ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 6, Number 2, Spring 1976

COMMUTING SKEW ELEMENTS IN RINGS WITH INVOLUTION

I. N. HERSTEIN[1] AND PJEK-HWEE LEE

We shall be concerned here with rings with involution and their skew elements. Let R be a ring with involution $*$ and let $K = \{x \in R \mid x^* = -x\}$ and $S = \{x \in R \mid x^* = x\}$ be the sets of skew and symmetric elements, respectively, of R. We shall also be concerned with a special subset, K_0, of K defined by $K_0 = \{x - x^* \mid x \in R\}$; we call the elements of K_0 *skew-traces*. We shall consistently use the notation Z, or $Z(R)$ to denote the center of R and J to denote the Jacobson radical of R.

In a recent paper [1], Herstein has shown that if every $a \in K_0$ satisfies $a^{n(a)} = a$, $n(a) > 1$, then any two elements in K must commute. On the other hand, Lee has shown in [2] that if R is a semi-simple ring, in which $2R = R$, and if given $a \in K$ then $a - a^2 p_a(a) \in Z$, where $p_a(t)$ is a polynomial with integer coefficients which depend on a, then the structure of R is that of a subdirect product of fields and 2×2 matrices over fields, where the involution is completely described. As a consequence it is true, in Lee's situation, that any two elements in K must commute. It is easy to change the proof of Lee's Theorem 8 to obtain that even if R is not semi-simple, then $ab - ba \in J$ for all $a, b \in K$. We shall show this — in fact in a slightly more general form — below.

In this paper we shall show that this result of Lee can be considerably sharpened, for it will turn out, in fact, that in rings satisfying Lee's condition on the elements of K_0 (and not necessarily on all of K) we must have $ab = ba$ for all a and b in K. Of course this also extends Herstein's result mentioned earlier, at least for rings in which $2R = R$.

Our aim is to prove the

THEOREM. *Let R be a ring with involution $*$ such that $2R = R$. Suppose that, given $a \in K_0$ then $a - a^2 p_a(a) \in Z$ where $p_a(t)$ is a polynomial with integer coefficients which depend on a. Then $uv = vu$ for all $u, v \in K$.*

Received by the editors on July 12, 1974, and in revised form on December 5, 1974.

[1]The work of the first author was supported in part by NSF grant GP 29269 at the University of Chicago.

REMARK 0. If R is a $*$-prime ring such that $2R = R$, then R is 2-torsion free, so $2K = K$ and therefore $K_0 = K$.

Before getting down to the proof of the theorem we make a slight improvement in Theorem 8 of [2]. We claim that if R is semi-simple and $a - a^2p_a(a) \in Z$ for all $a \in K_0$, then, if $2R = R$, any two elements in K must commute.

We prove this by indicating the changes needed in the proof that Lee gave. Let P be a primitive ideal of R. If $P^* \neq P$ then $(P^* + P)/P$ is a non-zero ideal in the primitive ring $\bar{R} = R/P$. Moreover — as Lee shows — every element in $(P^* + P)/P$ is the image of a skew trace in R, hence every element u in $(P^* + P)/P$ satisfies a relation $u - u^2p_u(u) \in Z(\bar{R})$. This forces R to be commutative — Lee's argument here carries over. On the other hand, if $P^* = P$, then since $2R = R$, $2\bar{R} = \bar{R}$ where $\bar{R} = R/P$. Since by Remark 0, $\bar{K}_0 = \bar{K}$, any two elements in $\bar{K}$ commute by Lee's Theorem 8. So, if $u, v \in K$ then $uv - vu \in P$. Since $uv - vu \in P$ for all primitive ideals P of R and because R is semi-simple, $\bigcap P = 0$, we have $uv = vu$ for all $u, v \in K$.

We now return to our theorem. The theorem will be a consequence of the lemmas we are about to prove. However, we first make a few preliminary *remarks* which shall be used throughout.

1. Since skew-traces in R/U are images of skew traces in R, if $U^* = U$, the hypothesis on elements of K_0 carries over to the skew-traces in R/U.

2. We may assume that R is generated by K.

3. Since $2R = R$, if $2x \in Z$ then $x \in Z$.

4. If $a \in K_0$, then in the polynomial $a^2p_a(a)$ we may assume that only *odd* powers of a occur. For, if $b = a + m_1a^2 + m_2a^3 + \cdots + m_ka^k \in Z$, then $b^* = -a + m_1a^2 + \cdots \in Z$, hence $b - b^* = 2(a + m_2a^3 + \cdots) \in Z$. By remark 3, $a + m_2a^3 + m_4a^5 + \cdots \in Z$, as claimed.

5. Since $a^{2k+1} = a^kaa^k$, if $a \in K_0$, then $a^{2k+1} \in a^kK_0a^k \subset K_0$; thus we have $a - a^2p_a(a) \in Z$ where, by remark 4, $a^2p_a(a)$ involves only odd powers of a, and so $a^2p_a(a) \in K_0$. Hence $a^2p_a(a) - q(a^2p_a(a))(a^2p_a(a))^2 \in Z$ for a suitable polynomial q with integer coefficients. This gives us, on adding to $a - a^2p_a(a) \in Z$, that $a - a^4t(a) \in Z$ for a suitable polynomial $t(a)$ with integer coefficients. Continuing in this way, we get $a - a^rf_a(a) \in Z$ for r arbitrarily high.

6. In view of remark 5, all nilpotent elements in K_0 are in Z.

Recall that a ring R with involution is *$*$-subdirectly irreducible* if the intersection of all its nonzero $*$-ideals U, (i.e., $U^* = U$), is a nonzero ideal of R. Thus, in this case, R has a minimal $*$-ideal $M \neq 0$ and $M \subset U$ for all $*$-ideals $U \neq 0$ of R. Since every ring with involution is a subdirect product of $*$-subdirectly irreducible rings, to prove our theorem it is sufficient to prove it for $*$-subdirectly irreducible rings. Thus *we assume henceforth* that R is a $*$-subdirectly irreducible ring, with $2R = R$ and in which our running hypothesis on K_0 holds.

We shall use the commutator notation $[x, y] = xy - yx$ and $[A, B]$ for the additive subgroup of R generated by all $[a, b]$, where $a \in A, b \in B$.

Let $M \neq 0$ be the minimal $*$-ideal of R, and let $A(M) = \{x \in R \mid xM = Mx = 0\}$. $A(M)$ is a $*$-ideal of R. Our first objective is to show that if $[K, K] \neq 0$ then $A(M) \neq 0$. Recall that J is the Jacobson radical of R.

LEMMA 1. *If* $[K, K] \neq 0$, *then* $J \neq 0$ *and* $J \subset A(M)$. *Hence* $M^2 = 0$.

PROOF. As we indicated in our improvement of Lee's Theorem 8, $[K, K] \subset J$; hence, since $[K, K] \neq 0$, we have that $J \neq 0$. Because $J^* = J, J \supset M$.

If $M \cap K_0 \neq 0$, let $a \neq 0 \in M \cap K_0$. Thus $a - a^2 p_a(a) = b \in Z \cap M$; by remark 4, we may assume that $b \in K_0$. Since $a \in J$, $a \neq a^2 p_a(a)$, hence $b \neq 0$. Now $bJ = Jb$ is a $*$-ideal of R since $b^* = -b \in Z$. If $bJ \neq 0$ we must have $bJ = M$. Therefore $bj = b$ for some $j \in J$; this gives $b = 0$. Thus $bJ = Jb = 0$. This tells us that $W = \{x \in R \mid xJ = Jx = 0\}$ is not 0; therefore W, being a $*$-ideal of R, contains M. This gives $MJ = JM = 0$, and so $J \subset A(M)$, as claimed.

On the other hand, if $M \cap K_0 = 0$, then $x = x^*$ for all $x \in M$. If $s \neq 0 \in M$ then $ys \in M$ for any $y \in R$; hence $(ys)^* = ys$, which gives us $ys = sy^*$ for all $y \in R$. Thus $sR = Rs$ is a $*$-ideal of R, as is $sJ = Js$. If $sJ \neq 0$ then $sJ = M$ follows, and so $sj = s$ for some $j \in J$. This gives $s = 0$; hence here too, $MJ = JM = 0$ results. Hence $J \subset A(M)$.

We pass to

LEMMA 2. $[K, K] \subset Z$.

PROOF. If $[K, K] = 0$ then it certainly lies in Z. So suppose that $[K, K] \neq 0$. Our aim is to show that if $a, b \in K$ then $c = ab - ba$ is nilpotent for then, by remark 6 since $c \in K_0$ is nilpotent it must be in Z.

Suppose then that $c = ab - ba \neq 0$ is not nilpotent. Let U be a $*$-ideal maximal with respect to exclusion of the powers of c, and let $\bar{R} = R/U$. Since a power of $\bar{c}$, the image of c in $\bar{R}$, falls in every nonzero $*$-ideal of $\bar{R}$, $\bar{R}$ is $*$-prime, hence semi-prime. Since $\bar{c} = [\bar{a}, \bar{b}] \neq 0$, in $\bar{R}$, $[\bar{K}, \bar{K}] \neq 0$, hence by Lemma 1, $\bar{R}$ cannot be $*$-subdirectly irreducible, for if it were, its minimal $*$-ideal would be nilpotent. So the intersection of the nonzero $*$-ideals of $\bar{R}$ is 0.

Let $\bar{V} \neq 0$ be a $*$-ideal of $\bar{R}$; thus $\bar{c}^n \in \bar{V}$ for some $n \geqq 2$. However, since $\bar{c} \in [\bar{K}, \bar{K}] \subset \bar{K}_0$, by remark 5, $\bar{c} - \bar{c}^n q(\bar{c}) \in Z(\bar{R})$ for some polynomial q with integer coefficients. Thus, for any $\bar{x} \in \bar{R}$, $\bar{c}\bar{x} - \bar{x}\bar{c} = \bar{c}^n q(\bar{c})\bar{x} - \bar{x}\bar{c}^n q(\bar{c}) \in \bar{V}$, which is to say, $\bar{c}\bar{x} - \bar{x}\bar{c}$ is in every nonzero $*$-ideal of $\bar{R}$. But then $\bar{c}\bar{x} - \bar{x}\bar{c} = 0$, and so $\bar{c} \in Z(\bar{R})$.

Because $\bar{R}$ is $*$-prime and $\bar{c} \neq 0 \in Z(\bar{R})$, since $\bar{c}^* = -\bar{c}$, $\bar{c}$ cannot be a zero-divisor in $\bar{R}$; since $\bar{c} = [\bar{a}, \bar{b}] \neq 0$, $\bar{a} \notin Z(\bar{R})$, hence $\bar{a}$ cannot be nilpotent (remark 0 and 6). Therefore $\bar{c}\bar{a}^2$ is not nilpotent; now $\bar{c}\bar{a}^2 = \bar{a}\bar{c}\bar{a} \in \bar{K}_0$ since $\bar{c} \in \bar{K}_0$ and $\bar{a} \in \bar{K}$. The argument used for $\bar{c}$ works equally well for $\bar{c}\bar{a}^2$; for, if $\bar{V} \neq 0$ is a $*$-ideal of $\bar{R}$, then $\bar{c}^n \in \bar{V}$, hence $(\bar{c}\bar{a}^2)^n = \bar{c}^n\bar{a}^{2n} \in \bar{V}$. This gives us that $\bar{c}\bar{a}^2 \in Z(\bar{R})$, and since $\bar{c} \neq 0 \in Z(\bar{R})$, we get that $\bar{a}^2 \in Z(\bar{R})$. Therefore $0 = [\bar{a}^2, \bar{b}] = \bar{a}[\bar{a}, \bar{b}] + [\bar{a}, \bar{b}]\bar{a} = 2\bar{a}\bar{c}$. By Remark 0, $\bar{R}$ has no 2-torsion. We get, therefore, that $\bar{a}\bar{c} = 0$ and so $\bar{a} = 0$. This clearly contradicts that $\bar{c} = [\bar{a}, \bar{b}] \neq 0$. We showed now that $c = [a, b]$ must be nilpotent, hence is in Z. Thus $[K, K] \subset Z$.

We get some information on $A(M)$ now.

LEMMA 3. *If $x \in A(M)$, then $x - x^* \in Z$.*

PROOF. If $[K, K] = 0$, since R is generated by K we would be done. Suppose, then, that $[K, K] \neq 0$. By Lemma 1, $A(M) \neq 0$.

Let $x \neq 0 \in A(M)$ and let $a = x - x^*$. Since $a \in K_0$, $a - a^2p(a) \in Z$ for some polynomial $p(t)$ with integer coefficients. If $b \in K$ by Lemma 2, $ab - ba \in [K, K] \subset Z$. Thus $ab - ba = a^2p(a)b - ba^2p(a) = q(a)(ab - ba)$, where $q(t)$ is the derivative of $t^2p(t)$. Thus $q(a)$ is a multiple of a, hence is in $A(M)$.

If $ab - ba \neq 0$, since it is in Z and is skew, $ab - ba$ generates a nonzero $*$-ideal of R which thus contains M. If $y \neq 0 \in M$ then $y = r(ab - ba) + n(ab - ba)$ where $r \in R$ and n is an integer. Thus, since $q(a) \in A(M)$ and $ab - ba = q(a)(ab - ba)$,

$$\begin{aligned} 0 = yq(a) &= r(ab - ba)q(a) + n(ab - ba)q(a) \\ &= r(ab - ba) + n(ab - ba) = y \neq 0. \end{aligned}$$

With this contradiction we have $ab = ba$ for all $b \in K$. Since K generates R we then have that $a = x - x^*$ must be in Z. This proves the lemma.

We need one more preliminary lemma prior to proving our theorem.

LEMMA 4. *If $a \neq 0$ is in $[K, K]$ and $xa = 0$, then $x \in A(M)$.*

PROOF. By Lemma 2, $0 \neq a \in Z$; since $a^* = -a$, and $a \in Z$, a generates a nonzero $*$-ideal T of R. Then $T \supset M$. But since $xa = ax = 0$, we have $xT = Tx = 0$, hence $xM = Mx = 0$, whence $x \in A(M)$.

We have all the pieces now to prove the theorem.

Proof of the theorem. We may suppose that R is $*$-subdirectly irreducible and generated by K, and that $[K, K] \neq 0$. Since $[K, K] \subset J \subset A(M)$, $\bar{R} = R/A(M)$ is commutative.

We claim that R is 2-torsion free. For, if R has 2-torsion then $2M = 0$ follows. Hence $RM = (2R)M = R(2M) = 0$, and $MR = 0$; that is, $R = A(M)$. By Lemma 3 we then have $x - x^* \in Z$ for all $x \in R$. If $k \in K$ then $2k = k - k^* \in Z$, hence, by remark 3, $k \in Z$. This gives $[K, K] = 0$ in contradiction to $[K, K] \neq 0$. We now have, then, that $K_0 = K$, and our hypothesis on the elements of K_0 holds on all elements of K.

By Lemma 3 and Remark 3, then, all elements in $K \cap A(M)$ are in Z. Since $K \not\subset Z$ we must have that $A(M) \neq R$, and so $\bar{R} = R/A(M) \neq 0$. Note that $\bar{R}$ is also 2-torsion free, for if $2\bar{x} = 0$ in $\bar{R}$ then $2x \in A(M)$ hence $2xM = 0$. But $2M = M$, giving us $xM = 0$; similarly, $Mx = 0$. Thus $x \in A(M)$ whence $\bar{x} = 0$.

Since $[K, K] \neq 0$ and $K \cap A(M) \subset Z$ we have $a, b \in K$, $a \notin A(M)$, $b \notin A(M)$ such that $ab - ba \neq 0$. We claim that the image, $\bar{a}$, of a in $\bar{R}$ is invertible in $\bar{R}$. Since $a - a^2p(a) \in Z$ and $ab - ba \in [K, K] \subset Z$ by Lemma 2, $ab - ba = a^2p(a)b - ba^2p(a) = aq(a)(ab - ba)$ where $q(a) = ap'(a) + 2p(a)$ and $p'(t)$ is the derivative of $p(t)$. If $x \in R$ then $(x - xaq(a))(ab - ba) = 0$; since $ab - ba \neq 0$ is in $[K, K]$, by Lemma 4, $x - xaq(a) \in A(M)$. In $\bar{R}$ this translates into $\bar{a}q(\bar{a}) = 1$, where q is a polynomial with integer coefficients. Thus $\bar{a}$ is indeed invertible in $\bar{R}$.

By the above there is a non-constant polynomial with integer coefficients — in fact $t^2q(t) - t$ will do — which, when evaluated at a, falls in $A(M)$. Let $f(t)$ be such a polynomial of minimal odd degree; then since $f(a) \in A(M)$, $f(a)^* = f(-a)$ is also in $A(M)$, hence $f(a) - f(-a) \in A(M)$. In short, we may assume, since R is 2-torsion free, that $f(a)$ is a polynomial involving only odd powers of

a. Thus $f(a) \in A(M) \cap K \subset Z$. Therefore, $0 = f(a)b - bf(a) = f'(a)(ab - ba)$, where $f'(t)$ is the derivative of $f(t)$, since $ab - ba \in Z$. By Lemma 4, $af'(a) \in A(M)$; since $f'(t)$ is of lower degree than $f(t)$ and $af'(a) \in A(M)$, we easily get that $na \in A(M)$ for some integer $n > 0$. Thus $naM = 0$, and so $a(nM) = 0$. Since $a \notin A(M)$ we conclude that $nM = 0$. By the $*$-irreducibility of R we quickly sharpen this to $pM = 0$ for p some prime, $p \neq 2$, and $\bar{R} = R/A(M)$ is of characteristic p, $p \neq 2$.

Since $a \in K$, $pa \in K$; however, $pa \in A(M)$, hence $pa \in K \cap A(M) \subset Z$. If $k \in K$, by Lemma 2, $[a, k] \in Z$ hence $[a^p, k] = pa^{p-1}[a, k] = a^{p-1}[pa, k] = 0$ since $pa \in Z$. Thus a^p centralizes K; but because K generated R, we can conclude that $a^p \in Z$.

Let $a, b \in K$ be as above, that is, $ab - ba \neq 0$. If $c \in K$, $c \notin A(M)$ is in Z then $c^2a \in K$ and $[c^2a, b] = c^2[a, b] \neq 0$ since $c^2a \notin A(M)$ (using Lemma 4). The argument above then shows that c^2a is invertible in $\bar{R}$, hence $\bar{c}$ in invertible in $\bar{R}$. In short, every skew element in $\bar{R}$ is invertible in $\bar{R}$.

If $\bar{s} \neq 0$ is symmetric in $\bar{R}$ then $\bar{s}\bar{a} \neq 0$ is skew, so is invertible in $\bar{R}$. Therefore $\bar{s}$ is invertible in $\bar{R}$. Since $\bar{a}$ is algebraic over the prime field — for $\bar{a}\bar{q}(\bar{a}) = 1$ — the ring generated by $\bar{a}^2$ over the prime field is finite. Every nonzero element in this ring is symmetric, so is invertible (in this subring). That is, $\bar{a}^2$ generated a finite field. Hence, since the characteristic of $\bar{R}$ is p, $(\bar{a}^2)^{p^n} = \bar{a}^2$ for some $n > 0$. This gives us $(\bar{a}^{p^n} - \bar{a})(\bar{a}^{p^n} + \bar{a}) = 0$; since p is odd, each of $\bar{a}^{p^n} \pm \bar{a}$ is skew, so is invertible or 0. We thus get that $\bar{a}^{p^n} = \bar{a}$ or $\bar{a}^{p^n} = -\bar{a}$. In R this translates into $a^{p^n} + a \in A(M)$ or $a^{p^n} - a \in A(M)$. But since $a^{p^n} + a$ and $a^{p^n} - a$ are skew, we get, via Lemma 3 and Remark 3, that either $a^{p^n} + a \in Z$ or $a^{p^n} - a \in Z$. In either case, since $a^p \in Z$ we are left with $a \in Z$. But then $[a, b] = 0$ contrary to $[a, b] \neq 0$. With this the theorem is proved.

References

1. I. N. Herstein, *Rings with periodic symmetric or skew elements*, Journal of Algebra **30** (1974), p. 144-154.

2. P.-H. Lee, *On primitive rings with involution* (to appear in Journal of Algebra).

University of Chicago, Chicago, Illinois 60637