A NOTE ON DIVISION RINGS WITH INVOLUTIONS

I. N. Herstein and Susan Montgomery

There has been much interest recently in questions of the following type: if the symmetric elements of a ring (or algebra) with involutions are subjected to certain conditions, how does this affect the global structure of the ring (or algebra) itself? Samples of results in this vein can be found in S. A. Amitsur [1], W. Baxter and W. Martindale [2], I. N. Herstein [5], Martindale [10], S. Montgomery [11], and M. Osborn [13]. The results we prove here are in the same general direction.

A well-known theorem of Jacobson asserts that a ring R in which $x^{n(x)} = x$ for all $x \in R$, where $n(x) > 1$ is an integer, is commutative [6], [8]. However, if we impose the condition only on the symmetric elements of a ring with involution, the result need no longer be true. For instance, consider the 2-by-2 matrices over a finite field of characteristic not 2, relative to the involution defined by $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^* = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$; here the symmetric elements satisfy the condition stated above, yet the ring is not commutative. Clearly, we could use such rings to build a wider class of rings with the same property. Nonetheless, the result does become true for division rings, as we show below. We also show that an appropriate generalization of the condition $x^{n(x)} = x$ on the symmetric elements of a division ring leads to a complete description of the ring. Further, we obtain a parallel result under the appropriate condition on the skew-symmetric elements.

Let D be a division ring with involution $*$, and let $S = \{x \in D \mid x^* = x\}$ be its set of symmetric elements. Suppose that for each $s \in S$ there exists an integer $n(s) > 1$ such that $s^{n(s)} = s$.

Now if $s^n = s$ and $(2s)^m = 2s$, where $n > 1$ and $m > 1$, then clearly $s^q = s$ and $(2s)^q = 2s$, where $q = (n - 1)(m - 1) + 1 > 1$. Hence $2s = 2^q s^q = 2^q s$, and this implies that $(2^q - 2)s = 0$. In other words, D is of characteristic $p \neq 0$. Let P be the prime field of D; then $P \subset Z$, where Z is the center of D.

LEMMA 1. *Let* $x \in D$ *be such that* $x^*x = xx^*$. *Then* x *is algebraic over* P, *and* $x^{n(x)} = x$ *for some integer* $n(x) > 1$.

Proof. Since $x^*x = xx^*$, we see immediately that $x + x^*$ commutes with x^*x and that both of these commute with x. By our basic hypothesis on S, the elements $x + x^*$ and x^*x are algebraic over P, hence $F = P(x + x^*, x^*x)$ is a finite field. Every element in F commutes with x. If $\alpha = x + x^*$ and $\beta = x^*x$, then $\alpha, \beta \in F$ and $x^2 - \alpha x + \beta = 0$. Therefore x is algebraic over F, and consequently it is algebraic over P. Since $P(x)$ is a finite field, $x^{n(x)} = x$ for some integer $n(x) > 1$.

COROLLARY. *The center* Z *of* D *is algebraic over* P.

Proof. If $z \in Z$, then certainly $z^*z = zz^*$; hence the result follows.

LEMMA 2. *If the characteristic of* D *is not* 2 *and if* $a \in S$ *is such that* $a^2 \in Z$, *then* $a \in Z$.

Proof. Of course, we may assume that $a \neq 0$. Let $b \in S$; then, if $c = ba - ab$, we see that $c^* = -c$ and $ac = -ca$. Since $c^2 \in S$, it must be algebraic over P.

Received July 9, 1970.

Michigan Math. J. 18 (1971).

Therefore c is algebraic over P and so has finite multiplicative order. Since $a \in S$, it also has finite order. From these facts and the relation $ac = -ca$ we immediately get that a and c generate a finite division ring D_0 over P. By Wedderburn's theorem, D_0 is commutative; since $a, c \in D_0$, we obtain $ac = ca$. But $ac = -ca$, from which we deduce that $2ac = 0$. However, the characteristic of D is not 2, and $a \neq 0$; it thus follows that $c = 0$. In other words, a commutes with all the symmetric elements of D.

Now it is known that if $\dim_Z D > 4$, the symmetric elements generate D ([7], [12]). Thus, if $\dim_Z D > 4$, then $a \in Z$. On the other hand, if $\dim_Z D \leq 4$, then D is algebraic over Z, and by the corollary to Lemma 1, Z is algebraic over P. In short, D is algebraic over P. Therefore, if $x \in D$, then $x^{n(x)} = x$ with $n(x) > 1$; by the result of Jacobson [6], [8] mentioned earlier, D is commutative. In this case, a is certainly in Z. The lemma has now been proved.

Our first main result is the following.

THEOREM 1. *Let* D *be a division ring with involution such that each* $s \in S$ *satisfies* $s^{n(s)} = s$ *for some integer* $n(s) > 1$. *Then* D *is commutative. Moreover,* D *is algebraic over the prime field* P.

Proof. If we show that D is algebraic over P, then the theorem follows from the theorem of Jacobson cited earlier. Therefore we set about proving that D is algebraic over P.

If $S \subset Z$, then it is almost trivial to show that $x^*x = xx^*$ for all $x \in D$. By Lemma 1, we see that each x in D is algebraic over P, and the desired conclusion follows.

We may therefore assume that some element $a \in D$ with $a = a^*$ does not lie in Z. We shall show that this is not possible.

Since a is algebraic over P and D is of characteristic $p \neq 0$, a special case of the Skolem-Noether theorem (see [4], for instance) implies that there exists an element $b \in D$ such that $bab^{-1} = a^i \neq a$. Note that if b is of finite multiplicative order, such a relation is not possible, for then a and b generate a finite division ring D_0 over P; by Wedderburn's theorem, D_0 is commutative, and this leads to the contradiction $a = bab^{-1} = a^i \neq a$.

We shall show that in the relation $bab^{-1} = a^i \neq a$ we can replace b by an element c of finite order such that $cac^{-1} = bab^{-1} = a^i \neq a$. This will finish the proof of the theorem.

Applying * to the relation $bab^{-1} = a^i$ and using $a^* = a$, we get the relations $(b^*)^{-1}ab^* = a^i = bab^{-1}$. Thus b^*b commutes with a. Let $\lambda = b^*b$; since $\lambda^* = \lambda$, our hypothesis on S implies that $\lambda^k = \lambda$ for some $k > 1$.

If k is even, then we are done. For if $\mu = \lambda^{k/2}$, then $\lambda = \mu^2 = \mu^*\mu$ and μ commutes with a. Since $b^*b = \lambda = \mu^*\mu$, $(b\mu^{-1})^*(b\mu^{-1}) = 1$. If $c = b\mu^{-1}$, then $c^*c = 1 = cc^*$; hence, by Lemma 1, c is algebraic over P and so has finite order. But, since $\mu a = a\mu$,

$$cac^{-1} = b\mu^{-1}a\mu b^{-1} = bab^{-1} = a^i \neq a,$$

and this we have seen to be impossible. Therefore k cannot be even. In particular, the characteristic of D *cannot* be 2; for if the characteristic of D is 2 and λ is algebraic over $P = GF(2)$, then $\lambda = \lambda^{2^t}$ with $t \geq 1$.

Thus we may assume that whenever $\lambda^k = \lambda$, the exponent k is odd, and furthermore, that the characteristic of D is not 2. A consequence of these reductions is that λ has *even* order.

Suppose that λ is of order $2^v m$, where m is odd and $v \geq 1$. The Sylow decomposition of the cyclic group generated by λ yields that $\lambda = \lambda_1 \lambda_2$, where λ_1 and λ_2 are powers of λ, and where

$$\lambda_1^{2^v} = 1, \quad \lambda_2^m = 1, \quad \lambda_1^* = \lambda_1, \quad \lambda_2^* = \lambda_2.$$

Now $\lambda_2^{m+1} = \lambda_2$; hence $\lambda_2 = \mu^2 = \mu^* \mu$, where $\mu = \lambda_2^{(m+1)/2}$. Let $c = b\mu^{-1}$. Since $b^* b = \lambda = \lambda_1 \lambda_2$,

$$c^* c = \mu^{-1} b^* b \mu^{-1} = \mu^{-1} \lambda_1 \lambda_2 \mu^{-1} = \lambda_1.$$

But then $(c^* c)^{2^v} = 1$; since the characteristic of D is not 2, we can use Lemma 2 repeatedly to obtain that $c^* c \in Z$. But then $c^* c = cc^*$, and so, by Lemma 1, c is algebraic over P. However, this implies that c has finite order; in addition, $cac^{-1} = b\mu^{-1} a \mu b^{-1} = bab^{-1} = a^i \neq a$. As we showed earlier in the proof, this is not possible. The theorem is thereby proved.

We now prove another theorem of a similar sort. This result generalizes, at least for division rings, a result proved in [3].

THEOREM 2. *Let* D *be a division ring with involution, and let* S *be its set of symmetric elements. Suppose that for each* $s \in S$ *there exists an integer* $n(s) > 1$ *such that* $s^{n(s)} - s \in Z$ (*the center of* D). *Then* D *is either commutative or* 4-*dimensional over* Z.

Proof. We shall first show that $S \subset Z$. Let $s \in S$, and let $S^+ = Z \cap S$; clearly, Z^+ is a subfield of Z. Let $K = Z^+(s)$; if $s \notin Z$, then $K \supset Z^+$ but $K \neq Z^+$. Since both $Z^+ = S \cap Z \subset S$ and $s \in S$, every element of K is in S. Hence, for $u \in K$, our hypothesis implies that $u^{n(u)} - u \in Z$ for some $n(u) > 1$. Since $u^{n(u)} - u$ is also in S, $u^{n(u)} - u \in Z^+$. But then every $u \in K$ satisfies a relation of the form $u^{n(u)} - u \in Z^+$. By a theorem of Krasner [9] we see that K is of characteristic $p \neq 0$ and that every element of K is algebraic over the prime field P. Therefore Z^+ is algebraic over P. Since $z \in Z$ satisfies the quadratic equation $x^2 - (z + z^*)x + z^* z = 0$ over Z^+, Z is algebraic over Z^+, and hence Z is algebraic over P.

However, every element of S is algebraic over Z, by assumption; hence every element of S is algebraic over P. The upshot of this is that $s^{m(s)} = s$, for some $m(s) > 1$, for every $s \in S$. By Theorem 1, D is commutative, in contradiction to the existence of an $s \in S$, $s \notin Z$. In short, we have shown that $S \subset Z$.

But then, each $x \in D$ satisfies the quadratic relation $x^2 - (x + x^*)x + x^* x = 0$ over Z, since both $x + x^*$ and $x^* x$ are now in Z. Since D is quadratic over Z, by a standard ring-theoretic theorem [6] the dimension of D over Z is at most 4. This proves the theorem.

We conclude the paper with the skew-symmetric version of Theorem 1.

THEOREM 3. *Let* D *be a division ring with involution* *, *such that for each* $a \in D$ *with* $a^* = -a$ *there exists an integer* $n(a) > 1$ *for which* $a^{n(a)} = a$. *Then* D *is commutative. Moreover,* D *is algebraic over the prime field* P *of* p *elements.*

Proof. As in the case of Theorem 1, we immediately see that D is of characteristic $p \neq 0$. By Theorem 1, we may suppose that $p \neq 2$. Suppose that λ is a symmetric element in the center Z of D. Then, for each $a \in D$ with $a^* = -a$, we have the relation $(\lambda a)^n = \lambda a$. Playing these off against each other, we find that $\lambda^n = \lambda$. Hence every element in $Z \cap S$ is algebraic over the prime field P.

Suppose that there exists an element $\mu \neq 0$ in Z with $\mu^* = -\mu$. If $s \in S$, then $(\mu s)^* = -\mu s$; hence $(\mu s)^t = \mu s$ for some $t > 1$. Since $\mu^* = -\mu$, our hypothesis implies that $\mu^r = \mu$ for some $r > 1$. If we use $k = (r - 1)(t - 1) + 1$, the two relations $\mu^k = \mu$ and $(\mu s)^k = \mu s$ are satisfied. Together, they imply that $s^k = s$, for every $s \in S$. In that case, Theorem 1 is applicable and gives the commutativity of D.

Hence we may suppose that $\mu^* \neq -\mu$ for $\mu \neq 0$ in Z; that is, $\mu^* = \mu$ for all $\mu \in Z$. Consequently, Z is algebraic over P.

If $a^* = -a$, then $a^{n(a)} = a$, hence $a^{n(a)-1} \in Z$. Let k be the least positive integer with $a^k \in Z$. Since $(a^k)^* = a^k$ and $a^* = -a$, we see that k is even. If $k = 2^r m$, where m is odd, then $(a^m)^{2^r} \in Z$; if $b = a^m$, then, since $b^* = -b \neq 0$, $b \notin Z$ and $b^{2^r} \in Z$.

If $r > 1$, let $c = b^{2^{r-1}}$. Then $c^* = c$ and $c^2 \in Z$. Since Z is algebraic over P, c^2 is algebraic over Z; therefore the element c is algebraic over P. If $s \in S$, then $c(cs - sc) + (cs - sc)c = 0$, since $c^2 \in Z$. However, $(cs - sc)^* = -(cs - sc)$, whence $(cs - sc)^t = cs - sc$ for some $t > 1$. But then c and $cs - sc$ generate a finite division ring over P; by Wedderburn's theorem, this ring is commutative. As before, since $p \neq 2$, we find that $cs = sc$ for all $s \in S$. Therefore c centralizes S.

Now, if $\dim_Z D > 4$, then S generates D [7], and therefore $c \in Z$. On the other hand, if $\dim_Z D \leq 4$, then D is algebraic over P, since Z is algebraic over P. By Jacobson's theorem, we conclude that D is commutative.

Thus we have shown that if $b^{2^r} \in Z$ with $r > 1$, then $c = b^{2^{r-1}} \in Z$. In other words, we have reduced the proof to the case $b^2 \in Z$. We want to show that $b \in Z$.

Since $b^* = -b$, we see that $(bd - db)^* = -(bd - db)$ for each $d \in D$ satisfying $d^* = -d$; hence, by our basic hypothesis, the relation $(bd - db)^t = bd - db$ holds for some $t > 1$. But since $b^2 \in Z$, $b(bd - db) + (bd - db)b = 0$. As before, this allows us to conclude that $bd = db$ for each skew-symmetric d in D.

However, if $\dim_Z D > 4$, then the skew elements generate D [7], in which case we obtain that $b \in Z$. Since $b^* = -b$, and since we have seen that we may suppose that Z contains no skew elements, this is not possible. Thus $\dim_Z D \leq 4$. This forces D to be commutative. In short, we have proved the theorem.

One can wonder about the analogue of Theorem 2 for the skew-symmetric case; that is, suppose that $a^{n(a)} - a \in Z$ for all a with $a^* = -a$. It seems likely that this should imply that $\dim_Z D \leq 4$. However, to settle this will require certain types of purely field-theoretic results. We hope to return to this in a later paper.

REFERENCES

1. S. A. Amitsur, *Rings with involution.* Israel J. Math. 6 (1968), 99-106.
2. W. E. Baxter and W. S. Martindale, III, *Rings with involution and polynomial identities.* Canad. J. Math. 20 (1968), 465-473.
3. I. N. Herstein, *A generalization of a theorem of Jacobson.* Amer. J. Math. 73 (1951), 756-762.
4. ———, *Wedderburn's theorem and a theorem of Jacobson.* Amer. Math. Monthly 68 (1961), 249-251.
5. ———, *Special simple rings with involution.* J. Algebra 6 (1967), 369-375.
6. ———, *Noncommutative rings.* Carus Monograph, no. 15. The Mathematical Association of America, 1968.
7. ———, *Topics in ring theory.* Mathematics Lecture Notes, University of Chicago, 1969.
8. N. Jacobson, *Structure theory for algebraic algebras of bounded degree.* Ann. of Math. (2) 46 (1945), 695-707.
9. M. Krasner, *The non-existence of certain extensions.* Amer. J. Math. 75 (1953), 112-116.
10. W. S. Martindale, III, *Rings with involution and polynomial identities.* J. Algebra 11 (1969), 186-194.
11. M. Susan Montgomery, *Polynomial identity algebras with involution.* Proc. Amer. Math. Soc. (to appear).
12. ———, *Lie structure of simple rings of characteristic* 2. J. Algebra 15 (1970), 387-407.
13. J. M. Osborn, *Jordan algebras of capacity two.* Proc. Nat. Acad. Sci. U.S.A. 57 (1967), 582-588.

University of Chicago
Chicago, Illinois 60637
and
DePaul University
Chicago, Illinois 60614