Canad. Math. Bull. Vol. **22** (3), 1979

ON DERIVATIONS IN PRIME RINGS AND A QUESTION OF HERSTEIN

BY
AMOS KOVACS

1. In [2], Herstein proves the following result:

THEOREM. *Let R be a prime ring, $d \neq 0$ a derivation of R such that $d(x)\, d(y) = d(y)\, d(x)$ for all $x, y \in R$. Then, if* char $r \neq 2$, *R is commutative, and if* char $R = 2$, *R is commutative or an order in a simple algebra which is 4-dimensional over its center.*

In the same paper Herstein asks whether the natural generalization of this theorem holds, namely:

QUESTION A. If $S_k[x_1, \ldots, x_k]$ is the standard identity of degree k, and if $d \neq 0$ is a derivation of a prime ring R such that $S_k[d(x_1), \ldots, d(x_k)] = 0$ for all $x_1, \ldots, x_k \in R$ can we conclude that R must be rather special or must satisfy S_k?

We shall start by reproving Herstein's theorem for the case char $R \neq 2$. Our proof, while similar in flavor to the original proof, is simpler and makes it clear that we can hardly hope for an affirmative answer to the question. We proceed then to construct several examples to demonstrate that the answer to Herstein's question, and to some possible weaker version of it, is negative.

2. THEOREM 1 (Herstein). *Let R be a prime ring,* char $R \neq 2$. *$d \neq 0$ a derivation of R such that $d(x)\, d(y) = d(y)\, d(x)$ for all $x, y \in R$, then R is commutative.*

Proof. As in ([2], Th. 2) one gets easily that $d^2 \neq 0$. Let A be the subring of R generated by $d(R)$. Since $d^2 \neq 0$ we have $d(A) \neq 0$. $d(AR) \subseteq d(A)R + Ad(R)$ which implies $d(A)R \subseteq A$. We have then that $0 \neq d(A) + d(A)R$ is a right ideal of R contained in A. Since by the assumption A is commutative, so is the ideal $d(A) + d(A)R$. It is now an easy exercise to show that a prime ring containing a commutative one sided ideal is itself commutative.

One sees from this proof the difficulty of generalizing the result to higher degrees of commutativity; the fact that a ring A is generated by elements satisfying $S_k[\ ]$ does not guarantee that the ring will satisfy $S_k[\ ]$—unless $k = 2$. (There is still another technical difficulty in trying to generalize this proof. The fact that a prime ring R has a one sided ideal satisfying an identity does not

Received by the editors July 31, 1978.
Technion preprint series No MT396.

imply that R satisfies an identity—see [1]. This could be overcome rather easily by assuming $d^3 \neq 0$ and using Theorem 1 of [2] and Theorem 1 of [1].)

3. Question A, as phrased is of course quite vague. But unless one is ready to admit some very "nice" rings as exceptions, we have a negative answer in the following easy example.

EXAMPLE 1. Let F be any field, $R = M_n(F)$ $(n \geq 2)$ the ring of $n \times n$ matrices over F, $\{e_{ij} \mid 1 \leq i, j \leq n\}$ the standard matrix units of R and d the inner derivation of R induced by e_{11}, i.e.

$$d(a) = e_{11}a - ae_{11} = [e_{11}, a] \qquad a \in R.$$

An easy computation will show that

$$d(R) = \{[e_{11}, a] \mid a \in R\} = \text{Span}_F\{e_{i1}, e_{1j} \mid 2 \leq i, j \leq n\}.$$

Since $\dim_F d(R) = 2n - 2$, $d(x_1), \ldots, d(x_{2n-1})$ will be linearly dependent over F for all $x_1, \ldots, x_{2n-1} \in R$. By well known properties of the standard identity this implies $S_{2n-1}[d(x_1), \ldots, d(x_{2n-1})] = 0$. On the other hand, $M_n(F) = R$ does not satisfy $S_{2n-1}[\ ]$.

At this stage, one naturally tries for the less restrictive and more difficult question:

QUESTION B. Let $f(x_1, \ldots, x_k)$ be some non zero polynomial in non-commuting variables $x_1, \ldots, x_k$. Let $d \neq 0$ be a derivation of a prime ring R such that $f(d(x_1), \ldots, d(x_k)) = 0$ for all $x_1, \ldots, x_k \in R$. Does R satisfy a polynomial identity?

Our next example shows that the answer to question B is still negative, even when f is a standard polynomial. To construct it, we shall carry over the idea of example 1 to the infinite dimensional case.

EXAMPLE 2. Let F be any field, ${}_FV$ a vector space with a denumerable basis $\{v_i \mid i = 1, 2, \ldots\}$. Let $R = \text{Hom}_F(V, V)$, R is a primitive (hence prime) ring which satisfies no polynomial identities. Denote by e_{11} the transformation in R defined by

$$e_{11}v_i = \delta_{1i}v_1$$

and let d be the inner derivation of R defined by e_{11}. We shall proceed via several claims to establish that (R, d) provides the desired example. As before, $d(R) = \{[e_{11}, a] \mid a \in R\}$ is a subspace of R.

CLAIM 1. If $T \in d(R)$ then for $i > 1$ $T(v_i) = \lambda_i v_1$.

Proof. Note first that for any $v \in V$ $e_{11}v = \lambda v_1$. Now if $T = [e_{11}, a] \in d(R)$ then $Tv_i = (e_{11}a - ae_{11})v_i = (e_{11}a)v_i = e_{11}(av_i) = \lambda_i v_1$.

Call a transformation $T \in d(R)$ basic if there is an $n > 1$ and a scalar $\lambda_1 \in F$

https://doi.org/10.4153/CMB-1979-042-0 Published online by Cambridge University Press

such that $Tv_1 = \lambda_1 v_n$. Denote by B the set of all basic transformations in $d(R)$.

CLAIM 2. Every $T \in d(R)$ is a (finite) sum of basic transformations.

Proof. This is immediate once we note that for any $T \in d(R)$

$$Tv_1 = \sum_{i \geq 2} \alpha_i v_i \qquad \alpha_i \in F$$

Let now $A^1, \ldots, A^{2p}$ be basic transformations. For any $1 \leq \nu \leq 2p$ write

$$A^\nu v_1 = a_1^\nu v_{n(\nu)} \qquad A^\nu v_i = a_i^\nu v_1 \ (i > 1) \qquad a_j^\nu \in F.$$

We shall now examine the action of the product $A^1, \ldots, A^{2p}$ on v_1.

$$\begin{aligned} A^1 \cdots A^{2p} v_1 &= A^1 \cdots A^{2p-1}(a_1^{2p} v_{n(2p)}) = a_1^{2p} A^1 \cdots (A^{2p-1} v_{n(2p)}) \\ &= a_1^{2p} A^1 \cdots A^{2p-2}(a_{n(2p)}^{2p-1} v_1) = a_1^{2p} a_{n(2p)}^{2p-1} A^1 \cdots (A^{2p-2} v_1) \\ &= \cdots = a_1^{2p} a_{n(2p)}^{2p-1} a_1^{2p-2} a_{n(2p-2)}^{2p-3} \cdots a_1^2 a_{n(2)}^1 v_1. \end{aligned}$$

A similar consideration will show that

$$S_{2p}[A^1, \ldots, A^{2p}] v_1 = \left(\sum_{\sigma \in S_{2p}} (-1)^\sigma a_1^{\sigma(2p)} a_{n(\sigma(2p))}^{\sigma(2p-1)} \cdots a_1^{\sigma(2)} a_{n(\sigma(2))}^{\sigma(1)} \right) v_1.$$

Denote now for any permutation $\sigma \in S_{2p}$

$$\alpha_\sigma = a_1^{\sigma(2p)} a_{n(\sigma(2p))}^{\sigma(2p-1)} \cdots a_1^{\sigma(2)} a_{n(\sigma(2))}^{\sigma(1)} \in F.$$

We have therefore

$$S_{2p}[A^1, \ldots, A^{2p}] v_1 = \left(\sum_{\sigma \in S_{2p}} (-1)^\sigma \alpha_\sigma \right) v_1$$

Let us consider the following set of permutations in S_{2p}.

$$S_{2p} \supseteq H = \left\{ \tau \in S_{2p} \;\middle|\; \begin{array}{l} \tau(2k) = 2l \\ \tau(2k-1) = \tau(2k) - 1 \end{array} \right\}$$

Note that the permutations in H act separately on even and odd digits and that their action on the even digits determines them completely. Let $\tau, \pi \in H$ and assume $\tau(2k) = 2l$ for some $1 \leq k, l \leq p$. Clearly the product $\pi\tau$ acts separately on even and odd digits, moreover,

$$\begin{aligned} \pi\tau(2k-1) = \pi(\tau(2k-1)) = \pi(\tau(2k)-1) = \pi(2l-1) \\ = \pi(2l) - 1 = \pi(\tau(2k)) - 1 = \pi\tau(2k) - 1, \end{aligned}$$

and so the product $\pi\tau$ is again in H. H is therefore a subgroup of S_{2p} whose order is clearly $p!$ In fact, $H \simeq S_p$ under the correspondence $\tau \to \tilde{\tau}$ where

$$\tilde{\tau}(k) = \frac{\tau(2k)}{2} \qquad 1 \leq k \leq p.$$

CLAIM 3. H contains only even permutations.

Proof. Let $\tau \in H$, to find the parity of τ we count the number of inversions under τ, that is the cardinality of the set $I = \{(i, j) \mid i < j, \tau(i) > \tau(j)\}$.

We may write I as a disjoint union of 4 sets relative to the parity of i and j as follows:

$$I = I_{00} \dot{\cup} I_{11} \dot{\cup} I_{01} \dot{\cup} I_{10}$$

where

$$I_{kl} = \{(i, j) \mid (i, j) \in I,\ i \equiv k (\mathrm{mod}\ 2),\ j \equiv l (\mathrm{mod}\ 2)\}$$

We leave it to the reader to check that there is a one to one correspondence between I_{00} and I_{11} given by

$$I_{00} \to I_{11}$$
$$(i, j) \to (i-1, j-1)$$

and between I_{10} and I_{01} given by

$$I_{10} \to I_{01}$$
$$(i, j) \to (i+i, j-1).$$

(To varify the second assertion, note that if $(i, j) \in I_{10}$ then i and j cannot be consecutive integers!)

It follows now that I has even cardinality and so τ is an even permutation

CLAIM 4. If $\tau \in H$ then $\alpha_1 = \alpha_\tau$.

Proof. Since $\tau(2k-1) = \tau(2k) - 1$ we have

$$\alpha_\tau = a_1^{\tau(2p)} a_{n(\tau(2p))}^{\tau(2p)-1} a_1^{\tau(2p-2)} a_{n(\tau(2p-2)}^{\tau(2p-2)-1} \cdots a_1^{\tau(2)} a_{n(\tau(2))}^{\tau(2)-1}.$$

Now, since τ interchanges even digits, clearly α_τ is a product of all terms of the form a_1^{2k} and $a_{n(2l)}^{2l-1}$ for all $1 \le k, l \le p$. These are, in a different order, exactly the factors of α_1 – hence our claim.

Let now $\pi \in S_{2p}$ be any permutation, and denote

$$A^{\pi(\nu)} = B^\nu \qquad a_i^{\pi(\nu)} = b_i^\nu, \qquad 1 \le \nu \le 2p, \qquad i = 1, 2, \ldots$$

Define $\beta_\sigma \in F$ by using the $b_i^\nu - s$, in the same way the α_σ were defined using the $a_i^\nu - s$. As before,

$$B^{\sigma(1)} \cdots B^{\sigma(2p)} v_1 = \beta_\sigma v_1.$$

On the other hand,

$$B^{\sigma(1)} \cdots B^{\sigma(2p)} v_1 = A^{\pi\sigma(1)} \cdots A^{\pi\sigma(2p)} v_1 = \alpha_{\pi\sigma} v_1.$$

https://doi.org/10.4153/CMB-1979-042-0 Published online by Cambridge University Press

We conclude therefore that $\beta_\sigma = \alpha_{\pi\sigma}$ for all $\sigma \in S_{2p}$. Claim 4 applied to the $\beta - s$ gives $\beta_1 = \beta_\tau$ for all $\tau \in H$. Combining these two equalities we get

CLAIM 5. For any $\pi \in S_{2p}$ and $\tau \in H$

$$\alpha_\pi = \alpha_{\pi\tau}.$$

Choose now $\pi_1 \cdots \pi_t$, where $t = (2p)!/p!$, a set of representatives for the different left cosets of H in S_{2p}, then S_{2p} is the disjoint union $S_{2p} = \cup_{i=1}^{t} \pi_i H$ and so, using claims 3 and 5 we have:

$$S_{2p}[A^1, \ldots, A^{2p}]v_1 = \left(\sum_{\sigma \in S_{2p}} (-1)^\sigma \alpha_\sigma\right) v_1 = \left(\sum_{i=1}^{t} \left(\sum_{\tau \in H} (-1)^{\pi_i \tau} \alpha_{\pi_i \tau}\right)\right) v_1$$

$$= \left(p! \sum_{i=1}^{t} (-1)^{\pi_i} \alpha_{\pi_i}\right) v_1.$$

In particular this proves:

CLAIM 6. If σ char $F = p > 0$ then for any $2p$ basic transformations $A^1 \cdots A^{2p}$ we have

$$S_{2p}[A^1, \ldots, A^{2p}]v_1 = 0.$$

We are now ready to prove our main result which will establish (R, d) as a counterexample to Question B.

THEOREM 2. *Let* char $F = p > 0$, R *and* d *as defined above, then*

$$S_{4p+1}[d(x_1), \ldots, d(x_{4p+1})] = 0 \quad \text{for all} \quad x_1, \ldots, x_{4p+1} \in R.$$

Proof. We have to show that $S_{4p+1}[A^1, \ldots, A^{4p+1}] = 0$ for any substitution of transformations $A^i \in d(R)$. Since S_{4p+1} is multilinear it is enough to show, in view of claim 2, that S_{4p+1} vanishes for any substitution of basic transformations $A^i \in B$.

A double application of "Laplace's expansion" to the standard polynomial $S_{4p+1}[x_1, \ldots, x_{4p+1}]$ will show that it can be written as a sum of the form

$$S_{4p+1}[x_1, \ldots, x_{4p+1}] = \sum^{\pm} S_{2p}[x_{i_1}, \ldots, x_{i_{2p}}] x_{i_{2p+1}} S_{2p}[x_{i_{2p+2}}, \ldots, x_{i_{4p+1}}]$$

and so, in order to prove our theorem, it is enough to show that the polynomial

$$p(x_1, \ldots, x_{4p+1}) = S_{2p}[x_1, \ldots, x_{2p}] x_{2p+1} S_{2p}[x_{2p+2}, \ldots, x_{4p+1}]$$

vanishes for any substitution of $A^i \in B$. Choose then A^i $i = 1, \ldots, 4p+1$, basic transformations, and consider

$$A = S_{2p}[A^1, \ldots, A^{2p}] A^{2p+1} S_{2p}[A^{2p+2}, \ldots, A^{4p+1}].$$

In order to show that $A = 0$, it is enough, since R acts faithfully on V, to show that $AV = 0$ and in particular that $Av_i = 0$ for all i.

https://doi.org/10.4153/CMB-1979-042-0 Published online by Cambridge University Press

By claim 6 we clearly have $Av_1 = 0$. Consider v_i for $i > 1$. The transformation $A^{2p+1}S_{2p}[A^{2p+2}, \ldots, A^{4p+2}]$ is a sum of products of odd length of basic transformations. From the definition of these, it is clear that any such odd product will take v_i, for $i > 1$, to a scalar multiple of v_1, hence

$$A^{2p+1}S_{2p}[A^{2p+2}, \ldots, A^{4p+2}]v_i = a_i v_1 \qquad a_i \in F.$$

Now, reapplying claim 6, we get

$$Av_i = S_{2p}[A^1, \ldots, A^{2p}](a_i v_1) = a_i S_{2p}[A^1, \ldots, A^{2p}]v_1 = 0.$$

When char $F = 0$ we have been unable to show that R satisfies a relation of the form $S_k[d(x_1), \ldots, d(x_k)] = 0$. Still one can easily show a bit less, namely:

EXAMPLE 3. If char $F = 0$ and R and d as before, then

$$[d(x_1)\, d(x_2), d(x_3)\, d(x_4)]\, d(x_5)[d(x_6)\, d(x_7), d(x_8)\, d(x_9)] = 0$$

for all $x_1, \ldots, x_9 \in R$.

Proof. As before, enough if we show that the polynomial

$$f(x_1, \ldots, x_9) = [x_1x_2, x_3x_4]x_5[x_6x_7, x_8x_9]$$

vanishes for all basic substitutions. If A, B, C, D are basic transformations then one sees easily that $ABv_1 = \alpha v_1$, $CDv_1 = \beta v_1$ for some $\alpha, \beta \in F$. This clearly implies $[AB, CD]v_1 = 0$ and now, an argument identical to the one used above will show that f vanishes under all basic substitutions.

Finally, we raise the following:

QUESTION C. If R is a prime ring with a derivation $d \neq 0$ satisfying a relation of the form $f(d(x_1), \ldots, d(x_k)) = 0$, what can be said about R? In particular, is R (or its central closure) primitive?

REFERENCES

1. L. P. Belluce and S. K. Jain, *Prime rings with a one sided ideal satisfying a polynomial identity*, Pacific J. Math. vol. **24,** No. 3, 1968, pp. 421–424.

2. I. N. Hernstein, *A note on derivations*, to appear.

DEPT. OF MATHEMATICS
TECHNION
I.I.T. HAIFA, ISRAEL