PACIFIC JOURNAL OF MATHEMATICS
Vol. 57, No. 1, 1975

ON A THEOREM OF BRAUER-CARTAN-HUA TYPE

I. N. HERSTEIN

We shall be concerned here with the nature of subrings of a ring with involution which are invariant with respect to certain combinations of elements. To be more precise, let R be a ring with involution $*$ and suppose that A is a subring of R such that $xAx^* \subset A$ for all $x \in R$. Can we say something definitive about the structure of A? We shall see that if R is semi-prime then we do get a dichotomy of the Brauer-Cartan-Hua type, namely, A must contain a nonzero ideal of R or A must be central.

Considerations of such kind of subrings of R arose in the Ph. D. thesis of P. Lee [2].

In what follows, R will be a semi-prime ring with involution $*$ and A will be a subring of R such that $xAx^* \subset A$ for all $x \in R$.

We begin with

LEMMA 1. *If A does not contain a nonzero ideal of R, then $ab^* = ba$ and $b^*a = ab$ for all $a, b \in A$.*

Proof. Let $a \in A$. Linearize $xax^* \in A$ by replacing x by $x + y$. We get

(1) $xay^* + yax^* \in A$ for all $a \in A$, $x, y \in R$.

In (1) replace x by xb, where $b \in A$. We get

(2) $xbay^* + yab^*x^* \in A$.

However, by (1), since $ba \in A$

(3) $x(ba)y^* + ybax^* \in A$.

Subtracting (3) from (1) gives $y(ab^* - ba)x^* \in A$ for all $x, y \in R$, hence $R(ab^* - ba)R \subset A$.

Since A does not contain a nonzero ideal of R, but $A \supset R(ab^* - ba)R$, we deduce that $R(ab^* - ba)R = 0$. However, since R is semi-prime, we conclude that $ab^* - ba = 0$, and so $ab^* = ba$.

If we use a similar argument, replacing y by yb^*, $b \in A$, in (1) we end up with the other relation, $b^*a = ab$.

From Lemma 1 we can settle the problem for A noncommutative.

LEMMA 2. *If A is noncommutative and $xAx^* \subset A$ for all $x \in R$ then A contains a nonzero ideal of R.*

Proof. Suppose the conclusion of the lemma is false. Then, by

Lemma 1, $ab^* = ba$ for all $a, b \in A$. Suppose that a, b, c are in A. Thus $ab^*c^* = bac^* = bca$. However, since A is a subring of R, and $b, c \in A$, we have $cb \in A$. Therefore $a(cb)^* = (cb)a$, that is, $ab^*c^* = cba$. Comparing these two evaluations of ab^*c^*, we get $(bc - cb)a = 0$, hence $(bc - cb)A = 0$. Because A is not commutative, $bc - cb \neq 0$ for some $b, c \in A$.

Let $W = \{w \in R \mid wA = 0\}$. Since $bc - cb \neq 0$ is in W, $W \neq 0$. If $w \in W$ and $x \in R$, $y \in A$, using (1) we have $xay^* + yax^* \in A$, hence $w(xay^* + yax^*) = 0$. But $wy = 0$ since $y \in A$; thus $wxay^* = 0$, which is to say, $WRAA^* = 0$. Therefore $WRAA^*R = 0$. Now $cb^* = bc$ and $bc^* = cb$, hence $bc - cb = cb^* - bc^* \in AA^*$. But $bc - cb \in W$. This gives that $((bc - cb)R)^2 \subset WRAA^*R = 0$. Since R is semi-prime, we get $(bc - cb)R = 0$, and so $bc = cb$. With this contradiction the lemma is proved.

We now turn our attention to what happens when A is commutative.

LEMMA 3. *If A is a commutative subring of R such that $xAx^* \subset A$ for all $x \in R$, then, if A does not contain a nonzero ideal of R, every element in A must be symmetric.*

Proof. Since A does not contain a nonzero ideal of R, by Lemma 1 $ab^* = ba$ and $b^*a = ab$ for every $a, b \in A$. Since $ab = ba$ we get $(b^* - b)a = 0$ and $b^*a = ab^*$, for all $a, b \in A$. Thus $(b^* - b)A = 0$ and A centralizes A^*. From $((b^* - b)A)^* = 0$ and the fact that A centralizes A^*, we have $(b^* - b)A^* = 0$.

Let $t = b^* - b$. If $x \in R$ then $xtx^* = xb^*x^* - xbx^* \in A^* + A$, hence $txtx^* \in tA^* + tA = 0$. We similarly have $x^*txt = 0$.

Linearize $txtx^* = 0$ on x; the result is $txty^* + tytx^* = 0$ for all $x, y \in R$. Multiply this last relation from the right by txt. Using $x^*txt = 0$ we obtain $txty^*txt = 0$ for all $x, y \in R$, that is, $txtRtxt = 0$. Since R is semi-prime, we get that $txt = 0$ for all $x \in R$, and so $tRt = 0$. The semi-primeness of R then gives us that $t = 0$. Since $t = b^* - b$ we have that $b^* = b$, and so every element in A is symmetric.

We have narrowed the possibilities that need be considered, on the road to our desired result.

LEMMA 4[1]. *Let A be a subring of R which consists of symmetric elements and satisfies $xAx^* \subset A$ for all $x \in R$. Then A is contained in the center of R.*

Proof. Since R is semi-prime with involution, it is a subdirect

[1] The author is grateful to Professor Susan Montgomery for suggestions which improved the proof of Lemma 4.

product of *-prime rings R_α with involution (i.e., if $I^* = I$ is a nonzero ideal of R_α then $Ix = 0$ implies $x = 0$). The image, A_α, of A in R_α satisfies the same property as A. So if we could prove $A_\alpha \subset Z(R_\alpha)$ we would get $A \subset Z(R)$. Thus, without loss of generality, R is *-prime.

Since A consists of symmetric elements, A must be a *commutative* subring of R.

In equation (1) we saw that $xay^* + yax^* \in A$ for all $x, y \in R$, $a \in A$. If $b \in A$, this gives $b(xay^* + yax^*) \in A$. On the other hand, $(bx)ay^* + ya(bx)^* \in A$; since $b^* = b$, this yields that $bxay^* + yax^*b \in A$. Thus we have $b(yax^*) - (yax^*)b = b(xay^* + yax^*) - (bxay^* + yax^*b) \in A$. If $U = RAR$, the ideal generated by A, this last relation translates into $bu - ub \in A$ for all $b \in A$, $u \in U$. In other words, A is a Lie ideal of U.

Since R is *-prime it is semi-prime, hence U is semi-prime. Because A is both a commutative subring and Lie ideal of U, if the characteristic of R is *not* 2, by the proof of Lemma 1.3 of [1], we have A is contained in the center of U. Since U is an ideal in the semi-prime ring R, the center of U is contained in the center of R. Hence we get $A \subset Z$, as desired.

So *we may suppose that R is of characteristic* 2. In this case, the proof of Lemma 1.3 of [1] tells us that if $a \in A$ then $a^2 \in Z$. We claim that $a^2 \neq 0$ for some $a \in A$. If not, $a^2 = 0$ and $(au - ua)^2 = 0$ for $u \in U = RAR$, $a \in A$. Thus $(au)^3 = a(au - ua)^2u = 0$; but then aU is a nil ideal in which every element has cube 0. By Lemma 1.1 of [1] we get, since R is semi-prime, that $aU = 0$. Hence $ARAR = 0$, and so $A = 0$.

Thus there is an element $a \in A$ such that $a^2 = \mu \neq 0$ is in Z^+, the set of symmetric elements of Z. By the *-primeness of R, the nonzero elements of Z^+ are not zero divisors in R. If $x \in R$ then $aax + x^*aa \in A$, (since $a^* = a$), that is, $\mu(x + x^*) \in A$ for all $x \in R$. Since A is commutative and μ is not a zero divisor, we get that $x + x^*$ commutes with $y + y^*$ for all x, y in R.

We claim that $\alpha^* = \alpha$ for all $\alpha \in Z$. For $\alpha x + (\alpha x)^* = \alpha x + \alpha^* x^*$ and $\alpha(x + x^*)$ commute with all $y + y^*$, hence $(\alpha + \alpha^*)x^* = \alpha x + \alpha^* x^* + \alpha(x + x^*)$ commutes with all $y + y^*$. But then it commutes with all combinations of the form $z + z^*$, whence with $(\alpha + \alpha^*)y^*$. This gives $(\alpha + \alpha^*)(xy - yx) = 0$ for all $x, y \in R$. So, if R is not commutative, $\alpha + \alpha^* = 0$, and so $\alpha = \alpha^*$ for all $\alpha \in Z$. Thus $Z = Z^+$.

We may assume that $AZ \subset A$ for $A + AZ$ satisfies the same hypothesis as does A; if it is in Z then so is A in Z. Hence we may suppose $AZ \subset A$.

Localize R at $Z(= Z^+)$. The localization R_Z of R is *-prime and since $A \supset Z$, the localization A_Z of A satisfies the basic hypotheses we have imposed on A. If A_Z is in the center of R_Z, then A is in the center of R. But now, all the nonzero elements of the center of R_Z are invertible in R_Z. Hence, without loss of generality, we may assume that all the nonzero elements of Z are invertible in R.

We claim that every $a \neq 0$ in A is invertible in R. If not, since $a^2 \in Z$, we must have $a^2 = 0$ for some $a \neq 0$ in A. Thus $0 = a^2A = aAa$; but $\mu(x + x^*) \in A$ all $x \in R$ where $\mu \neq 0$ is in Z. This gives $a(x + x^*)a = 0$ for all $x \in R$, that is, $axa = ax^*a$. Since $xax^* \in A$, $0 = a(xax^*)a = axaxa$, whence $(ax)^3 = 0$ for all $x \in R$. By Lemma 1.1 of [1] we get $a = 0$.

Let $0 \neq a \in A$; then $a^2 = \alpha \in Z$. If $F = Z[\beta]$ where $\beta^2 = \alpha$, since Z is a field and $\alpha^* = \alpha$ for all $\alpha \in Z$, we can extend the $*$ of R to $\bar{R} = R \otimes_Z F$. Moreover, $\bar{R}$ is $*$-prime. Furthermore, if $\bar{A} = A \otimes_Z F$, as is easily verified, $\bar{x}\bar{A}\bar{x}^* \subset \bar{A}$ for all $\bar{x} \in \bar{R}$. Therefore, by what we have shown, every element of $\bar{A}$ must be invertible in $\bar{R}$. But $\bar{b} = a \otimes 1 - 1 \otimes \beta$ is in $\bar{A}$ and $\bar{b}^2 = a^2 \otimes 1 - 1 \otimes \beta^2 = \alpha(1 \otimes 1) - \alpha(1 \otimes 1) = 0$. Hence $\bar{b} = 0$ and we get that a was indeed in Z. Thus $A \subset Z$ and the lemma is proved.

The four lemmas combine to prove

THEOREM 1. *Let R be a semi-prime ring with involution $*$ and suppose that A is a subring of R such that $xAx^* \subset A$ for all $x \in R$. Then either A must contain a nonzero ideal of R or A is contained in the center of R.*

We can sharpen the theorem a little in the second possibility, namely when $A \subset Z$. If $A = 0$ there is nothing further to be said. If $a \neq 0$, then, as the lemmas show, if A does not contain a nonzero ideal of R, A must consist of symmetric elements. If $a \neq 0 \in A$ then $axx^* = xax^* \in A \subset Z$. So, if $y \in R$, then $axx^*y = yaxx^* = ayxx^*$, hence $A(yxx^* - xx^*y) = 0$. In case R is $*$-prime this forces $xx^* \in Z$ for all $x \in R$. From this, by commuting with x, we get $xx^* = x^*x$ for all $x \in R$. It is fairly trivial from here to conclude that R satisfies the identities of the 2×2 matrices over a field, so in particular, the standard identity in 4 variables. Thus

THEOREM 2. *Let R be a $*$-prime ring, $A \neq 0$ a subring of R such that $xAx^* \subset A$ for all $x \in R$. If A does not contain a nonzero ideal of R then $A \subset Z$ and R satisfies the standard identity in 4 variables.*

Thus, for general semi-prime rings, if $A \neq 0 \subset Z$ and $xAx^* \subset A$ for all $x \in R$, if A does not contain a nonzero ideal of R, we can get the structure of R, as far as all the $*$-prime ideals P of R which do not contain A.

REFERENCES

1. I. N. Herstein, *Topics in Ring Theory*, Univ. of Chicago Press, 1969.
2. P. H. Lee, Ph. D. Dissertation (Chicago), 1974.

Received June 19, 1974. This work was supported in part by NSF Grant GP 29269 at the University of Chicago.

UNIVERSITY OF CHICAGO