Can. J. Math., Vol. XXVII, No. 5, 1975, pp. 1114–1126

STRUCTURE OF A CERTAIN CLASS OF RINGS WITH INVOLUTION

M. CHACRON, I. N. HERSTEIN, AND S. MONTGOMERY

Introduction. Let R be a ring with involution $*$, and let Z denote the center of R. In R let $S = \{x \in R | x^* = x\}$ be the set of symmetric elements of R. We shall study rings which are conditioned in the following way: given $s \in S$, then for some integer $k = k(s) \geqq 1$ and some polynomial $p(t)$, with integer coefficients which depend on s, $s^k - s^{k+1}p(s) \in Z$. What can one hope to say about such rings? Certainly all rings in which every symmetric element is nilpotent fall into this class. However, even in this particular case, it is open whether or not every element of the ring must be nilpotent [**12**]. Furthermore, even if we imposed the above condition on all elements of R, we would run into the problem of the structure of nil rings, a problem about which virtually nothing is known. Clearly, then, if we are to obtain any information about the rings in question, we must condition the situation a little more. One such extra condition which we shall impose is that the $k(s)$ above be bounded over S. In that case, satisfactory structure theorems can be obtained.

For example, for the case in which every symmetric element is periodic, in the sense that $s^{n(s)} = s$, $n(s) > 1$ for every $s \in S$, Montgomery has obtained a description of the rings [**13**; **14**]. In case $s - s^2p(s) \in Z$, with some further condition on the nature of $p(s)$, structure theorems were obtained by Burgess and Chacron [**3**].

If R is a semi-simple ring in which $x^n - x^{n+1}p(x) \in Z$ for all $x \in R$, when n is fixed, Chacron [**4**] has shown that R must satisfy a polynomial identity. This naturally leads to the following question: let R be a ring with involution such that $s^k - s^{k+1}p(s) \in Z$ for all $s \in S$ where k is fixed. Does R then satisfy a polynomial identity? We shall show that this is indeed the case. Knowing this, the structure of such rings will be fairly easy to describe.

Fundamental in these discussions will be the following result in linear algebra: let F be a field which is algebraic over a finite field, and let $*$ be an involution on F_n, the ring of $n \times n$ matrices over F. Then, as n goes to infinity, we have symmetric elements in F_n of arbitrarily high index of nilpotence. In fact, as we shall see, no matter what the involution $*$ may be, there is always a symmetric nilpotent element in F_n whose index of nilpotence is at least $[(n-1)/2]$.

Received July 9, 1974 and in revised form, Dec. 16, 1974.

The research of the second author was partially supported by NSF grant GP-2969 at the University of Chicago.

The research of the third author was supported by NSF grant GP-38601 at the University of Southern California.

1. Symmetric nilpotents in matrix rings. The result in this section concerns the symmetric nilpotent elements in F_n, the $n \times n$ matrices over a field F which is algebraic over a finite field. Our aim is to show that as n increases, F_n will contain symmetric nilpotents of ever higher index, regardless of the nature of the involution on F_n. The information we obtain here will be used, in the next section, to determine the nature of rings with involution whose symmetric elements satisfy certain algebraic properties.

We first need the following well-known lemma.

LEMMA 1. *Let $B(x, y)$ be a non-degenerate symmetric or alternate bilinear form on an n-dimensional vector space V over a finite field F. Then there exists a linear transformation on V which is self-adjoint relative to B and is nilpotent of index $\geqq [(n-1)/2]$.*

Proof. It is well-known [**11**, pp. 14-15, 23] that in the alternate case, one has a basis such that the matrix of B has the form

$$\begin{bmatrix} 0 & I_m \\ -I_m & 0 \end{bmatrix}, \quad \text{where } m = \frac{n}{2}.$$

Then the linear transformation whose matrix is

$$\begin{bmatrix} A & 0 \\ 0 & A^t \end{bmatrix}$$

is self-adjoint. Taking A to be nilpotent of index m, we obtain the result in this case.

Now assume B is not alternate. Then it is known that one has a base such that the matrix has the form

$$\begin{bmatrix} S & 0 & 0 \\ 0 & 0 & I_m \\ 0 & I_m & 0 \end{bmatrix},$$

where S is a $k \times k$ symmetric matrix and $k = 0$, 1, or 2. Here the linear transformation with matrix

$$\begin{bmatrix} 0 & & \\ & A & \\ & & A^t \end{bmatrix}$$

is self-adjoint and can be taken to be nilpotent of index m. This proves the lemma.

Our desired result now follows easily from known facts about the possible involutions on F_n. For, first of all, let $\alpha \to \bar{\alpha}$, $\alpha \in F$, denote the restriction of $*$ to F, and let $E = \{f \in F | \bar{f} = f\}$. Then E is a subfield of F, and E_n is a $*$-closed subring of F_n. Thus it will be enough to find symmetric nilpotents of the appropriate index in E_n; that is, we may assume that $*$ is an involution of the first kind.

Now, consider F_n acting as linear transformations on a vector space V of dimension n over F. Then, for any involution $*$ on F_n, it is known [**8**; **10**] that there exists a non-degenerate Hermitian or skew Hermitian scalar product g on V such that $*$ can be identified with the adjoint mapping relative to g. Now by our assumption that $*$ fixes every element of F, g must actually be a symmetric or alternate bilinear form, and thus Lemma 1 applies. We have proved:

THEOREM 1. *Let F be a field algebraic over a finite field. Then for any involution in F_n, F_n will contain a symmetric nilpotent of index at least $[(n-1)/2]$.*

2. Rings with symmetrics satisfying $s^k = s^{k+1}p(s)$. In this section we want to describe the structure of rings with involutions whose symmetric elements are algebraic over the integers in a rather restricted form. To be more precise, we shall be interested in the situation where, given a symmetric element $s \in S$, then $s^k = s^{k+1}p(s)$ with k a fixed integer and $p(x)$ a polynomial with integer coefficients which depend on s. To do so, we must first consider the case where subsets other than S itself are subject to such a condition. This motivates the definition we are about to make.

Definition. An additive subgroup $U \subset R$ is said to satisfy *Condition A* if, given $u \in U$ then $u^k = u^{k+1}p(u)$ where k is a *fixed* integer and $p(x)$ is a polynomial with integer coefficients which depend on u.

We shall refer to the smallest positive integer k, in the definition above, which works for all $u \in U$ as the *A-index* of U.

If, in addition, U is closed with respect to powers, that is, if $u \in U$ then $u^i \in U$ for $i \geqq 1$, we assert that Condition A assumes a much simpler form. We do this now.

Let U be an additive subgroup of R which is closed with respect to powers and which satisfies Condition A. We claim that if $u \in U$ then $u^k = u^{k+n(u)}$ where k is the A-index of U and $n(u) \geqq 1$ is an integer depending on u.

First of all, note that if $u \in U$ is nilpotent then $u^k = 0$; this follows trivially from the fact that $u^k = u^{k+1}p(u)$. Hence for such elements we certainly have $0 = u^k = u^{k+1}$. Suppose, then, that u is not nilpotent. From $u^k = u^{k+1}p(u)$ we easily get that $u^k = u^{2k}q(u)$ where $q(x)$ is a polynomial with integer coefficients. Thus $e = u^kq(u)$ is in U and satisfies $e^2 = e \neq 0$. Moreover, $u^ke = u^k$. Since $e \in U$, $2e$ is also in U, whence $(2e)^k = (2e)^{k+1}h(2e)$ for some polynomial $h(x)$ with integer coefficients. This gives us

$$(2^k - 2^{k+1}h(2))e = 0;$$

since the integer $2^k - 2^{k+1}h(2)$ is not 0, we have that $ne = 0$ for some positive integer n. Thus, since $u^k = u^ke$, $nu^k = nu^ke = 0$. In view of this and the fact that u^k is algebraic over the integers, the subring generated by u^k must be *finite*. But then $u^{ka} = u^{kb}$ for some integers $1 \leqq a \leqq b$. Pick such a relation

https://doi.org/10.4153/CJM-1975-117-8 Published online by Cambridge University Press

with a minimal. Now $u^k q(u) = e$ and $u^k e = u^k$; thus from $u^{ka} q(u) = u^{kb} q(u)$ we obtain, if $a > 1$, that

$$u^{k(a-1)} u^k q(u) = u^{k(b-1)} u^k q(u),$$

which is to say, $u^{k(a-1)} e = u^{k(b-1)} e$. The net result of this is that

$$u^{k(a-1)} = u^{k(b-1)};$$

violating the minimal nature of a. Hence $a = 1$ and $u^k = u^{kb} = u^{k+n(u)}$ for some $n(u) \geqq 1$.

We have shown that Condition A on the U in question really assumes the simpler form:

Condition A': $u \in U$ implies that $u^k = u^{k+n(u)}$, $n(u) \geqq 1$ where k is a *fixed* integer.

LEMMA 2. *Let R be a primitive ring satisfying Condition A. Then R satisfies the standard identity of degree $2k$, where k is the A-index of R.*

Proof. Any subring T of R satisfies Condition A and so does any homomorphic image T' or T. Moreover, the A-index of T' is at most k, the A-index of R. In consequence, any nilpotent element of T' has index of nilpotence at most k. Since R is primitive, using the argument above and the density theorem, we obtain that R is isomorphic to D_{k_1}, the $k_1 \times k_1$ matrices over a division ring D, with $k_1 \leqq k$. D also satisfies Condition A, hence Condition A'; thus in D, $x^{m(x)} = x$ for all x with $m(x) > 1$. By a well-known theorem of Jacobson [**9**], D is a field F and so, by the theorem of Amitsur-Levitzki [**2**], $R = F_{k_1}$ satisfies the standard identity of degree $2k_1$; since $k_1 \leqq k$, R satisfies the standard identity of degree $2k$.

We need an easy, general result about primitive rings which certainly must be known, but for which we could not locate a precise reference. Hence we prove it here.

LEMMA 3. *Let R be a primitive ring; suppose that the right ideal $\rho \neq 0$ satisfies a polynomial identity. Then R has a minimal right ideal.*

Proof. Let $T = \{x \in \rho | x\rho = 0\}$; T is an ideal of ρ and $\bar{\rho} = \rho/T$ is a primitive ring. Since ρ satisfies a polynomial identity, so does $\bar{\rho}$, hence by Kaplansky's theorem $\bar{\rho}$ is a finite-dimensional simple algebra. Thus $\bar{\rho}$ has a minimal right ideal $\bar{\rho}_0 \neq 0$. Let ρ_0 be the inverse image of $\bar{\rho}_0$ in ρ. We claim that $\rho_0\rho$ is a minimal right of R. Since $\bar{\rho}_0 \neq 0$, we have $\rho_0\rho \neq 0$. If $I \neq 0$ is a right ideal of R and $I \subset \rho_0\rho$, the minimality of $\bar{\rho}_0$ in $\bar{\rho}$ gives $I \subset T$ or $I + T = \rho_0$. If $I \subset T$ then $I\rho = 0$, which is not possible, since R is primitive. So, $I + T = \rho_0$. Thus

$$\rho_0\rho = (I + T)\rho = I\rho \subset I \subset \rho_0\rho,$$

that is, $I = \rho_0\rho$. This finishes the proof.

https://doi.org/10.4153/CJM-1975-117-8 Published online by Cambridge University Press

Note that the proof did not use the full force of the fact that ρ satisfies a polynomial identity. *The same proof works if we merely assume that ρ/T has a minimal right ideal.*

We now turn to rings with involution whose symmetric elements, S, satisfy Condition A.

LEMMA 4. *Let R be a primitive ring with involution in which S satisfies Condition A. Then R must satisfy the standard identity of degree $4(k+1)$, where k is the A-index of S.*

Proof. Since S satisfies Condition A, as we have seen, it must satisfy Condition A'; that is, if $s \in S$ then $s^k = s^{k+n(s)}$ where k is the A-index of S, and where $n(s) \geqq 1$.

If there are no non-zero nilpotent elements in S then the relation above implies that $(s - s^{n(s)+1})^k = 0$, hence $s = s^{n(s)+1}$. By a result due to Montgomery [**13**; **14**], we would have that R is at most 4-dimensional over its center, so satisfies the standard identity of degree 4.

Suppose, then, that there exists an element $s \neq 0$ in S such that $s^2 = 0$. Let $B = sR$; if $x \in R$ then $sx^* + xs \in S$, hence

$$(sx^* + xs)^k = (sx^* + xs)^{k+n}$$

where $n \geqq 1$ depends on $sx^* + xs$. Multiplying this on the left by s and on the right by x yields, on using $s^2 = 0$, that

$$(sx)^{k+1} = (sx)^{k+1+n}.$$

Hence the ring B satisfies Condition A with A-index at most $k+1$. If $T = \{x \in B | xB = 0\}$, then B/T is a primitive ring satisfying Condition A; by Lemma 2, B/T must satisfy a polynomial identity, and so B satisfies a polynomial identity. Since B is a right ideal of R, using Lemma 3, we obtain that R has a minimal right ideal.

Since R is a primitive ring with involution having a minimal right ideal, by a result of Kaplansky [**10**, Theorem 1, p. 82], if R is not simple artinian it would contain all infinite matrices of the form $\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$ where x is any matrix in D_n, for any n, over a division ring D. Moreover, the * of R induces an involution on D_n such that $D^* = D$. Since the symmetric elements of D must satisfy Condition A, D must be a field algebraic over a finite field. Since the symmetric elements in D_n which are nilpotent have index of nilpotence at most k, by Theorem 1, we would have the contradiction $n \leqq 2k+2$. Thus R is a simple artinian ring; hence R is isomorphic to some D_t for some division ring D. As we just saw, D must be a field and $t \leqq 2k+2$. Thus R satisfies the standard identity of degree $2t$, hence that of degree $4k+4$. The lemma is proved.

We now prove

THEOREM 2. *Let R be a ring with involution such that S satisfies Condition A.*

Then R must satisfy a polynomial identity. If R is semi-simple then it satisfies the standard identity of degree $4(2k + 1)$.

Proof. Let P be a primitive ideal of R. We divide the argument according as $P^* = P$ or $P^* \neq P$.

If $P^* = P$ then $*$ induces an involution on $\bar{R} = R/P$ which is a primitive ring. Moreover, if $\bar{s}$ is symmetric in $\bar{R}$ then $\bar{s}^2$ is the image of a symmetric element in R, hence $\bar{s}^{2k} = \bar{s}^{2k+1}p(s^2)$. Therefore the symmetric elements of $\bar{R}$ satisfy Condition A, and have A-index at most $2k$. By Lemma 4, $\bar{R}$ satisfies the standard identity of degree $4(2k + 1)$.

If $P^* \neq P$ then $\bar{A} = (P^* + P)/P$ is a non-zero ideal in the primitive ring $\bar{R} = R/P$. If $\bar{x} \in \bar{A}$ then $\bar{x} = \overline{x + x^*}$ where $x \in P^*$; since $x + x^* \in S$ we get $\bar{x}^k = \bar{x}^{k+1}p(\bar{x})$. Since $\bar{A}$ is primitive, Lemma 2 shows that $\bar{A}$ satisfies the standard identity of degree $2k$. Hence $\bar{A}$ must be a finite-dimensional simple algebra; thus $\bar{A}$ has a unit element $\bar{e}$, $\bar{A} = \bar{R}\bar{e} = \bar{e}\bar{R}$. But then $0 \neq \bar{e}$ is a central idempotent in $\bar{R}$. Since $\bar{R}$ is primitive we obtain that $\bar{e} = 1$, hence $\bar{A} = \bar{R}$. Therefore $\bar{R}$ satisfies the standard identity of degree $2k$.

Let $J(R)$ be the radical of R. Since $J(R) = \bigcap P$ over all primitive ideals P of R, by the preceding discussion we see that $R/J(R)$ satisfies the standard identity of degree $m = 4(2k + 1)$. If f denotes this standard identity, then for $s_1, \ldots, s_m \in S$, $b = f(s_1, \ldots, s_m)$ is in $J(R)$. Moreover, since m is divisible by 4, b must be symmetric. Hence $b \in S \cap J(R)$. Thus $b^k = b^{k+1}p(b)$. Because $b \in J(R)$ this last relation forces $b^k = 0$. In other words, S satisfies $f(s_1, \ldots, s_m)^k = 0$. By a result of Amitsur [**1**] we conclude that R satisfies a polynomial identity.

We make a short digression from our central theme. The result we get gives an affirmative answer to a special case of the following open question: If A is an algebra over a field, with involution, all of whose symmetric elements are algebraic, is A itself algebraic?

COROLLARY. *Let R be an algebra with involution over a field F, F algebraic over a finite field. Suppose that the symmetric nilpotent elements in R are of bounded index of nilpotence. Then, if the symmetric elements of R are algebraic over F, R itself must be algebraic over F.*

Proof. Since $s \in S$ is algebraic over F, and F is algebraic over a finite field, s generates a finite ring, hence $s^m = s^n$ with $m > n$. Thus $(s - s^{m-n+1})s^{n-1} = 0$; this gives $(s - s^{m-n+1})^n = 0$. Since $s - s^{m-n+1}$ is a symmetric nilpotent, $(s - s^{m-n+1})^k = 0$, where k is the bound of nilpotence of the symmetric nilpotent elements. Hence $s^k = s^{k+1}p(s)$ where $p(s)$ is a polynomial with integer coefficients. Theorem 2 then tells us that R satisfies a polynomial identity. By a theorem of Montgomery [**15**], since R satisfies a polynomial identity and its symmetric elements are algebraic, R must be algebraic.

3. Some technical lemmas. We shall prove some highly technical and special results now that will enable us to generalize the principal theorem of

Section 2. Many of these results are of a field-theoretic nature; with them in hand we can extend some known results about division rings to domains.

LEMMA 5. *Let $F \neq C$ be an algebraic extension of the field C which is not purely inseparable over C. Suppose that A is a subring of F such that:*

(i) *Given $x \in F$ then $x = a\lambda$ where $a \in A$, $\lambda \in C$.*

(ii) *For any $a \in A$, $a^k - a^{k+1}p(a) \in C$ where k and $p(t)$ depend on a, and $p(t)$ is a polynomial with integer coefficients.*

Then F is algebraic over a finite field.

Proof. Suppose that F is not algebraic over a finite field. Since F is not purely inseparable over C, by a result of [**16**] there exist two non-archimedean valuations v_1 and v_2 on F which coincide on C. Now if v_1 and v_2 coincide on A, since every $x \in F$ is of the form $x = a\lambda$, $a \in A$, $\lambda \in C$ we would get that $v_1(x) = v_2(x)$, contrary to $v_1 \neq v_2$. Thus there is an $a \in A$ such that $v_1(a) \neq v_2(a)$.

We claim that it is impossible that both $v_1(a) < 1$ and $v_2(a) < 1$. For, since $b = a^k + r_1a^{k+1} + \ldots + r_na^{k+n}$ is in C, with r_i integers, we have $v_1(b) = v_2(b)$. Now, on the integers, $v_1(r_i) \leqq 1$, $v_2(r_i) \leqq 1$ and since $v_1(a) < 1$ and the valuation is non-archimedean, $v_1(b) = v_1(a^k) = v_1(a)^k$; for the same reason, $v_2(b) = v_2(a)^k$. But then $v_1(a)^k = v_1(b) = v_2(b) = v_2(a)^k$, giving the contradiction $v_1(a) = v_2(a)$.

This allows us to rule out the case of characteristic 0 immediately. For in this case $v_1 = v_2$ on the integers and induces a p-adic valuation, hence for some integer $m \neq 0$ we can arrange it so that $v_1(ma) < 1$ and $v_2(ma) < 1$. By the above, $v_1(ma) = v_2(ma)$, giving us $v_1(a) = v_2(a)$, a contradiction.

Thus we may suppose that F is of characteristic $p \neq 0$. If $b = a^k + r_1a^{k+1} + \ldots + r_na^{k+1}$ is in C, where the r_i are integers and $r_n \neq 0$ then $v_1(b) = v_2(b)$. If $v_1(a) < 1$, as above, we get $v_1(b) = v_1(a)^k < 1$. Thus $v_2(b) < 1$; now we know that $v_2(a) \geqq 1$. If $v_2(a) > 1$ then $1 > v_2(b) = v_2(r_na^{n+k}) = v_2(a^{n+k}) = v_2(a)^{n+k}$, giving the contradiction $v_2(a) < 1$. The only possibility is $v_2(a) = 1$. Now $v_2(b) = v_1(b) < 1$, hence if $b \neq 0$, $v_1(ab) < 1$ and $v_2(ab) < 1$; by the above, $v_1(ab) = v_2(ab)$ giving us $v_1(a) = v_2(a)$. If $b = 0$ then a is algebraic over $GF(p)$; this would give the contradiction $v_1(a) = v_2(a) = 1$. So $v_1(a) < 1$ is not possible.

If $v_1(a) > 1$ then $v_1(b) = v_1(r_na^{n+k}) = v_1(a)^{n+k} > 1$. Hence $v_2(b) > 1$. But $1 < v_2(b) < \sup\ v_2(r_ia^{k+1})$; this yields that $v_2(a) > 1$. But then $v_2(b) = v_2(r_na^{n+k}) = v_2(a)^{n+k}$, ending up in $v_1(a) = v_2(a)$.

Since $v_1(a) \neq v_2(a)$, without loss of generality $v_1(a) < 1$ or $v_1(a) > 1$, neither of which is possible. This completes the proof.

Recall that a *domain*, commutative or non-commutative, is a ring without zero divisors. We wish to extend a result on division rings, proved in [**6**], to domains. But first we introduce:

Condition B. A subset $A \subset R$ is said to satisfy *Condition B* if, given $a \in A$

then $a^k - a^{k+1}p(a) \in Z$ for some integer k depending on a, and some polynomial $p(t)$. with integer coefficients, depending on a.

LEMMA 6. *Let R be a domain satisfying Condition B. Then R is commutative.*

Proof. Let Z_1 be the subset of non-zero elements of Z If Z_1 is empty then $x^k = x^{k+1}p(x)$ for every $x \in R$; since R is a domain this would yield $xp(x) = 1$, and this would force Z_1 not to be empty. Let $\Delta = RZ_1^{-1} = \{a/\lambda | a \in R, \lambda \in Z_1\}$ be the localization of R with respect to Z_1. It is trivial to verify that Δ is a division ring, and that the center $\bar{Z}$ of Δ is the ring of fractions of Z, the center of R. If $x \in \Delta$ then $x = az^{-1}$, $a \in R$, $z \in Z_1$; since a is algebraic over Z it follows that x is algebraic over $\bar{Z}$. If $R \neq Z$ then $\Delta \neq \bar{Z}$; hence there is an element $x_0 = a_0\lambda_0^{-1}$, $a_0 \in R$, $\lambda_0 \in Z$, which is separable over $\bar{Z}$. Let $F = \bar{Z}(x_0)$ be the subfield of Δ generated by $\bar{Z}$ and x_0. Then F is an algebraic, separable extension of $\bar{Z}$. By the very nature of $x_0 = a_0\lambda_0^{-1}$, $F = \bar{Z}(a_0)$; since $\bar{Z} = ZZ_1^{-1}$, $F = Z(a_0)Z_1^{-1} = A\bar{Z}$ where $A = Z[a_0]$. It is clear, now, that A, $C = \bar{Z}$ and F satisfy the conditions of Lemma 5. Thus F is algebraic over a finite field. But then $\bar{Z}$ is algebraic over a finite field; since Δ is algebraic over $\bar{Z}$, Δ is algebraic over a finite field. By Jacobson's theorem, Δ must be commutative; since $R \subset \Delta$, R is commutative.

We generalize Lemma 6 to the case of rings with involution.

LEMMA 7. *Let R be a domain with involution and suppose that S, the symmetric elements of R, satisfies Condition B. Then all elements of the form xx^* and $x + x^*$ are in the center of R. (So, if the characteristic of R is not 2, $S \subset Z$).*

Proof. Let $Z^+ = Z \cap S$ and let Z_1^+ be the set of non-zero elements in Z^+. Localizing R at Z_1^+ it is easy to see that we get a division ring Δ all of whose symmetric elements are algebraic over the center, $Z(\Delta)$, of Δ. If every symmetric element in Δ is purely inseparable over $Z(\Delta)$, then the conclusion we desire follows from [**5**, Theorem 4]. If some $s \in \Delta$, $s^* = s$, $s \notin Z(\Delta)$ is separable over $Z(\Delta)$, then let F be the subfield obtained by adjoining s to the subfield $Z(\Delta)^+$ of symmetric elements of $Z(\Delta)$. If $x \in F$, $x = a\lambda^{-1}$, $a \in S$, $\lambda \in Z_1^+$; so, if $A = F \cap S$, A is a subring of R, lies in F and $F = AZ(\Delta)^+$. These subrings satisfy the conditions of Lemma 5, hence F is algebraic over a finite field. Thus, $Z(\Delta)^+$, whence $Z(\Delta)$, is algebraic over a finite field. But Δ is algebraic over $Z(\Delta)$. By Jacobson's theorem, we get that Δ is commutative, hence R is. With this contradiction the lemma is proved.

Recall that a ring R with involution is **-prime* if $AB = 0$, $A^* = A$, $B^* = B$ ideals of R implies that $A = 0$ or $B = 0$.

We are now ready to prove.

LEMMA 8. *Let R be a *-prime ring whose symmetric elements satisfy Condition B. Suppose that R has no non-trivial symmetric idempotents. If the symmetric nilpotent elements of R are of bounded index of nilpotence, then all $x + x^*$ and xx^* are in the center of R. (In particular, if* char $R \neq 2$, *then $S \subset Z$).*

https://doi.org/10.4153/CJM-1975-117-8 Published online by Cambridge University Press

Proof. Before proving the lemma, note that the condition that symmetric nilpotents be of bounded index is automatically satisfied in domains, and in rings where, in Condition B, the integer $k = k(s)$ is bounded.

If $s \in S$ is a zero divisor then $s^k - s^{k+1}p(s) \in Z$ is also a zero divisor. By the *-primeness of R this yields that $s^k = s^{k+1}p(s)$, and so $s^k = 0$ or $s^kq(s)$ is a non-zero idempotent for some polynomial $q(s)$ with integer coefficients. Since there are no non-trivial symmetric idempotents, we have $s^k = 0$ or s is invertible; s is not invertible, so $s^k = 0$. Thus any symmetric element is regular or nilpotent of index k.

Localize R at $Z^+ = Z \cap S$. The ring R_1 we obtain is *-prime and every symmetric element is nilpotent of index k or invertible. R_1 must be semi-simple, for any symmetric element in its radical is nilpotent of index k; as is well known, this gives rise to a nilpotent ideal. Thus we can invoke Theorem 7 of [7] to obtain that R_1 is an order in the 2×2 matrices over a field relative to the symplectic involution, a division ring, or the direct sum of a division ring and its opposite. If R_1 is the 2×2 matrices with symplectic involution, all xx^* and $x + x^*$ are central in R_1, hence certainly also in R. If R_1 is a division ring, R is a domain; by Lemma 7 the result follows. Finally, if R_1 is a direct sum of a division ring and its opposite, R is a subdirect sum of a domain and its opposite, and furthermore this domain satisfies Condition B. By Lemma 6, this domain is commutative, hence R is commutative. This finishes the proof.

4. The objective of this final section is to describe the structure of rings with involution which satisfy Condition B in a bounded form. To do so, we first need a result which parallels that of Lemma 8.

LEMMA 9. *Let R be a *-prime ring whose symmetric elements satisfy Condition B, with k bounded* (i.e., *for a fixed integer k, $s^k - s^{k+1}p(s) \in Z$ for all $s \in S$*). *Suppose that R does not satisfy Condition A. Then all $x + x^*$ and xx^* are in the center of R. In particular, R is quadratic over Z and satisfies the standard identity of degree* 4.

Proof. We claim that R cannot contain a non-trivial symmetric idempotent. For suppose that $e^2 = e = e^*$ and $e \neq 0, 1$. If $\lambda \neq 0$ is a symmetric element in Z, then λe is symmetric, hence satisfies $(\lambda e)^k - (\lambda e)^{k+1}p(\lambda e) \in Z$. But $(\lambda e)^k - (\lambda e)^{k+1}p(\lambda e) = (\lambda^k - \lambda^{k+1}p(\lambda)e$ is then a symmetric zero divisor in Z; by the *-primeness of R we conclude that $\lambda^k = \lambda^{k+1}p(\lambda)$, and so $1 = \lambda p(\lambda)$. Since the coefficients of $p(\lambda)$ are integers, and this holds for all $\lambda^* = \lambda$ in Z, we get that λ is algebraic over a finite field, hence $\lambda^{n(\lambda)} = \lambda$ for some $n(\lambda) > 1$. If $s \in S$ then $\lambda = s^k - s^{k+1}p(s)$ is a symmetric element of Z, hence by the above, $s^k - s^{k+1}p(s) = (s^k - s^{k+1}p(s))^{n(\lambda)}$. This gives $s^k = s^{k+1}q(s)$ for some polynomial $q(x)$ with integer coefficients. In short, R would satisfy Condition A, a contradiction. Thus R has no non-trivial symmetric idempotents. Also, if $s \in S$ is nilpotent then since $s^k - s^{k+1}p(s) \in Z$ we quickly get, since this is a zero divisor, that $s^k = s^{k+1}p(s)$ and so $s^k = 0$. Thus the nilpotent symmetric

elements in R are of bounded index of nilpotence. Thus R satisfies the hypotheses of Lemma 8; therefore we have that xx^* and $x + x^*$ are all in Z.

Since $x^2 - (x + x^*)x + x^*x = 0$, R is quadratic over Z. Since R is semiprime we immediately have that R satisfies the standard identity of degree 4.

We now come to the final theorem of the paper.

THEOREM 3. *Let R be a *-prime ring whose symmetric elements satisfy $s^k - s^{k+1}p(s) \in Z$, where k is a fixed integer and $p(x)$ is a polynomial with integer coefficients which depend on s. Then R is one of the following types:*

(1) *an order in a simple algebra of dimension at most 4 over its center;*

(2) *an order in the direct sum of a field with itself, where $*$ is the exchange involution;*

(3) *F_n, the ring of $n \times n$ matrices over a field F which is algebraic over a finite field, with $n \leqq 2(k + 1)$; or*

(4) *the direct sum of F_n with itself, F as in Part 3, with $n \leqq k$, relative to the exchange involution.*

Proof. If R does *not* satisfy Condition A, by Lemma 9 R satisfies the standard identity of degree 4. If R is prime, by Posner's theorem R must be an order in a simple algebra of dimension at most 4 over its center. If R is *not* prime, then it contains a prime ideal $P \neq 0$ such that $P \cap P^* = 0$. Since, by Lemma 9, all $x + x^* \in Z$, we immediately get from $P \cap P^* = 0$ that P must be contained in Z, and so $P + P^*$ is a commutative *-ideal of R and lies in Z. But then the *-primeness of R forces R to be commutative, and R is an order in $F \oplus F$ where F is the field of quotients of R/P. In other words, if R satisfies Condition B but not Condition A then it is either of type 1 or 2 in the assertion of the theorem.

Suppose then that R satisfies Condition A. If R is prime then, by Theorem 2 it satisfies a polynomial identity so, by Posner's theorem, R must be an order in a simple algebra Q which is finite-dimensional over its center C, and $Q = RC$. Moreover, by a result of Rowen [**17**], the center C of Q is the field of quotients of the center Z of R. But if $\lambda \neq 0$ is in Z, we saw that $\lambda^{n(\lambda)} = 1$ for some $n(\lambda) > 1$, hence $\lambda^{-1} \in Z$. Thus $C = Z$, and so, $Q = R$. Since Z is algebraic over a finite field we get that R is isomorphic to F_n (where $F = Z$). Because R satisfies Condition A, every symmetric nilpotent element in R has index of nilpotence at most k. The isomorphism of R with F_n then tells us that every symmetric nilpotent element in F_n has index of nilpotence at most k. Invoking Theorem 1, we get that $n < 2(k + 1)$. Therefore R is of type 3 in the assertion of the theorem.

Finally, if R is *-prime but not prime, and satisfies Condition A, then R has a prime ideal $0 \neq P$ such that $P \cap P^* = 0$. Now, every element $\bar{x}$ in the non-zero ideal $T = (P + P^*)/P$ in the prime ring R/P is the image of an element of the form $x + x^*$ where $x \in P^*$, hence $\bar{x}^k = \bar{x}^{k+1}p(\bar{x})$. T is a prime

https://doi.org/10.4153/CJM-1975-117-8 Published online by Cambridge University Press

ring and satisfies Condition A; it follows easily from Lemma 2 that T must satisfy a polynomial identity. Also, the center of T is algebraic over a finite field, as a consequence of Condition A. Again invoking Posner's theorem and the result of Rowen used in the paragraph above gives us that T is a simple algebra finite dimension over its center. Thus T has a unit element; since $T \neq 0$ is an ideal in R/P, the unit element of T must be a central idempotent in the prime ring R/P, hence must be 1. Thus $(P + P^*)/P = T = R/P$, whence $R = P \oplus P^*$ is isomorphic to $(R/P) \oplus (R/P^*)$. Since T, and so R/P, satisfies Condition A with A-index k, R/P must satisfy the standard identity of degree $2k$ by Lemma 2. Thus we get R/P to be isomorphic to F_n where $n \leqq k$ and F is a field algebraic over a finite field. In short, in this last case, R is of type 4 of the theorem. With this the theorem is proved.

The structure of *-prime rings expressed in Theorem 3 immediately translates into a structure theorem for semi-prime rings with involution, since those semi-prime rings are subdirect sums of *-prime rings. However, in passing to a *-prime homomorphic image of R, if this image is of characteristic 2, it may be that not all symmetric elements in the image came from symmetric elements in R. However, the square of every symmetric element in this *-prime ring is the image of a symmetric element in R. This may lead to a doubling of the k in Theorem 3 for some of the homomorphic images of R. With this we can state the

COROLLARY 1. *Let R be a semi-prime ring with involution. Suppose that every symmetric element in R satisfies $s^k - s^{k+1}p(s) \in Z$ where k is a fixed integer and $p(x)$ is a polynomial with integer coefficients which depend on s. Then R is a subdirect sum of rings of the following types:*

(1) *an order in a simple algebra of dimension at most 4 over its center;*

(2) *an order in the direct sum of a field with itself, relative to the exchange involution;*

(3) *F_n, the ring of $n \times n$ matrices over a field F which is algebraic over a finite field, with $n \leqq 2(2k + 1)$; or*

(4) *the direct sum of F_n with itself, F as in Part 3, with $n \leqq 2k$, relative to the exchange involution.*

A special case of Corollary 1, which may have some interest, is the situation in which $s - s^2p(s) \in Z$ for all $s \in S$, $p(t)$, as usual, a polynomial with integer coefficients depending on s. This is

COROLLARY 2. *Let R be a semi-prime ring in which $s - s^2p(s) \in Z$ for all $s \in S$. Then R satisfies the standard identity of degree 4.*

Proof. Let $\bar{R}$ be a *-prime image of R. If $\bar{a} \in \bar{R}$ is symmetric, then $\bar{a}^2 = \bar{a}\bar{a}^* = \bar{a}\bar{a}^*$ is the image of a symmetric element of R, hence $\bar{a}^2 - \bar{a}^4p(\bar{a}^2) \in \bar{Z}$, the center of $\bar{R}$. In particular, if $\bar{a}$ is nilpotent, since $\bar{Z}$ has no nilpotent symmetric elements in $\bar{R}$ which is *-prime, we have $\bar{a}^2 = 0$.

If the symmetric elements of $\bar{R}$ satisfy Condition A, this above remark tells us that the A-index of the symmetric elements in $\bar{R}$ must be 2. But then, as we have seen in looking at Conditions A and A', we must have

$$\bar{b}^2 = \bar{b}^{2+n(\bar{b})},$$

$n(\bar{b}) > 1$ for all symmetric $\bar{b}$ in $\bar{R}$. If $\bar{t} = \bar{x} + \bar{x}^* = \overline{x + x^*}$, then $\bar{t}^2 = \bar{t}^{2+n(\bar{t})}$ yields

$$(\bar{t} - \bar{t}^{n(\bar{t})+1})^2 = 0.$$

But

$$\bar{c} = \bar{t} - \bar{t}^{n(\bar{t})+1}$$

is the image of a symmetric element in $\bar{R}$, so $\bar{c} - \bar{c}^2 q(\bar{c}) \in Z$. Since $\bar{c}^2 = 0$, we have $\bar{c} \in \bar{Z}$ is a nilpotent symmetric. In short, $\bar{c} = 0$. Thus

$$\bar{t} = \bar{t}^{n(\bar{t})+1}$$

for all traces $\bar{t} \in \bar{R}$. By the results of Montgomery [**13**; **14**] we then have that $\bar{R}$ satisfies the standard identity of degree 4.

On the other hand, if the symmetric elements of $\bar{R}$ do not satisfy Condition A, since they do satisfy $\bar{b}^2 - \bar{b}^4 p(\bar{b}^2) \in \bar{Z}$, according to Lemma 9 $\bar{R}$ satisfies the standard identity of degree 4.

Hence in all cases $\bar{R}$ satisfies the standard identity of degree 4. Since R is a subdirect sum of all these $\bar{R}$, we have that R satisfies the identity of degree 4. This proves the corollary.

But more can be said. Even if the ring R has nilpotent ideals we can say that it must satisfy an identity of fairly low degree, namely 14. We show this now.

Let R be a ring with * such that $s - s^2 p(s)$ is in Z for all $s \in S$. Let N be the lower radical of R; certainly $N^* = N$. If $s \in N \cap S$ then, iterating $s - s^2 p(s) \in Z$, we get $s - s^{2^n} p_n(s) \in Z$ where $p_n(s)$ is a polynomial with integer coefficients. But s is nilpotent, so $s^{2^n} = 0$ for some n; this results in $s \in Z$. In particular, if $x \in N$ then $x + x^* \in N \cap S$ and $x^*x \in N \cap S$, so, by the above, $x + x^* \in Z$ and $x^*x \in Z$. Since $x^2 - (x + x^*) + x^*x = 0$, we have that N is quadratic over Z. If $y \in R$ and $x \in N$ then $x^2y - yx^2 - (x + x^*)(xy - yx) = 0$ which gives $(x^2y - yx^2)(xy - yx) = (xy - yx)(x^2y - yx^2)$. Now N is the intersection of all the *-prime ideals P of R and R/P satisfies the standard identity of degree 4, $f(x_1, x_2, x_3, x_4)$. So if a_1, a_2, a_3, and a_4 are in R then $x = f(a_1, a_2, a_3, a_4) \in N$ so $(x^2y - yx^2)(xy - yx) = (xy - yx)(x^2y - yx^2)$ gives us a polynomial identity of degree 14 for R.

Acknowledgment. The authors would like to thank the referee for pointing out to them the present brief proof of Theorem 1.

References

1. S. A. Amitsur, *Rings with involution*, Israel J. Math. *6* (1968), 99–106.

2. S. A. Amitsur and Jacob Levitzki, *Minimal identities for algebras*, Proc. Amer. Math. Soc. *1* (1950), 449–463.

3. W. Burgess and M. Chacron, *A generalization of a theorem of Herstein and Montgomery*, J. Algebra (to appear).

4. M. Chacron, *On a theorem of Herstein*, Can. J. Math. (to appear).

5. ——— *A generalization of a theorem of Kaplansky and rings with involution*, Michigan Math. J. *20* (1973), 45–54.

6. I. N. Herstein, *The structure of a certain class of rings*, Amer. J. Math. *75* (1953), 864–871.

7. I. N. Herstein and Susan Montgomery, *Invertible and regular elements in rings with involution*, J. Algebra *25* (1973), 390–400.

8. Nathan Jacobson, *Lectures on quadratic Jordan algebras* (Tata Institute, Bombay 1969).

9. ——— *A structure theory for algebraic algebras of bounded degree*, Ann. of Math. *46* (1945), 695–707.

10. ——— *Structure of rings* (AMS Colloquium Publ. *37* ,1964).

11. I. Kaplansky, *Linear algebra and geometry* (Allyn & Bacon, Boston, 1969).

12. K. McCrimmon, *On Herstein's theorems relating Jordan and associative algebras*, J. Algebra *13* (1969), 382–392.

13. Susan Montgomery, *A generalization of a theorem of Jacobson*, Proc. Amer. Math. Soc. *28* (1971), 366–370.

14. ——— *A generalization of a theorem of Jacobson II*, Pacific J. Math. *44* (1973), 233–240.

15. ——— *Polynomial identity algebras with involution*, Proc. Amer. Math. Soc. *27* (1971), 53–56.

16. M. Nagata, T. Nakayama and T. Tuzuku, *On an existence lemma in valuation theory*, Nagoya Math. J. *6* (1953), 59–61.

17. Louis Rowen, *Some results on the center of a ring with polynomial identity*, Bull. Amer. Math. Soc. *79* (1973), 219–223.

Carleton University,
Ottawa, Ontario;
University of Chicago,
Chicago, Illinois;
University of Southern California,
Los Angeles, California