

Setting $m = n - 1$ we may also write (6) as

$$(a_\ell^2 - a_r^2)(a_\ell - a_r)^m(R) = 0. \tag{7}$$

Translating (7) via Lemma 2 to an equation in $A^\circ \underset{C}{\otimes} A$ we first have

$$(a^2 \otimes 1)\sum_{j=0}^{m}(-1)^j \binom{m}{j} a^{m-j} \otimes a^j - \left(\sum_{j=0}^{m}(-1)^j \binom{m}{j} a^{m-j} \otimes a^j\right)(1 \otimes a^2) = 0$$

which can finally be rewritten as

$$\sum_{j=0}^{m+2}(-1)^j \left[\binom{m}{j} - \binom{m}{j-2}\right] a^{m+2-j} \otimes a^j = 0 \tag{8}$$

where it is understood that $\binom{m}{j} = 0$ if $j < 0$ or $j > m$. Returning to (7) we have as a direct consequence

$$(\operatorname{ad} a^2)^n(R) = \left[(a^2)_\ell - (a^2)_r\right]^n(R) = 0 \tag{9}$$

and so by Theorem A we have

https://doi.org/10.4153/CJM-1991-060-2 Published online by Cambridge University Press

LEMMA 6. *$a^2 - \mu$ is nilpotent for some $\mu \in C$.*

3. **Proof of the Main Theorem.** Suppose first that * is of the second kind, i.e., C contains a non-zero skew element μ. There exists a *-ideal $U \neq 0$ of R for which the *-ideal $V = \mu U \subseteq R$. We write $2U \subseteq U_S + U_K$ (the "symmetric" and "skew" components of U) and note that $(\operatorname{ad} a)^n$ vanishes on both U_K and μU_S. It follows that $(\operatorname{ad} a)^n(V) = 0$ whence by [3] (see also [6]) $(\operatorname{ad} a)^n(R) = 0$. By Theorem A we then have $(a - \lambda)^{[\frac{n+1}{2}]} = 0$ for some $\lambda \in C$. It follows that the minimum polynomial for a over C is of the form $(x - \lambda)^m = x^m - \lambda x^{m-1} + \cdots$. We write $\lambda = \mu + \tau$, $\mu \in K$, $\tau \in S$, and proceed to show that $\tau = 0$. If m is even (resp. odd) the skew (resp. symmetric) component of $(a - \lambda)^m = 0$ is $-m\tau a^{m-1} + \cdots = 0$. By the minimality of m it follows that $\tau = 0$ and so part 1 of the Main Theorem has been proved. (We should remark that for involutions of the second kind this proof shows that for any $a \in R$, $(\operatorname{ad} a)^n(K) = 0$ implies $(a - \lambda)^{[\frac{n+1}{2}]} = 0$ but the λ will not necessarily be in K in this case.) ∎

We assume henceforth that * is of the first kind. In view of Lemma 3 the case $n = 1$, namely, $[a, K] = 0$, forces $\tilde{R} \cong M_2(F)$ with * of transpose type, which is conclusion 2(a).

Next we analyze the situation in which $a^2 = 0$. Without loss of generality we can assume $n = 2$, in which case (4) reduces to $aKa = 0$. By Lemma 4 we reach the contradiction $a = 0$, and so we may assume henceforth that $a^2 \neq 0$.

By Lemma 6 $a^2 - \lambda$ is nilpotent for some $\lambda \in C$, and we set $s = a^2 - \lambda$.

Suppose first that $s = 0$, i.e., $a^2 = \lambda \neq 0$. Thus a^2, and hence a, is invertible in A. We write (4) as

$$a^n k + \binom{n}{2} a^{n-2} k a^2 + \cdots = \binom{n}{1} a^{n-1} k a + \binom{n}{3} a^{n-3} k a^3 + \cdots \tag{10}$$

for all $k \in K$. Substituting λ for a^2 in (10) and using $\operatorname{char} R = 0$ and the fact that $1 + \binom{n}{2} + \cdots = \binom{n}{1} + \binom{n}{3} + \cdots$ we have for $n = 2q$ even:

$$\lambda^q k = \lambda^{q-1} aka \tag{11}$$

and for $n = 2q + 1$ odd:

$$\lambda^q ak = \lambda^q ka \tag{12}$$

In either case (just multiply (11) on the right by a) we are led to $ak = ka$ for all $k \in K$, since $\lambda \neq 0$. This is simply $n = 1$ which we have already handled.

We now assume that $s = a^2 - \lambda \neq 0$ and first treat the situation in which $\lambda \neq 0$. Again a^2, and hence a, is invertible, since $\lambda \neq 0$ and s is nilpotent. If r is the index of nilpotency of s we know that $r \geq 2$ and $1, s, s^2, \ldots, s^{r-1}$ are C-independent symmetric elements. We now return to (8) and conclude that

$$\sum_{0 \leq j \leq [\frac{m+2}{2}]} \left[\binom{m}{2j} - \binom{m}{2j-2} \right] a^{m+2-2j} \otimes a^{2j} = 0, \tag{13}$$

this being the " symmetric $\otimes$ symmetric " (resp. "skew $\otimes$ symmetric ") component of (8) if $n = m + 1$ is odd (resp. even). Setting $q = \left[\frac{m+2}{2}\right]$ and recalling $a^2 = s + \lambda$ we rewrite (13) as

$$\sum_{j=0}^{q}\left[\binom{m}{2j} - \binom{m}{2j-2}\right](s+\lambda)^{q-j} \otimes (s+\lambda)^j = 0, \tag{14}$$

noting that if $n = m + 1$ were even an $a \otimes 1$ was cancelled. In particular the coefficient of the $1 \otimes s$ term must be 0, that is:

$$\sum_{j=0}^{q}\left[\binom{m}{2j} - \binom{m}{2j-2}\right]\lambda^{q-j}(j\lambda^{j-1}) = 0. \tag{15}$$

Cancelling λ^{q-1} from (15) (since $\lambda \neq 0$) we have

$$\sum_{j=0}^{q} j\left[\binom{m}{2j} - \binom{m}{2j-2}\right] = 0. \tag{16}$$

Expanding (16) we have

$$\left[\binom{m}{2} - \binom{m}{0}\right] + 2\left[\binom{m}{4} - \binom{m}{2}\right] + 3\left[\binom{m}{6} - \binom{m}{4}\right] + \cdots = 0$$

which reduces to the contradiction

$$-\left[\binom{m}{0} + \binom{m}{2} + \binom{m}{4} + \cdots\right] = 0.$$

It follows that $\lambda = 0$ and so a^2 is nilpotent. Therefore a is nilpotent and accordingly we may choose r such that $a^r \neq 0$, $a^{r+1} = 0$, noting that $1, a, a^2, \ldots, a^r$ are C-independent. It is now convenient to write (8) in the form

$$\sum_{j=0}^{n+1} \beta_j a^{n+1-j} \otimes a^j = 0, \quad \beta_j \in C \tag{17}$$

where each $\beta_j \neq 0$ except in the one case when n is odd and $j = \frac{n+1}{2}$. From (17) we know a is algebraic of degree $\leq n + 1$ and therefore $r \leq n + 1$. If $r \geq \left[\frac{n+1}{2}\right] + 1$ we rewrite (17) as

$$\sum_{j=0}^{r} \beta_j a^{n+1-j} \otimes a^j = 0$$

and conclude in particular that $a^{n+1-r} = 0$, since $\beta_r \neq 0$ and $1, a, \ldots, a^r$ are independent. But this says that $r < n + 1 - r$, which gives the contradiction $r < \frac{n+1}{2}$. Therefore we have shown in any case

$$a^{\left[\frac{n+1}{2}\right]+1} = 0. \tag{18}$$

https://doi.org/10.4153/CJM-1991-060-2 Published online by Cambridge University Press

For n even (18) says that $a^{\frac{n}{2}+1} = 0$ and consequently (4) reduces to $a^{\frac{n}{2}}ka^{\frac{n}{2}} = 0$ for all $k \in K$. For n odd (18) says that $a^{\frac{n+1}{2}+1} = 0$ and (4) reduces to

$$a^{\frac{n+1}{2}}ka^{\frac{n-1}{2}} = a^{\frac{n-1}{2}}ka^{\frac{n+1}{2}} \tag{19}$$

for all $k \in K$. Multiplying (19) on the right by a yields $a^{\frac{n+1}{2}}ka^{\frac{n+1}{2}} = 0$. Thus in any case $a^{[\frac{n+1}{2}]}ka^{[\frac{n+1}{2}]} = 0$. For $n \equiv 1 \pmod 4$ or $n \equiv 2 \pmod 4$ $a^{[\frac{n+1}{2}]} \in K$ and so by Lemma 4 $a^{[\frac{n+1}{2}]} = 0$. For $n \equiv 0 \pmod 4$ or $n \equiv 3 \pmod 4$ $a^{[\frac{n+1}{2}]}$ is symmetric and, if $a^{[\frac{n+1}{2}]}$ is not already 0, an application of Lemma 5 completes the proof of the Main Theorem. ∎

4. **Examples.** In this section we shall construct for each $n \equiv 0 \pmod 4$ and each $n \equiv 3 \pmod 4$ examples to show that possibilities (2b) of the Main Theorem can actually occur.

Let F be the complex numbers and consider the following matrices over F:

$$A = \begin{bmatrix} 1 & 1 \\ i & i \end{bmatrix}, \quad B = A^t = \begin{bmatrix} 1 & i \\ 1 & i \end{bmatrix}, \quad D = \begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}.$$

One readily checks that D is of rank 1 and that

$$\begin{aligned} &(i) \quad A^kB^k = \alpha_k D, \quad \alpha_k \neq 0 \text{ for all } k \\ &(ii) \quad BA = 0 \end{aligned} \tag{20}$$

In the matrix ring $M_q\big(M_2(f)\big) = M_{2q}(F)$ we set

$$U = U_q = \begin{bmatrix} 0 & A & & & \\ & 0 & A & & \\ & & \ddots & \ddots & \\ & & & 0 & A \\ & & & & 0 \end{bmatrix}, \quad V = V_q = \begin{bmatrix} 0 & & & & \\ B & 0 & & & \\ & B & \ddots & & \\ & & \ddots & 0 & \\ & & & B & 0 \end{bmatrix}.$$

It is straightforward to verify

$$(i) \quad U^q = 0, \tag{21}$$

$$(ii)\ U^{q-1} = \begin{bmatrix} 0 & \cdots & 0 & A^{q-1} \\ & \ddots & & 0 \\ & & \ddots & \vdots \\ & & & 0 \end{bmatrix}, \quad (iii)\ U^{q-2} = \begin{bmatrix} 0 & \cdots & 0 & A^{q-2} & 0 \\ & \ddots & & 0 & A^{q-2} \\ & & \ddots & & 0 \\ & & & \ddots & \vdots \\ & & & & 0 \end{bmatrix}$$

with similar results for V^q, V^{q-1}, V^{q-2}.

We now set $W = W_q = U_q - V_q$. Using (20(ii)) we note that $VU = 0$. From this we easily obtain an expression for the powers of W:

$$W^m = (U - V)^m = \sum_{j=0}^{m} (-1)^j U^{m-j} V^j. \tag{22}$$

https://doi.org/10.4153/CJM-1991-060-2 Published online by Cambridge University Press

For $n \equiv 0 \pmod 4$ we set $q = \frac{n}{4} + 1$ and for $n \equiv 3 \pmod 4$ we set $q = \frac{n+1}{4} + 1$. Letting $R = M_{2q}(F) = M_q\big(M_2(F)\big)$ with transpose involution, we will show that the skew matrix $W = W_q \in R$ has the properties we want:

(a) $W^{[\frac{n+1}{2}]}$ is a rank 1 symmetric matrix

(b) $W^{[\frac{n+1}{2}]+1} = 0$

(c) $(\operatorname{ad} W)^n(L) = 0$ for all skew matrices L (i.e., property (3) holds).

We first take up the case $n \equiv 0 \pmod 4$, in which $q = \frac{n}{4} + 1$. By (22), (21i), (21ii), and (20i) we see that

$$
\begin{aligned}
W^{[\frac{n+1}{2}]} &= W^{\frac{n}{2}} = (-1)^{\frac{n}{4}} U^{\frac{n}{4}} V^{\frac{n}{4}} \\
&= (-1)^{\frac{n}{4}} \begin{bmatrix} 0 & & 0 & A^{\frac{n}{4}} \\ & \ddots & & 0 \\ & & \ddots & \\ & & & 0 \end{bmatrix} \begin{bmatrix} 0 & & & \\ & \ddots & & \\ 0 & & \ddots & \\ B^{\frac{n}{4}} & 0 & & 0 \end{bmatrix} \\
&= (-1)^{\frac{n}{4}} \begin{bmatrix} A^{\frac{n}{4}} B^{\frac{n}{4}} & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \end{bmatrix} = \alpha \begin{bmatrix} D & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \end{bmatrix}, \qquad \alpha \neq 0
\end{aligned}
$$

which establishes (a). Expansion of $W^{\frac{n}{2}+1}$ by (22), in conjunction with (21i), implies (b). Because of (b), showing that $(\operatorname{ad} W)^n(L) = 0$, L skew, reduces to showing that $W^{\frac{n}{2}} L W^{\frac{n}{2}} = 0$. But, already knowing that $W^{\frac{n}{2}} = \alpha \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$, we see that this follows from the simple matrix calculation

$$
\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.
$$

We have thereby shown (c) and thus completed the case $n \equiv 0 \pmod 4$.

Now suppose $n \equiv 3 \pmod 4$, with $q = \frac{n+1}{4} + 1$. The same proof as in the case $n \equiv 0 \pmod 4$ (with $n + 1$ playing the role of n) goes through to establish (a) and (b). In view of (b), since n is odd, showing $(\operatorname{ad} W)^n(L) = 0$. L skew, reduces to showing

$$
-\binom{n}{\frac{n-1}{2}} W^{\frac{n+1}{2}} L W^{\frac{n-1}{2}} + \binom{n}{\frac{n+1}{2}} W^{\frac{n-1}{2}} L W^{\frac{n+1}{2}} = 0.
$$

In other words, in order to establish (c) it suffices to show

$$
W^{\frac{n+1}{2}} L W^{\frac{n-1}{2}} = W^{\frac{n-1}{2}} L W^{\frac{n+1}{2}}, \quad L \text{ skew}. \tag{23}
$$

To this end we first compute $W^{\frac{n-1}{2}}$. Expanding $W^{\frac{n-1}{2}}$ by means of (22) and using (21i) we see that

$$
W^{\frac{n-1}{2}} = (-1)^{q-2} U^{q-1} V^{q-2} + (-1)^{q-1} U^{q-2} V^{q-1}. \tag{24}
$$

https://doi.org/10.4153/CJM-1991-060-2 Published online by Cambridge University Press

Now, using (21ii), (21iii) and (20i), we may expand (24) into:

$$
\begin{aligned}
W^{\frac{n-1}{2}} &= (-1)^q \begin{bmatrix} 0 & \cdots & 0 & A^{q-1} \\ & \ddots & & 0 \\ & & \ddots & \vdots \\ & & & 0 \end{bmatrix} \begin{bmatrix} 0 & & & & \\ \vdots & \ddots & & & \\ 0 & & \ddots & & \\ B^{q-2} & 0 & & \ddots & \\ 0 & B^{q-2} & 0 & \cdots & 0 \end{bmatrix} \\
&\quad + (-1)^{q-1} \begin{bmatrix} 0 & \cdots & 0 & A^{q-2} & 0 \\ & \ddots & & 0 & A^{q-2} \\ & & \ddots & & 0 \\ & & & \ddots & \vdots \\ & & & & 0 \end{bmatrix} \begin{bmatrix} 0 & & & \\ \vdots & \ddots & & \\ 0 & & \ddots & \\ B^{q-1} & 0 & \cdots & 0 \end{bmatrix} \\
&= (-1)^q \begin{bmatrix} 0 & A^{q-1}B^{q-2} & 0 & \cdots \\ 0 & 0 & 0 & \cdots \\ \vdots & \vdots & & \end{bmatrix} + (-1)^{q-1} \begin{bmatrix} 0 & 0 & \cdots \\ A^{q-1}B^{q-2} & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \end{bmatrix} \\
&= \alpha \left[\begin{array}{cc|c} 0 & (-1)^q AD & 0 \\ (-1)^{q-1} DB & 0 & \\ \hline \multicolumn{2}{c|}{0} & 0 \end{array}\right].
\end{aligned}
$$

On the other hand we already know (in establishing (b)) that

$$
W^{\frac{n+1}{2}} = \delta \left[\begin{array}{cc|c} D & 0 & 0 \\ 0 & 0 & \\ \hline \multicolumn{2}{c|}{0} & 0 \end{array}\right].
$$

It is now clear that in order to show (23)it suffices to prove

$$
\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} M & E \\ -E^t & N \end{bmatrix} \begin{bmatrix} 0 & AD \\ -DB & 0 \end{bmatrix} = \begin{bmatrix} 0 & AD \\ -DB & 0 \end{bmatrix} \begin{bmatrix} M & E \\ -E^t & N \end{bmatrix} \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix} \tag{25}
$$

where M, N, E are 2×2 matrices with M and N skew. In turn showing (25) reduces to verifying the two equations

$$
DMAD = 0 \tag{26}
$$

$$
DEDB = ADE^tD. \tag{27}
$$

($DBMD = 0$ follows from (26) by taking transposes.)

To show (26) we may take $M = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and simply verify that

$$
\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ i & i \end{bmatrix} \begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.
$$

To show (27) we set $E = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$ and verify that

$$
\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix} \begin{bmatrix} 1 & i \\ 1 & i \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ i & i \end{bmatrix} \begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}.
$$

We have thus constructed, for each $n \equiv 0$ or $n \equiv 3 \pmod 4$, an element W lying in a matrix ring $R = R_n = M_{2q}(F)$ satisfying (a), (b), (c). We remark that, at the cost of adding some more notation, we could just as well have formed a single ring R, namely the ring consisting of all countably infinite sized "corner" matrices over F of the form

$$\begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix}$$

where A is an $n \times n$ matrix, n varies, and the 0's are approxpriate size infinite blocks. The involution is again traspose and the elements W_q all lie in this ring. Thus a ring illustrating possibility 2(b) of the Main Theorem need not be PI (although indeed it must be GPI).

REFERENCES

1. I. N. Herstein, *Sui commutator degli anelli semplici.* Rendiconte del Seminario Matematico e Fisico di Milana **XXXIII**, 1963.

2. A. Kovacs, *Nilpotent derivations.* Technion Preprint Series, No. NT-453.

3. C. Lanski, *Differential identities in prime rings with involution*, TAMS **292**(1985), 765–787.

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

5. ———, *Lie isomorphisms of prime rings*, Trans. Amer. M. Soc. **142**(1969), 437–455.

6. ———, *Lectures at Jilen University*. University of Massachusetts, unpublished.

7. W. S. Martindale and C. R. Miers, *On the iterates of derivations of prime rings*, Pac. J. Math. **104**(1983), 179–190.

8. ———, *Herstein's Lie theory revisited*, J. Algebra **98**(1986), 14–37.

Department of Mathematics
University of Massachusetts
Amherst, Massachusetts 01003
USA

Department of Mathematics and Statistics
University of Victoria
Victoria, BC V8W 3P4