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).