HOUSTON JOURNAL OF MATHEMATICS, Volume 1, No. 1, 1975.

POWERS OF SKEW AND SYMMETRIC ELEMENTS IN DIVISION RINGS

Maurice Chacron and I. N. Herstein[1]

Throughout this paper D will denote a division ring with involution *, and $S = \{x \in D \mid x^* = x\}$ and $K = \{x \in D \mid x^* = -x\}$ will always denote the sets of symmetric and skew elements, respectively, of D. An element $r \in D$ is said to be a *norm* if $r = xx^*$ for some $x \in D$; the set of all norms, N, of D is clearly a subset of S. If Z is the center of D, and if $N \not\subset Z$ then it is known that N generates D [3,11]; if $N \subset Z$ then $[D:Z] \leqslant 4$. If the characteristic of D is not 2 and if $N \subset Z$ then it is trivial that $S \subset Z$.

We shall carry over some results which hold for general division rings to the context of division rings with involution, where, instead of imposing the conditions globally on D we impose them on S or on K.

For instance, it is easy to show that if in a division ring R, $a^m b^n = b^n a^m$, for all $a,b \in R$, and appropriate $m,n > 0$ depending on a and b, then R is a field. We shall show that if we merely insist that $a^m b^n = b^n a^m$ for all $a,b \in S$ then D can be at most 4-dimensional over Z, and all norms in D must be in Z. In particular, if char $D \neq 2$, we get that all the symmetric elements must be central. If $a^m b^n = b^n a^m$ for all $a,b \in K$, we again show that D is 4-dimensional over Z and $a^2 \in Z$ for every $a \in K$.

A result of Faith [2] says that if R is a division ring and $A \neq R$ is a subring of R such that $x^{n(x)} \in A$, $n(x) > 0$, for every $x \in R$, then R is commutative. We shall prove two analogs of this result here. We shall show that if $A \neq D$ is a subring of D and $s^{n(s)} \in A$, $n(s) > 0$, for every $s \in S$ then D is at most 4-dimensional over Z, and $N \subset Z$. If $k^{n(k)} \in A$ for every $k \in K$ we shall show that D is at most 4-dimensional over Z and $k^2 \in Z$ for every $k \in K$.

Recall that an involution on D is said to be of the *first kind* if $\alpha^* = \alpha$ for every α

[1]The research of the first author was supported by RNC A7876. The research of the second author was supported by NSF grant GP 29269.

in Z; otherwise * is said to be of the *second kind.*

We shall consistently use the notation Z for the center of D and Z^+ for $Z \cap S$. If R is a subring of D then Z(R) will denote the center of R and $Z(R)^+ = Z(R) \cap S$. If X is a subset of R, then $C_R(X)$ will be the *centralizer* of X in R; that is $C_R(X) = \{v \in R \mid vx = xv \text{ all } x \in X\}$.

Of crucial importance in some of the arguments that follow will be both the main result and techniques of [4] which treat subdivision rings of D which are invariant with respect to conjugation by the unitary elements of D. By a *unitary element* u we mean an element $u \in D$ such that $uu^* = 1$.

We begin with

LEMMA 1. *Suppose that for every $a,b \in S$ there exists an integer $n = n(a,b) \geqslant 1$ such that $ab^n = b^n a$. Then $N \subset Z$.*

PROOF. Let D_0 be the subdivision ring of D generated by a and b, where $a,b \in S$; then certainly $D_0^* = D_0$. If $s \in D_0 \cap S$ then, for suitable $m > 0$, $n > 0$, $s^m a = as^m$, $s^n b = bs^n$, hence s^{mn} commutes with both a and b, and so must be in $Z(D_0)$. By a result of Chacron [1], all norms in D_0 are in $Z(D_0)$; since a^2 is a norm in D_0, and $b \in D_0$, we get that $a^2 b = ba^2$. If $S \not\subset Z$, then S generates D [3,11], in which case we get that $a^2 \in Z$ for any $a \in S$, since we saw that a^2 centralizes S. But then, directly or by again quoting Chacron's result, we have that $N \subset Z$. If $S \subset Z$ then, since $N \subset S$, we certainly have that $N \subset Z$. Thus, always, $N \subset Z$.

DEFINITION. Let D be any division ring with involution *, and let $A \neq D$ be a subring of D. D is said to be S-*radical* over A if, given $s \in S$, then $s^{n(s)} \in A$ for some $n(s) \geqslant 1$.

If D is S-radical over A it is S-radical over A*, hence over $A \cap A^*$; clearly $A \cap A^*$ is invariant re *. If $s \neq 0 \in A \cap A^*$ and $s = s^*$ then $(s^{-1})^* = s^{-1}$, hence $(s^{-1})^n \in A \cap A^*$; together with $s^{n-1} \in A \cap A^*$ this yields $s^{-1} \in A \cap A^*$. If $x \in A \cap A^*$, then $(xx^*)^{-1} \in A \cap A^*$, hence $x^{-1} = x^*(xx^*)^{-1}$ is in $A \cap A^*$. In other words, $A \cap A^*$ is a subdivision ring of D. So, If D is S-radical over A, we may assume that A *is a subdivision ring invariant re* *.

We proceed to

LEMMA 2. *Let D be any division ring with involution *, and suppose that D is S-radical over $A \neq D$. Suppose that $N \not\subset Z$. Then D is of characteristic p, $p \neq 0$, and,*

given $s \in S$, $s^{p^n} \in A$ for some $n = n(s) \geqslant 0$.

PROOF. Since $N \not\subset Z$, N must generate D, hence $N \not\subset A$, and so $S \not\subset A$. Let $s \in S$, $s \notin A$ and let $Z^+ = Z \cap S$, $F = Z^+(s)$, the field obtained by adjointing s to Z^+. Every element in F is symmetric, so, given $x \in F$, $x^{n(x)} \in F \cap A \neq F$. By a result of Kaplansky [5,9], char $D = p \neq 0$, and either F is purely inseparable over $F \cap A$, or F is algebraic over a finite field.

In this latter case, since $Z^+ \subset F$, we have that Z^+ is algebraic over a finite field. Also, since $s \in F$, s is algebraic over a finite field. Let $d = d^* \in C_D(s) \cap A$; then ds is symmetric and not in A, hence ds is algebraic over a finite field, or ds is purely inseparable over A. If $(ds)^{p^k} \in A$ for some k, then $s^{p^k} \in A$; since s is algebraic over a finite field, $s = (s^{p^k})^q$ for some q, so we would have the contradiction $s \in A$. Therefore, ds is algebraic over a finite field, and so d is algebraic over a finite field for every $d = d^*$ in $C_D(s)$, since $C_D(s)$ is S-radical over $C_D(s) \cap A$. By a result of Herstein and Montgomery [7], $C_D(s)$ must be commutative. Hence $C_D(s)$ is a maximal subfield of D. Since s is algebraic over Z we have that D must be finite-dimensional over Z. However, Z^+ is algebraic over a finite field, and so Z also is; but then D is algebraic over a finite field. By a well-known result of Jacobson [5,8], D is commutative, a contradiction.

Hence s is purely inseparable over $F \cap A$, whence $s^{p^n} \in A$ for some $n \geqslant 0$. This proves the lemma.

The next two lemmas give us results which are very special cases of the more definitive results we shall obtain later. But we need them in their present form in order to obtain our final results.

LEMMA 3. *If Z is infinite and $s \in S$ commutes with t^m for all $t \in S$, where $m > 0$ is a fixed integer, then $s^m \in Z$.*

PROOF. If $\lambda^* = \lambda \in Z$ and $t \in S$ then, by hypothesis, s commutes with $(s + \lambda t)^m = s^m + \lambda(s^{m-1}t + s^{m-2}ts + \ldots + sts^{m-2} + ts^{m-1}) + \lambda^2 q_2(s,t) + \ldots + \lambda^m t^m$. Because $Z \cap S$ is infinite, using a vander Monde determinant argument we get that s commutes with $s^{m-1}t + s^{m-2}ts + \ldots + sts^{m-2} + ts^{m-1}$. However this gives us that $s^m t = ts^m$ for all $t \in S$. If $S \subset Z$ then certainly $s^m \in Z$. On the other hand, if $S \not\subset Z$ then S generated D; but since s^m centralizes S we get that $s^m \in Z$. This proves the lemma.

LEMMA 4. *Suppose that D is S-radical over $A \neq D$, and that Z is infinite. If*

$t^m \in A$ for all $t \in S$, where $m > 0$ is a fixed integer, then $N \subset Z$ and $\dim_Z D \leqslant 4$.

PROOF. Suppose that $N \not\subset Z$. Thus, by the result of Chacron [1], D cannot be S-radical over Z; since D is S-radical over A, A cannot be S-radical over Z. Thus there is an element $a^* = a$ in A such that $a^{m^2} \notin Z$. By Lemma 3, since Z is infinite, there exists a $t \in S$ such that $b = a^m t^m - t^m a^m \neq 0$. By assumption, $b \in A$.

Since Z is infinite, and Z^+ is purely inseparable over A by Lemma 2, $Z^+ \cap A$ is infinite. Let $\lambda = \lambda^* \in Z \cap A$; if $s \in S$ then $(a + \lambda s)^m \in A$, hence $a^m + \lambda(a^{m-1}s + a^{m-2}sa + \ldots + asa^{m-2} + sa^{m-1}) + \lambda^2 q_2(a,s) + \ldots + \lambda^m s^m \in A$. A vander Monde determinant argument using λ's in $Z^+ \cap A$ shows us that $c = a^{m-1}s + a^{m-2}sa + \ldots + asa^{m-2} + sa^{m-1}$ is in A, hence $a^m s - sa^m = ac - ca \in A$. In particular, $a^m t^{m+1} - t^{m+1}a^m \in A$. But $a^m t^{m+1} - t^{m+1}a^m = (a^m t^m - t^m a^m)t + t^m(a^m t - ta^m)$; since $a^m t - ta^m$, t^m are in A, and $a^m t^m - t^m a^m = b \neq 0$ is in A, we have $bt \in A$, and so, $t \in A$.

Thus, if $a^m t^m \neq t^m a^m$, where $t \in S$, we must have $t \in A$. If $t_0 \notin A$ and $t \in A$ are symmetric, as in the argument above, from the fact that $t_0 + \lambda t \notin A$ for $\lambda \in Z^+ \cap A$ we have that a^m commutes with $(t_0 + \lambda t)^m$. Expanding and using the vander Monde determinant argument again gives us that a^m commutes with t^m, where $t = t^* \in A$. Thus a^m commutes with s^m for all $s \in S$, contradicting $b = a^m t^m - t^m a^m \neq 0$ for some $t \in S$. The lemma is thereby proved.

This last lemma allows us to settle the case where D is S-radical over A, and where D is finite-dimensional over Z.

LEMMA 5. *If D is finite-dimensional over Z and is S-radical over A, $A \neq D$, then $N \subset Z$ and $\dim_Z D \leqslant 4$.*

PROOF. If $N \not\subset Z$, by Lemma 2, $s^{p^n} \in A$ for every $s \in S$, where $p = \text{char } D \neq 0$. Also, Z must be infinite, otherwise D is algebraic over a finite field, so must be commutative by Jacobson's theorem.

Our aim is to show that $s^{p^m} \in A$ for $s \in S$, where m is a *fixed* integer.

Since D is finite-dimensional over Z, and hence over Z^+, the degree of inseparability of any element in D over Z^+ is bounded. Hence, if $Z^+ \subset A$, the degree of inseparability of any symmetric element over A is bounded. Thus, by Lemma 2, $s^{p^m} \in A$ for all $s \in S$, where m is a fixed integer. By Lemma 4 we would have the desired result $N \subset Z$.

Now D is S-radical over $A_1 = C_D(Z(A))$, and $A_1 \supset Z$; by the above, if $A_1 \neq D$,

we would have $N \subset Z$. Thus we may assume that $A_1 = D$, which is to say, $Z(A) \subset Z$. If D is finite-dimensional over Z(A), the argument above on the degree of inseparability carries over, and we get $N \subset Z$.

Since $Z^+ \not\subset A$, let $\alpha^* = \alpha \in Z$, $\alpha \notin A$, and let D_0 be the subdivision ring generated by A and α. D_0 is S-radical over $A \neq D_0$. Since A is finite-dimensional over Z(A) and $\alpha^m \in A \cap Z \subset Z(A)$, D_0 is finite-dimensional over Z(A). By the argument above, all norms in D_0 are central; hence A is S-radical over Z(A). But because D is S-radical over A, we get that D is S-radical over $Z(A) \subset Z$. By [1] we have that $N \subset Z$. This proves the lemma.

DEFINITION. If D is any division ring with involution, $W = \{ w \in D \mid ws^n = s^n w, n = n(s,w) \geqslant 1, \text{ for all } s \in S \}$.

We prove

LEMMA 6. *If $N \not\subset Z$ and $w = w^*$ is in W, then $w \in Z$.*

PROOF. Let $w = w^* \in W$ and $s \in S$, and let D_1 be the subdivision ring of D generated by w and s. If $ws \neq sw$ then D_1 is S-radical over $C_{D_1}(w) \neq D_1$. If $t \in C_{D_1}(s)$ is symmetric then, since $t^n w = wt^n$ for some n, t^n commutes with w and s, so is in $Z(D_1)$. This implies that all norms in $C_{D_1}(s)$ are central there, and since s is algebraic over $Z(D_1)$, D_1 is finite-dimensional over $Z(D_1)$. By Lemma 5, all norms in D_1 are in $Z(D_1)$, hence $s^2 w = ws^2$. In short, $s^2 w = ws^2$ for *all* $s \in S$. Since $N \not\subset Z$, then $\{ s^2 \mid s \in S \}$ generates D, and so $w \in Z$ follows.

If D is S-radical over A, $A \neq D$, and $N \not\subset Z$, by considering D_1, the subdivision ring generated by z, z^* and s, where $z \in Z(A)$, $s \in S$, $sz \neq zs$, using the argument in the preceding lemma we get $s^2 z = zs^2$, so again $z \in Z$. This is

LEMMA 7. *If D is S-radical over A, $A \neq D$ and $N \not\subset Z$ then $Z(A) \subset Z$.*

We can now dispose of the case in which D is of characteristic 2.

LEMMA 8. *If char D = 2 and D is S-radical over A, $A \neq D$, then $N \subset Z$.*

PROOF. Suppose that $N \not\subset Z$. Let $s \in S$, $s \notin A$ such that $s^2 \in A$. So, $sAs = sAs^{-1}$ is a subdivision ring of D invariant re *. Similarly, $(1 + s)A(1 + s)$ and $s(1 + s)As(1 + s)$ are subdivision rings of D invariant re *. Let $B = A \cap sAs \cap (s+1)A(s+1) \cap s(s+1)As(s+1)$. Then $s \notin B$ but $sBs^{-1} = B$ and $(s+1)B(s+1)^{-1} = B$ since s^2 and $(1+s)^2 = 1+s^2$ are in A. This forces s to centralize B, hence $B \subset C_D(s)$.

Let $C_1 = sAs \cap (s+1)A(s+1) \cap s(s+1)As(s+1)$; then C_1 is S-radical over

$C_1 \cap A = B$, hence s commutes with a power of every symmetric element in C_1. Because $s^2 \in C_1$, using Lemma 6, we obtain $s^4 \in Z(C_1)$; using the form of C_1 we get s^4 is in the center of $A \cap sAs \cap (s+1)A(s+1)$. Let $C_2 = sAs \cap (s+1)A(s+1)$ since C_2 is S-radical over $A \cap C_2 \subset C_D(s^4)$, and $s^4 \in C_2$, by Lemma 6, again, $s^8 \in Z(C_2)$. This gives us that s^8 is in the center of $A \cap s(s+1)As(s+1)$. Let $C_3 = s(s+1)As(s+1)$; C_3 is S-radical over $A \cap C_3$, so s^8 commutes with a power of every symmetric element in C_3; since $s^8 \in C_3$, we get by Lemma 6 that $s^{16} \in Z(C_3)$. This gives us that s^{16} is, in fact, in $Z(A) \subset Z$.

Thus we have shown that if $s \in S$, $s \notin A$ but $s^2 \in A$ then $s^{16} \in Z$. Using Lemma 2, we see from this above remark that if $s \in S$, $s \notin A$ then $s^{2^r} \in Z$ for some appropriate r.

Let $s \in S$, $s \notin A$, $s^{2^r} \in Z$, and consider $C_D(s)$; $C_D(s)$ is S-radical over $A \cap C_D(s)$. For any $d = d^* \in C_D(s) \cap A$, $sd \notin A$ hence $(sd)^{2^k} \in Z$ for some k; because $s^{2^r} \in Z$, we get that $d^{2^{k+r}} \in Z$. Hence $C_D(s)$ is S-radical over Z, so by [1] is 4-dimensional, at most, over $Z(C_D(s))$. Since s is algebraic over Z, D must be finite-dimensional over Z. Lemma 5 then gives us the result $N \subset Z$.

Having disposed of the case char $D = 2$, we can now concentrate on the case char $D \neq 2$.

LEMMA 9. *If char $D \neq 2$ and D is S-radical over A, $A \neq D$, where A is finite-dimensional over $Z(A)$, then $S \subset Z$.*

PROOF. Since $Z(A) \subset Z$, for any unitary element u in D, $Z(A) \subset B = A \cap uAu^{-1}$, so $[B:Z(B)] \leqslant [A:Z(A)]$, with equality holding if and only if $uAu^{-1} = A$. Now D is also S-radical over uAu^{-1}, so D is S-radical over B.

Pick $A \neq D$ of lowest possible dimension over Z(A) such that D is S-radical over A. By the above, $uAu^{-1} = A$ for all unitary u in D. Since $\dim_Z D = \infty$, by [4], either $A = D$ or $A \subset Z$. Since $A \neq D$, we have $A \subset Z$, hence D is S-radical over Z. By the result of Chacron [1], $S \subset Z$ follows.

COROLLARY. *If char $D \neq 2$ and D is S-radical over a commutative subring then $S \subset Z$.*

This corollary is a result of Loustau [10].

We now want to show that A contains a substantial part of the center of D. *We assume that* char $D \neq 2$ *from now to Theorem 1.*

LEMMA 10. *If D is S-radical over A, $A \neq D$, and if $S \not\subset Z$ then $A \supset Z^+$.*

PROOF. If Z^+ is finite then, since Z^+ is purely inseparable over $Z^+ \cap A$ by Lemma 2, Z^+ must be contained in A.

If Z^+ is infinite then, since Z^+ is purely inseparable over $Z^+ \cap A$, $Z^+ \cap A$ must be infinite. By Lemma 5, D must be infinite-dimensional over Z, hence there is a $k \in K$ such that $k^2 \notin Z$. By Lemma 6 there is an $s \in S$ such that $ks^n \neq s^n k$ for all $n > 0$.

Pick $0 \neq \alpha^* = \alpha \in Z^+ \cap A$ such that $\alpha^2 \neq 1$. If $0 \neq \beta \in Z^+$, the elements $u = (1-k)^{-1}(1+k)$, $v = (1-\alpha k)^{-1}(1+\alpha k)$ and $w = (1-\beta k)^{-1}(1+\beta k)$ are all unitary. Hence there exists an integer $m > 0$ such that s^m, $us^m u^{-1}$, $vs^m v^{-1}$, and $ws^m w^{-1}$ are all in A. Following the argument of Lemmas 1 and 2 in [4] we get, where $b = (ks^m - s^m k)^{-1}$, $c = ((\alpha k)s^m - s^m(\alpha k))^{-1} = \alpha^{-1} b$, that:

1. $b - kbk \in A$,
2. $\alpha^{-1} b - (\alpha k)(\alpha^{-1} b)(\alpha k) = c - (\alpha k)c(\alpha k) \in A$.

Hence, since $\alpha^2 - 1 \neq 0 \in A \cap Z$, we get that $b \in A$ from (1) and (2). Thus $b^{-1} \in A$, which is to say, $ks^m - s^m k \in A$.

Similarly, $\beta(ks^m - s^m k) = (\beta k)s^m - s^m(\beta k)$ is in A. Since $ks^m - s^m k \neq 0$ is in A we get from this that $\beta \in A$. Hence $A \supset Z^+$.

COROLLARY 1. *If D is S-radical over A, $A \neq D$, and if $s \in S$ is not in Z, then all the symmetric elements in $C_D(s)$ are in $Z(C_D(s))$.*

PROOF. Since D is infinite-dimensional over Z and $A \not\subset Z$, by [4] there exists a unitary element $u \in D$ such that $t = usu^{-1} \notin A$. Thus, to prove the corollary, we may assume that $s \in A$.

Now $s \in Z(C_D(s))^+$ but $s \notin A \cap C_D(s) = A_1$. Since $C_D(s)$ is S-radical over A_1, and $Z(C_D(s))^+ \not\subset A_1$, by Lemma 10 we must have that all symmetric elements in $C_D(s)$ are in $Z(C_D(s))$, the center of $C_D(s)$.

COROLLARY 2. *If D is S-radical over A, $A \neq D$, and if $k \in K$ then, if $xk^n = k^n x$ for some $n > 0$, we must have $xk^2 = k^2 x$.*

PROOF. If $k^2 \in Z$ then, of course, the result is correct. If $k^2 \notin Z$ then, as in the argument of Corollary 1, we may assume that $k^2 \notin A$.

Now $C_D(k)$ is S-radical over $A_1 = A \cap C_D(k)$ and $A_1 \neq C_D(k)$. Moreover, $k^2 \in Z(C_D(k))$ but $k^2 \notin A_1$. By Lemma 10, all the symmetric elements in $C_D(k)$ must be in $Z(C_D(k))$. But k, which is skew, is also in $Z(C_D(k))$; thus we have that $C_D(k)$ is a

field, so must be a maximal subfield of D.

Since $C_D(k) \subset C_D(k^n)$ and is a maximal subfield of $C_D(k^n)$, and since $k^n \in Z(C_D(k^n))$, $C_D(k^n)$ must be finite-dimensional over $Z(C_D(k^n))$. By Lemma 5, $S \cap C_D(k^n) \subset Z(C_D(k^n))$, hence $k^2 \in Z(C_D(k^n))$. Since $x \in C_D(k^n)$ we get that $xk^2 = k^2x$, as claimed in the corollary.

COROLLARY 3. *If D is S-radical over A, $A \neq D$, and if $k \in K$ is such that k^2 commutes with a^m, for some $m = m(a) > 0$, for every skew element $a \in A$, then $k^2 \in Z$.*

PROOF. If $S \subset Z$ then, since $k^2 \in S$, we would certainly have $k^2 \in Z$.

On the other hand, if $S \not\subset Z$, by Lemma 9, A must be infinite-dimensional over Z(A), hence A must be generated by $\{ a^2 \mid a^* = -a \in A \}$. By Corollary 2, k^2 commutes with a^2 for every skew a in A, thus k^2 centralizes A. Hence $k^2 \in W$; by Lemma 6, $k^2 \in Z$.

We have all the necessary pieces to prove our first theorem.

THEOREM 1. *If D is S-radical over A, $A \neq D$, then $N \subset Z$ (and so, $\dim_Z D \leqslant 4$).*

PROOF. If char D = 2 this is merely Lemma 8. So we may assume that char $D \neq 2$.

Suppose that $S \not\subset Z$. If $k \in K$, $k^2 \notin Z$ by Corollary 3 above there is an $a^* = -a$ in A such that k^2 commutes with no power of a. If $u = (1-k)^{-1}(1+k)$, $v = (1-k-a)^{-1}(1+k+a)$, $w = (1-k+a)^{-1}(1+k-a)$, since these are unitary, $ua^{2m}u^{-1}$, $va^{2m}v^{-1}$ and $wa^{2m}w^{-1}$ are all in A for some $m > 0$. As in the proof of Lemmas 1 and 2 and the first part of the proof of the theorem in [4], we get $ka^{2m} - a^{2m}k \in A$.

Since $k^2a \neq ak^2$, by Corollary 2 above a commutes with no power of k. But $k^{2q} \in A$ for some $q > 0$ and k^{2q+1} is skew. So there is an $n > 0$ such that $k^{2q+1}a^n - a^nk^{2q+1} \in A$. Trivially, we can pick m = n; thus $A \ni k^{2q+1}a^n - a^nk^{2q+1} = (k^{2q}a^n - a^nk^{2q})k + k^{2q}(ka^n - a^nk)$. However, k^{2q}, $ka^n - a^nk$ and $0 \neq k^{2q}a^n - a^nk^{2q}$ are all in A, so $(k^{2q}a^n - a^nk^{2q})k \in A$ whence $k \in A$. In other words, if $k \in K$, $k^2 \notin Z$ then k must be in A, and so certainly $k^2 \in A$. If $k^2 \in Z$, since $k^2 \in Z^+$ and $Z^+ \subset A$, by Lemma 10, k^2 must again be in A. But then $k^2 \in A$ for all $k \in K$. However, $\{ k^2 \mid k \in K \}$ generates D. This gives the contradiction A = D. With this the theorem is proved.

With Theorem 1 at our disposal we are able to get a symmetric-element analog,

for division rings, of a general commutativity theorem [6].

THEOREM 2. *Let D be a division ring with involution in which, given $a, b \in S$, there exist integers $m = m(a,b) \geq 1$, such that $a^m b^n = b^n a^m$. Then $N \subset Z$ and $\dim_Z D \leq 4$.*

PROOF. Lemma 1 says that if $N \not\subset Z$ then there is an $s \in S$ such that $A = \{x \in D \mid xs^r = s^r x, \text{ some } r \geq 1\}$ is not all of D. By hypothesis, D is S-radical over A. Hence by Theorem 1, $N \subset Z$.

We now turn to a study of the analogous questions for the skew elements.

DEFINITION. D is K-*radical* over A, $A \neq D$, if for every $k \in K$, $k^{n(k)} \in A$ for some $n(k) \geq 1$.

We now want to study division rings which are K-radical over proper subrings. If D is K-radical over A, and D is *not* a field then we claim that we may assume that $A = A^*$ and that A is a subdivision ring of D. Since D is K-radical over A it is also K-radical over A^*, hence over $A \cap A^*$; thus, without loss, we may assume that $A = A^*$. If A is commutative then D is also K-radical over $\tilde{A}$, the field of quotients of A, and $\tilde{A} \neq D$. If A is not commutative then it must have a skew element $a^* = -a \neq 0$. If $x \neq 0 \in A$ then $xax^* \in A$ is skew, hence $((xax^*)^{-1})^n \in A$ for some n. Together with $(xax^*)^{n-1} \in A$ we have $(xax^*)^{-1} \in A$. This gives us that x is invertible in A. Hence A is a subdivision ring of D. *Thus, in what follows about K-radicality, we may assume that* $A = A^*$ *is a subdivision ring of* D, char $D \neq 2$.

If D is K-radical over A, $A \neq D$, and * is of the second kind, then we easily see that D is S-radical over A. By Theorem 1, $S \subset Z$; since $K = \alpha S$, $\alpha^* = -\alpha \in Z$, we get that D is commutative. In particular, if D is K-radical over A, if $k^* = -k \neq 0 \in K$, $k \notin A$, *then* $C_D(k)$ *is a field and, so, a maximal subfield of* D; for $C_D(k) \neq A \cap C_D(k)$ is radical over $A \cap C_D(k)$ and * is of the second kind on $C_D(k)$, since $k^* = -k \in Z(C_D(k))$.

Henceforth, we assume that the involution on D *is of the first kind.* We now prove

LEMMA 11. *If D is K-radical over Z then $k^2 \in Z$ for all $k \in K$; hence $\dim_Z D \leq 4$.*

PROOF. As we pointed out above, if $a^* = -a \neq 0$ then $C_D(a)$ is a field, and is, in fact, a maximal subfield of D.

Suppose that $a^2 \notin Z$; let $F = Z^+(a^2)$. If $t \in F$ then $t^* = t$, and ta is skew; thus $(ta)^n \in Z$ for some $n \geqslant 1$, and since $a^m \in Z$ for some $m \geqslant 1$. we get that $t^{mn} \in Z$, and so, $t^{mn} \in Z^+$. Since $F \neq Z^+$, by Kaplansky's theorem [9], char $D = p \neq 0$ and either F is purely inseparable over Z^+, or F is algebraic over a finite field. In this latter case, Z^+ must be algebraic over a finite field, hence Z also is. Since K is algebraic over Z, we would have that K is algebraic over a finite field. By [7], D would be commutative.

Hence we must assume that a^2 is purely inseparable over Z, say $(a^2)^{p^n} \in Z$. Since char $D \neq 2$ $p \neq 2$. Thus $b = a^{p^n}$ is skew and $b^2 \in Z$. But $C_D(b)$ is a maximal subfield of D, and $b^2 \in Z$. In consequence, $\dim_Z D \leqslant 4$. Since the involution is of the first kind, it is trivial now that $k^2 \in Z$ for every $k \in K$.

A trivial adaptation of the proof of Lemma 1, making use of Lemma 11, shows

LEMMA 12. *If for all $a,b \in K$, $ab^n = b^n a$ for some $n = n(a,b) \geqslant 1$, then $a^2 \in Z$ for all $a \in K$, and $\dim_Z D \leqslant 4$.*

DEFINITION. $M = \{x \in D \mid xk^n = k^n x \text{ some } n \geqslant 1 \text{ all } k \in K\}$.

We prove a result parallel to that of Lemma 6.

LEMMA 13. *If $\dim_Z D > 4$ then $M \subset Z$.*

PROOF. As we remarked earlier, we may assume that * is of the first kind, otherwise the result follows from Lemma 6. Also $M \neq D$, otherwise $\dim_Z D \leqslant 4$ by Lemma 12.

Clearly M, and $Z(M)$, are invariant with respect to conjugation by the unitary elements of D. Since $Z(M)$ is commutative, and $\dim_Z D > 4$, by [4] we have that $Z(M) \subset Z$; since, trivially, $Z \subset M$, we have $Z(M) = Z$. Also, if $\dim_Z D > 16$, since $M \neq D$, by [4] we would have that $M \subset Z$.

So we may assume that $\dim_Z D \leqslant 16$ and $M \neq Z(M)$. Because * is of the first kind, $\dim_Z D$ is a power of 2, and since $\dim_Z D > 4$, we must have $\dim_Z D = 16$ and $\dim_Z M = 4$. The subring generated by $M \cap K$ is also invariant re the unitaries, and is not in $Z = Z(M)$, hence is all of M, since every proper subdivision algebra of M is commutative. Thus all symmetric elements in M must be in $Z(M) = Z$, exploiting the fact that $\dim_Z M = 4$.

By standard results in the theory of algebras, $D = M \otimes_Z C_D(M)$. $C_D(M)$ is also invariant re the unitaries and is not commutative, otherwise it would be in Z as above; as above, all symmetric elements in $C_D(M)$ must be in Z.

We can find a basis $1, a_1, a_2, a_3$ of M over Z where a_1, a_2, a_3 are skew. Since $a_i \in M$, $a_i k^{n_i} = k^{n_i} a_i$ for any $k \in K$, hence $a_i k^n = k^n a_i$, where $n = n_1 n_2 n_3$, for $i = 1,2,3$; in short, $k^n \in C_D(M)$. But k^{2n} is a symmetric element in $C_D(M)$, so must be in Z. In other words, D is K-radical over Z. By Lemma 11 we get the contradiction $\dim_Z D \leqslant 4$. Hence $M \subset Z$.

COROLLARY 1. *If D is K-radical over A, $A \neq D$, and $\dim_Z D > 4$ then $C_D(A) = Z$.*

PROOF. Since $C_D(A) \subset M$, by the lemma, we must have $C_D(A) \subset Z$. Clearly, $Z \subset C_D(A)$, whence $Z = C_D(A)$.

COROLLARY 2. *If D is K-radical over A, $A \neq D$, and $\dim_Z D > 4$, then $Z(A) \subset Z$.*

PROOF. $Z(A) \subset C_D(A) \subset M \subset Z$.

We sharpen this last corollary to $Z(A) = Z$.

LEMMA 14. *If D is K-radical over A, $A \neq D$, and $\dim_Z D > 4$ then $Z(A) = Z$.*

PROOF. $0 \neq k \in K$ then $k \notin Z$ since * is of the first kind. Hence, by Lemma 13, there is a $t \in K$ such that k commutes with no power of t.

The elements $u_1 = (1-k)^{-1}(1+k)$, $u_2 = (1-k-t)^{-1}(1+k+t)$ and $u_3 = (1-k+t)^{-1}(1+k-t)$ are all unitary. Therefore there is an $n > 0$ such that $t^n \in A$ and $u_i t^n u_i^{-1} \in A$ for $i = 1,2,3$. As in [4], this leads to $tbt \in A$ where $b = (kt^n - t^n k)^{-1}$.

If $0 \neq \alpha \in Z$ then $\alpha^* = \alpha$ and αk is skew and commutes with no power of t. Thus, as above, we can find an n such that *both* $tbt \in A$ and $tct \in A$ where $c = ((\alpha k)t^n - t^n(\alpha k))^{-1} = \alpha^{-1} b$. Since $\alpha^{-1} tbt = tct \in A$ we get that $\alpha^{-1} \in A$ and so $\alpha \in A$. Thus $A \supset Z$. Since we already know that $Z(A) \subset Z$ we get that $Z(A) = Z$.

COROLLARY. *If D is K-radical over A, $A \neq D$, and $\dim_Z D > 4$ then A cannot be finite-dimensional over Z.*

PROOF. By the lemma $Z(A) = Z$. If A is finite-dimensional over Z then $D = A \otimes_Z C_D(A)$. However, by Corollary 1 to Lemma 13, $C_D(A) = Z$. This gives the contradiction $D = A$.

We are now able to prove

THEOREM 3. *If D is K-radical over A, $A \neq D$, then $k^2 \in Z$ for all $k \in K$, and $\dim_Z D \leqslant 4$.*

PROOF. Since, by Theorem 1, the result is correct if char D = 2, we may assume

that char $D \neq 2$. Also, by Theorem 1, we may assume that * is of the first kind. By the corollary above, we may assume that $Z = Z(M)$ and that $\dim_Z A$ is infinite. A is therefore not commutative, hence has skew elements. The argument of Lemma 10 then shows that, given $k \in K$, $t \in K$ then $kt^m - t^m k \in A$ for some $m \geqslant 1$.

If $k \notin A$, since $k^{2r} \in A$ for some r, and since k^{2r+1} is skew, $k^{2r+1}t^n - t^n k^{2r+1} \in A$ for some $n \geqslant 1$. We can pick $m = n$ in such a way that $t^m \in A$. Now $A \ni k^{2r+1}t^n - t^n k^{2r+1} = (k^{2r}t^n - t^n k^{2r})k + k^{2r}(kt^n - t^n k)$ and, since $k^{2r}(kt^n - t^n k) \in A$, we have $(k^{2r}t^n - t^n k^{2r})k \in A$. However, $k \notin A$ and $k^{2r}t^n - t^n k^{2r} \in A$; the net result of this is that $k^{2r}t^n = t^n k^{2r}$. In other words, $k^{2r} \in M$. By Lemma 13, $M = Z$, hence if $k \in K$, $k \notin A$ then $k^{2r} \in Z$ for some $r \geqslant 1$. Consider $C_D(k)$; it is K-radical over $C_D(k) \cap A$. If $s^* = s \in C_D(k) \cap A$ then $ks \notin A$ and is skew, hence $(ks)^{2w} \in Z$ for some $w \geqslant 1$; since $k^{2r} \in Z$ we have $s^{4rw} \in Z$. In other words, $C_D(k) \cap A$ is S-radical over Z. If $b^* = -b$ is in $C_D(k)$ then $b^2 \in C_D(k) \cap S$ hence for some $h \geqslant 1$, $b^{2h} \in C_D(k) \cap A$ is symmetric whence $b^{2hq} \in Z$ for some $q \geqslant 1$. Thus $C_D(k)$ is K-radical over Z; by Lemma 11, $C_D(k)$ is finite-dimensional over its center. Since k is algebraic over Z we have that D is finite-dimensional over Z. By the Corollary to Lemma 14 we have that $\dim_Z D \leqslant 4$. From this we have $a^2 \in Z$ for all $a \in K$. The theorem is completely proved.

We conclude the paper with the skew analog of Theorem 2.

THEOREM 4. *Let D be a division ring in which, given a, $b \in K$, $a^m b^n = b^n a^m$ for some $m = m(a,b) \geqslant 1$, $n = n(a,b) \geqslant 1$. Then $a^2 \in Z$ for all $a \in K$, and $\dim_Z D \leqslant 4$.*

PROOF. If the result were false, by Lemma 12 there would be an element $b \in K$ such that $B = \{x \in D \mid xb^m = b^m x, \text{ some } m \geqslant 1\}$ is not all of D. But D is K-radical over B, by the hypothesis we have put on D. By Theorem 3 we get a contradiction.

REFERENCES

1. Maurice Chacron, *A generalization of a theorem of Kaplansky*, Mich. Math. Journ. 20(1973), 45-54.
2. Carl Faith, *Algebraic division ring extensions*, PAMS 11(1960), 43-53.
3. I. N. Herstein, *Topics in Ring Theory*, University of Chicago Press, 1969.
4. I. N. Herstein, *A unitary version of the Brauer-Cartan-Hua theorem*, Jour. of Algebra 32(1974), 555-560.
5. I. N. Herstein, *Non-commutative Rings*, Carus Monograph No. 15, Math. Assoc. America, Buffalo, N.Y. 1975.

6. I. N. Herstein, *A commutativity theorem* (to appear) Journal of Algebra.
7. I. N. Herstein and Susan Montgomery, *A note on division rings with involution*, Mich. Math. Journ. 18(1971), 75-79.
8. Nathan Jacobson, *Structure of Rings*, Amer. Math. Soc. Colloq. Publ. 37, 1964.
9. Irving Kaplansky, *A theorem on division rings*, Canadian Jour. Math 3(1951), 290-292.
10. J. A. Loustau, *Radical extensions of Jordan rings* Jour. of Alg. 30(1974), 1-11.
11. Susan Montgomery, *Lie structure of simple rings of characteristic 2*, Jour. of Algebra 15(1970), 387-407.

Carleton University
Ottawa (1), Ontario, Canada

University of Chicago
Chicago, Illinois 60637

Received April 28, 1975.