RINGS WITH INVOLUTION AND POLYNOMIAL IDENTITIES

W. E. BAXTER AND W. S. MARTINDALE III

An involution $*$ of a ring A is a one-one additive mapping of A onto itself such that $(xy)^* = y^*x^*$ and $x^{**} = x$ for all $x, y \in A$. If A is an algebra over a field Φ, one makes the additional requirement that $(\lambda x)^* = \lambda x^*$ for all $\lambda \in \Phi$, $x \in A$. S will generally denote the set of symmetric elements $s^* = s$, K the set of skew elements $k^* = -k$, and Z the centre of A.

The theory of simple rings with involution has been studied extensively by Herstein **(1; 2)**. Our viewpoint in the present paper is to consider arbitrary rings with involution, and to study some specific problems in which the hypotheses (previously made on the whole ring) are only made on the symmetric elements S. In §1 an easy but useful structure theory for arbitrary rings with involution is worked out. Section 3 culminates in Theorem 10: if A is an algebra with involution over Φ such that S satisfies a polynomial identity over Φ and is algebraic over Φ, then A is locally finite over Φ. In §4 we initiate a study of rings in which $s^{n(s)} - s$ is central for all $s \in S$ and obtain results for some special cases.

1. Our purpose in this section is to indicate how the Jacobson structure theory for rings can be modified so as to provide a useful structure theory for rings with involution. To this end we make the following definitions.

Let A be a ring with involution $*$. A right A-module M is $*$-faithful if, for $r \in A$, $Mr = Mr^* = 0$ implies that $r = 0$. A is $*$-primitive if there exists an irreducible right A-module which is $*$-faithful. U is an $*$-ideal of A if U is an ideal of A such that $U^* = U$. (We remark that if U is a $*$-ideal of A, then the involution induced in A/U will still be denoted by $*$.) U is a $*$-primitive ideal of A if U is a $*$-ideal of A such that A/U is $*$-primitive.

Let I be the set of irreducible right A-modules, and denote by N the Jacobson radical of A. If $M \in I$, we set $R(M) = \{a \in A \mid Ma = Ma^* = 0\}$. It is clear that N and $R(M)$ are $*$-ideals of A. We first establish

THEOREM 1. *If I is non-empty, then $N = \bigcap_{M \in I} R(M)$.*

Proof. Set $\tilde{N} = \bigcap R(M)$ and let $M \in I$. Since $N = N^*$, we have $MN = MN^* = 0$, and hence $N \subseteq \tilde{N}$. Now let $x \in \tilde{N}$ and let $M \in I$. In particular $Mx = 0$ and so $x \in N$.

It is also straightforward to verify

Received August 23, 1966.

https://doi.org/10.4153/CJM-1968-043-6 Published online by Cambridge University Press

THEOREM 2. *U is a $*$-primitive ideal of A if and only if $U = R(M)$ for some $M \in I$.*

Proof. Suppose $U = R(M)$ and set $\bar{A} = A/U$. Then M is a well-defined, irreducible right $\bar{A}$-module according to: $m\bar{r} = mr$, $m \in M$, $r \in A$. If $M\bar{r} = M(\bar{r}^*) = 0$, then $Mr = Mr^* = 0$, and so $r \in R(M)$, or $\bar{r} = 0$. Hence $U = R(M)$ is a $*$-primitive ideal.

Conversely, if U is a $*$-primitive ideal, $\bar{A} = A/U$ is a $*$-primitive ring, with M an irreducible, $*$-faithful $\bar{A}$-module. By defining $mr = m\bar{r}$, $m \in M$, $r \in A$, M becomes an irreducible right A-module. If $x \in U$, then $x^* \in U$ and thus $Mx = Mx^* = 0$, whence $x \in R(M)$. For $x \in R(M)$, $Mx = Mx^* = 0$, or $M\bar{x} = M\bar{x}^* = 0$. Since M is a $*$-faithful $\bar{A}$-module, $\bar{x} = 0$ and hence $x \in U$. We have therefore shown that $U = R(M)$.

As a corollary to these first two theorems we have

THEOREM 3. *If A is a semi-simple ring with involution, then A is a subdirect sum of $*$-primitive rings.*

The relation between $*$-primitive rings and primitive rings is indicated in

THEOREM 4. *If A is a $*$-primitive ring, then A is either a primitive ring or there is a non-zero ideal U of A such that $U \cap U^* = 0$, A/U is (right) primitive, and A/U^* is (left) primitive.*

Proof. Let M be an irreducible, $*$-faithful right A-module. We may suppose that M is not faithful. Then $U = \{r \in A \mid Mr = 0\}$ is a non-zero ideal of A, and M is an irreducible, faithful right (A/U)-module, that is, A/U is right primitive. Now $M \cong A - J$, J a maximal modular right ideal. Set $M' = A - J^*$, J^* a maximal modular left ideal. We now show that $U^* = \{r \in A \mid rM' = 0\}$. Let $xM' = 0$, i.e., $xA \subseteq J^*$. Then $Ax^* \subseteq J$, that is, $x^* \in U$, or $x \in U^*$. Next let $x \in U^*$. Then $x^* \in U$ and $Ax^* \subseteq J$, or $xA \subseteq J^*$, or $xM' = 0$. Therefore M' is an irreducible faithful left (A/U^*)-module. Finally, let $x \in U \cap U^*$. This means that $Mx = 0$ and $xM' = 0$. The latter says that $xA \subseteq J^*$, i.e., $Ax^* \subseteq J$, or $Mx^* = 0$. Hence $x = 0$, since M is $*$-faithful.

We remark that the structure theory as developed in this section for rings with involution carries over in the usual way to the theory of algebras with involution.

2. Before proceeding to our main results, we shall find it convenient to list in this section several remarks which will be used in the following. *We also take this opportunity to assert that for the remainder of this paper we shall assume that $2A = A$ and that $2x = 0$ implies $x = 0$.*

Remark 1. Let A be an algebra with involution over a field Φ. The set S of symmetric elements of A is said to satisfy a polynomial identity of degree d over Φ if there exists a non-zero element $f(t_1, t_2 \ldots, t_n)$ of the free algebra over

Φ freely generated by the t_i such that $f(s_1, s_2, \ldots, s_n) = 0$ for all $s_i \in S$. The element $f(t_1, t_2, \ldots, t_n)$ is multilinear of degree n if and only if it is of the form $\sum_\sigma \alpha(\sigma) t_{\sigma 1}\, t_{\sigma 2} \ldots t_{\sigma n}$, $\alpha(\sigma) \in \Phi$, some $\alpha(\sigma) \neq 0$, where σ ranges over all permutations of $(1, 2, \ldots, n)$. If S satisfies a polynomial identity of degree n, then S satisfies a multilinear identity of degree $\leqslant n$. (The proof of (**5**, p. 225, Proposition 1) carries over here.)

Remark 2. Let A be an algebra over a field Φ and suppose that a is a non-nilpotent non-invertible algebraic element of A. Then there is an idempotent $e = a^k p(a)$, where $p(a)$ lies in the subalgebra formally generated by 1 and a, such that $a^k e = a^k$, for some $k \geqslant 1$. (See, for example, the proof of (**5**, p. 210, Proposition 1).)

Remark 3. Let A be a simple ring with involution $*$ satisfying the minimum condition on right ideals. Then A can be written as a matrix ring D_k, where D has an involution $\lambda \to \bar{\lambda}$. The involution $*$ is given by

$$(\textstyle\sum \alpha_{ij}\, e_{ij})^* = \sum \gamma_j^{-1}\, \bar{\alpha}_{ij}\, \gamma_i\, e_{ji}$$

where the $\gamma_i = \bar{\gamma}_i$ are fixed invertible symmetric elements of D. D is either a division ring or is isomorphic to the matrix ring Z_2, Z the centre of A, in which case $\bar{\lambda} = \sigma^{-1}\lambda'\sigma$, λ' the transpose of λ,

$$\sigma = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

and all the $\gamma_i = 1$; see (**7**, p. 311, Example A).

Remark 4. Let A be a primitive algebra with involution over Φ such that S satisfies a polynomial identity of degree n. Then there are at most n non-zero orthogonal symmetric idempotents; see (**8**, p. 1433, Theorem 2).

Remark 5. Let A be a primitive ring with involution such that $S \subseteq Z$. Then $[A\colon Z] \leqslant 4$ ((**5**, p. 226, Theorem 1) can be applied here).

Remark 6 (Noether–Jacobson). Let D be a division ring with involution properly containing its centre Z and such that S is algebraic over Z. Then D contains an element $x \in S \cup K$, $x \notin Z$, x separable over Z.

Proof. If $S \subseteq Z$, then by Remark 5 $[D\colon Z] = 4$ and D is separable over Z, since the characteristic is unequal to 2. We may assume that the characteristic is $p > 2$ and that there is an element $s \in S$ such that $s^p \in Z$ but $s \notin Z$. The proof which appears in (**5**, pp. 180–181, Proposition 2) carries over to the point where there exists an element $x \in D$ such that $s = xs - sx$. Setting $x = t + k$, $t \in S$, $k \in K$, we see in fact that $s = ks - sk$, or $s^{-1}ks = k + 1$. As k is algebraic, it follows that $Z(k)$ contains a separable element x not belonging to Z. Then $x^* \in Z(k)$ is separable and so $Z(x, x^*)$ is separable over Z. In particular either $x + x^*$ or $x - x^*$ is a separable element not belonging to Z.

Remark 7. Let D be a division ring with involution $*$ such that S is algebraic over Z. Suppose the dimensions of all finite-dimensional separable subfields M containing Z for which $M^* = M$ are bounded. Then $[D:Z]$ is finite and D has a maximal subfield P such that $P^* = P$ and P is separable over Z.

Proof. Following the proof of (**5**, p. 181, Theorem 1), we let $P = P^*$ be such a separable subfield of maximum finite dimension. The centralizer C of P is a division ring with involution whose centre, in view of (**5**, p. 165, Corollary), is P. If $C \neq P$, by Remark 6 there is a symmetric or skew element $x \in C, x \notin P$ which is separable over P. Then $Q = P(x)$ is finite-dimensional and separable over Z, and since $Q^* = Q$ and Q properly contains P, a contradiction results. Therefore $C = P$ is a maximal subfield and D is finite-dimensional over Z.

3. We begin this section with

LEMMA 1. *Let A be a primitive ring with involution $*$ and with an identity element. If S is a simple Jordan ring, then A is a simple ring.*

Proof. Let U be a non-zero ideal of A. Then $V = UU^*$ is a non-zero $*$-ideal of A since A is primitive. Suppose $V \cap S \neq 0$. Then $V \cap S = S$ and $1 \in V$, forcing $U = A$. Suppose $V \cap S = 0$. Then $V \subseteq K$ and in particular $v^2 = 0$ for all $v \in V$. But this contradicts the primitivity of A.

THEOREM 5. *Let A be a primitive algebra with involution $*$ over a field Φ. Suppose S is algebraic over Φ and contains no non-trivial idempotents. Then A is either a quaternion algebra over its centre or A is a division algebra.*

Proof. Suppose S has no non-zero nilpotent elements. Then by Remark 2 every non-zero element of S is invertible, since S is algebraic and contains no non-trivial idempotents. In particular, S is a simple Jordan algebra, and by Lemma 1 A must be simple. The conclusion then follows from a theorem of Osborn (**6**, p. 249, Lemma 4).

Therefore we may suppose that $s^2 = 0$ for some $s \neq 0 \in S$. From

$$\sum_{i=0}^{m} \lambda_i (sx + x^* s)^i = 0, \qquad \lambda_i \in \Phi,$$

we obtain

$$\sum_{i=0}^{m} \lambda_i (sx)^{i+1} = 0$$

by multiplying on the right by sx. In other words, sA is algebraic over Φ and so must contain a non-zero idempotent $e = sa$ (since sA cannot be nil). Since $e^*e = 0$, $e + e^* - ee^*$ is a non-zero symmetric idempotent, which therefore must equal 1. Suppose eAe is not a division algebra. Choose $g \in eAe$ such that g is an idempotent different from 0 and e. This can be done since eAe $(\subseteq sA)$ is an algebraic primitive algebra over Φ. Then $g + g^* - gg^*$ is a non-zero symmetric idempotent, which must be equal to 1. But then

$$e = (g + g^* - gg^*)e = g,$$

a contradiction. Hence eAe is a division algebra. Now consider $1 - e$. Since $(1 - e)e^* = e^* - ee^* = 1 - e$, it follows that $1 - e \in Ae^* \subseteq As$, which is algebraic. By the same argument as before, $(1 - e)A(1 - e)$ is a division algebra. Therefore $A \cong \Delta_2$, Δ a division ring, and since S has no non-trivial idempotents, A must actually be a quaternion algebra Z_2 according to Remark 3.

THEOREM 6. *Let D be a division algebra with involution $*$ over Φ, and suppose S satisfies a polynomial identity of degree n over Φ and is algebraic over Φ. Then D is finite-dimensional over its centre Z, where $[D : Z] \leqslant 4n^2$.*

Proof. By Remark 1 let $f(t_1, t_2, \ldots, t_n)$ be a multilinear identity satisfied by S.

If $*$ is of the second kind, then $f(x_1, x_2, \ldots, x_n) = 0$ for all $x_i \in D$; see, e.g., (**8**, p. 1433, Theorem 1). By a theorem of Kaplansky (**5**, p. 226, Theorem 1), $[D : Z] \leqslant \frac{1}{4}n^2 \leqslant 4n^2$. Therefore we may assume that $Z \subseteq S$.

Suppose the dimensions of all finite-dimensional separable subfields M containing Z for which $M^* = M$ are bounded. By Remark 7, D is finite-dimensional over Z with maximal subfield P. $D \otimes_Z P \cong P_q$ is again a ring with involution induced by $*$ whose symmetric elements also satisfy

$$f(t_1, t_2, \ldots, t_n) = 0.$$

In view of Remark 3, P_q has at least r orthogonal symmetric idempotents, where $q \leqslant 2r$. But $r \leqslant n$ by Remark 4 and so $q \leqslant 2r \leqslant 2n$, whence

$$[D : Z] = q^2 \leqslant 4n^2.$$

We may assume, then, that D contains a separable element x of degree l, where $l > 2n$. Set $E = Z(x)$. As in the proof of (**8**, p. 1439, Theorem 6), we see that $D \otimes_Z E \cong C_m$, C a division ring, is a ring with involution for which $l \leqslant m$, a contradiction to Remark 4.

THEOREM 7. *Let A be a primitive algebra with involution $*$ over a field Φ. Suppose S satisfies a polynomial identity of degree n over Φ and is algebraic over Φ. Then A is a finite-dimensional simple algebra over its centre Z, with $[A : Z] \leqslant 4n^2$.*

Proof. As in the first part of the proof of Theorem 6, if $Z \not\subseteq S$, then $[A : Z] \leqslant 4n^2$. Thus we may assume that $Z \subseteq S$. Let $E = \{e_1, e_2, \ldots, e_k\}$, $k \leqslant n$, by Remark 4, be a maximal set of orthogonal symmetric idempotents. By Theorem 5, e_1Ae_1 is either a quaternion algebra or a division algebra, and by Theorem 6, e_1Ae_1 is finite-dimensional over its centre. It follows that $[A : Z] < \infty$. According to Remark 3, $A \cong D_q$, where either $D \cong Z_2$ or D is a division algebra over Z with maximal subfield M such that $[M : Z] < \infty$. In the former case, since $q \leqslant n$ by Remark 4, $[A : Z] = 4q^2 \leqslant 4n^2$. In the latter case, we note first that $*$ induces an involution in $A \otimes_Z M \cong M_j$ for some j. Applying Remarks 3 and 4 to M_j, we obtain $j \leqslant 2n$ and so again $[A : Z] = j^2 \leqslant 4n^2$.

THEOREM 8. *Let A be a $*$-primitive algebra over Φ such that A is not a primitive algebra. Suppose S satisfies a polynomial identity of degree n over Φ and is algebraic over Φ. Then $A = U \oplus U^*$, where U is an ideal which is a simple algebra of dimension $\leqslant \frac{1}{4}n^2$ over its centre.*

Proof. By Theorem 4 there is an ideal $U \neq 0$ such that $U \cap U^* = 0$, and A/U and A/U^* are primitive rings. Setting $\bar{A} = A/U^*$, we see that

$$\bar{U} = (U + U^*)/U^*$$

is a non-zero ideal of $\bar{A}$. Let $\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_n \in \bar{U}$, and note that $\bar{u}_i$ may be written $\overline{u_i + u_i^*}$. Then

$$f(\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_n) = f(\overline{u_1 + u_1*}, \overline{u_2 + u_2*}, \ldots, \overline{u_n + u_n*}) = 0.$$

By Kaplansky's theorem (**5**, p. 226, Theorem 1) $\bar{U}$ is a simple algebra of dimension $\leqslant \frac{1}{4}n^2$ over its centre, and consequently $\bar{U} = \bar{A}$. Therefore $A = U \oplus U^*$, where $U \cong A/U^*$ is a simple algebra of dimension $\leqslant \frac{1}{4}n^2$ over its centre.

As an important corollary we have

THEOREM 9. *Let A be a semi-simple algebra with involution $*$ over Φ. Suppose S satisfies a polynomial identity of degree n over Φ and is algebraic over Φ. Then A satisfies a standard identity of degree $\leqslant 4n^2 + 1$.*

Proof. By Theorem 3, A is a subdirect sum of $*$-primitive algebras, each of which, in view of Theorems 7 and 8, is of dimension $\leqslant 4n^2$ over its centre. Thus each one satisfies a standard identity of degree $\leqslant 4n^2 + 1$, and it follows that A also satisfies this identity.

We now recall that an algebra A over a field Φ is locally finite over Φ if every finite subset generates a finite-dimensional subalgebra. If U is an ideal of A such that both U and A/U are locally finite, then A is locally finite. The locally finite kernel L of an algebra A is the sum of all the locally finite one-sided ideals of A and is itself locally finite. The locally finite kernel of A/L is 0. Of fundamental importance to us is the following recent result due to Procesi: if A is a PI-algebra (i.e., satisfies a polynomial identity) over Φ and if every element of A is the sum of algebraic elements, then A is locally finite over Φ.

LEMMA 2. *Let A be an algebra with involution $*$ over Φ. Suppose S satisfies a polynomial identity of degree n over Φ and is algebraic over Φ. Suppose there is an $a \neq 0 \in A$ such that $a^*a = 0$. Then $L \neq 0$.*

Proof. By Remark 1, S satisfies a multilinear identity $f(t_1, t_2, \ldots, t_n) = 0$. Let J be the right ideal generated by a and note that $J^*J = 0$. Let $x \in J$. Then

$$0 = \sum_{i=0}^{m} \lambda_i (x + x^*)^i = \sum_{i=0}^{m} \lambda_i (x + x^*)^i x = \sum_{i=0}^{m} \lambda_i x^{i+1} = 0,$$

$\lambda_i \in \Phi$. Hence J is algebraic over Φ. Now let $x_1, x_2, \ldots, x_n, x_{n+1} \in J$. We have

$$\begin{aligned} 0 &= f(x_1 + x_1^*, x_2 + x_2^*, \ldots, x_n + x_n^*) \\ &= f(x_1 + x_1^*, x_2 + x_2^*, \ldots, x_n + x_n^*)x_{n+1} \\ &= f(x_1, x_2, \ldots, x_n)x_{n+1} \\ &= g(x_1, x_2, \ldots, x_{n+1}). \end{aligned}$$

Thus J is a PI-algebra. J is then locally finite by Procesi's theorem, and hence L, which contains J, is not 0.

THEOREM 10. *Let A be an algebra with involution $*$ over a field Φ. Suppose S satisfies a polynomial identity over Φ and is algebraic over Φ. Then A is locally finite over Φ.*

Proof. We claim first that $N \subseteq L$. If not, we may assume that $L = 0$ and $N \neq 0$. All symmetric and skew elements of N, being algebraic, must actually be nilpotent, a contradiction to Lemma 2. Hence, $N = (0)$.

It therefore suffices to prove that A/N is locally finite. By Theorem 9, A/N is a PI-algebra. Since every element of A/N is the sum of a symmetric element and a skew element, A/N is locally finite by Procesi's theorem.

COROLLARY 1. *Let A be a simple algebra with involution $*$ over Φ such that S satisfies a polynomial identity of degree n over Φ and is algebraic over Φ. Then A is finite-dimensional over its centre, with $[A : Z] \leqslant 4n^2$.*

Proof. By Theorem 7 we may assume that A is a simple radical algebra. Since A is locally finite by Theorem 10, it is easy to see that it is actually locally nilpotent, which contradicts a theorem of Levitzki; see, e.g., (**3**, p. 31, Theorem 1.17).

4. In this final section we initiate an attempt to prove for rings with involution an analogue of Herstein's theorem (see, e.g., (**5**, p. 221, Theorem 2)) that if in a ring A, $x^{n(x)} - x$ is always central, $n(x) > 1$, then A is commutative.

THEOREM 11. *Let A be a finite simple ring with involution $*$ such that*

$$s^{n(s)} - s \in Z, \qquad n(s) > 1,$$

for all $s \in S$. Then A is either Z, Z_2 with canonical involution, or Z_2 with symplectic involution (see Remark 3).

Proof. Since A is a finite simple ring, we have by Remark 3 that $A \cong D_k$ and the involution is canonical. We have case 1, $D \cong Z$ (since D is a finite division ring), and case 2, $D \cong Z_2$ (see Remark 3 for exact details).

For case 1 it suffices to show that $k = 1$ or $k = 2$. If $k > 2$ we may assume without loss of generality that $k = 3$. Let F denote the symmetric elements of the involution $\gamma \to \bar{\gamma}$ induced in the coefficient field D. There are fixed non-zero elements $\rho, \lambda, \mu \in F$ such that the symmetric elements of A are of the form

$$\begin{bmatrix} \alpha_{11} & \bar{\alpha}_{21}\rho & \bar{\alpha}_{31}\lambda \\ \alpha_{21} & \alpha_{22} & \bar{\alpha}_{32}\mu \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{bmatrix};$$

$\alpha_{11}, \alpha_{22}, \alpha_{33} \in F$; $\alpha_{21}, \alpha_{31}, \alpha_{32} \in D$. F is a finite field, and by (**4**, p. 317, Lemma 7.7) there exist $\alpha, \beta \in F$ such that $1 + \alpha^2\lambda + \beta^2\mu = 0$. It follows that the matrix

$$a = \begin{bmatrix} -1 & 0 & \alpha\lambda \\ 0 & -1 & \beta\mu \\ \alpha & \beta & 1 \end{bmatrix}$$

is a symmetric element of A such that $r(a) = 2$ and $r(a^2) = 1$, where $r(x) =$ rank of x. On the other hand, we know that $a^n - a = z \in Z$. z must be 0 since otherwise a would be invertible and have rank 3. But now $a^n = a$ forces $r(a^2) = r(a) = 2$, a contradiction.

For case 2, we wish to show that $k = 1$. To this end we may assume that $k = 2$. One verifies that the matrix

$$b = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

is a symmetric matrix such that $b^2 = 0$, a contradiction to $b^n - b \in Z$.

THEOREM 12. *Let A be a primitive ring with involution $*$ for which there is a fixed integer $n > 1$ such that $s^n - s \in Z$ for all $s \in S$. Then A is either a field, a quaternion algebra, or the 2×2 matrices with canonical involution over a finite field.*

Proof. Suppose first that $S \subseteq Z$. It follows from Remark 5 that Z is a field and $[A : Z] \leqslant 4$. If $A \neq Z$, then $Z = S$ and A is a quaternion algebra over Z.

We may therefore assume that $S \not\subseteq Z$ and select an element $s \in S$, $s \notin Z$. If $Z \neq 0$, we claim that $S \cap Z$ is a finite field. Indeed, $(\lambda s)^n - \lambda s \in Z$ for all $\lambda \in S \cap Z$ forces $\lambda^n - \lambda = 0$ since $s \notin Z$. It follows that $S \cap Z$ is a finite commutative integral domain and hence a finite field. If $Z = 0$, we let C be the centroid of A and consider the subring P of C generated by the identity. The same argument as above shows that P is also a finite field.

If $Z \neq 0$, we set $\Phi = Z \cap S$, and if $Z = 0$ we set $\Phi = P$. A is then an algebra with involution $*$ over the finite field Φ. Since $s^n - s \in Z$ for all $s \in S$ and n is fixed, S satisfies a polynomial identity over Φ and S is algebraic over Φ. By Theorem 7, A is a finite-dimensional simple algebra with involution over the finite field $\Phi = S \cap Z$. Thus A is a finite simple ring and the conclusion follows from Theorem 11.

https://doi.org/10.4153/CJM-1968-043-6 Published online by Cambridge University Press

COROLLARY 2. *Let A be a semi-simple ring with involution $*$ for which there is a fixed integer $n > 1$ such that $s^n - s \in Z$ for all $s \in S$. Then A is a subdirect sum of rings A_α with involution which are either of the type described in Theorem* 12 *or are of the form $U + U^*$, where U is a field.*

Proof. By Theorem 3, A is a subdirect sum of $*$-primitive rings A_α. If A_α is primitive, we may apply Theorem 12. If A_α is not primitive, by Theorem 4 there is an ideal $U \neq 0$ such that $U \cap U^* = 0$. Since $u + u^* \in S$ for $u \in U$, $u^n - u$ lies in the centre of U and hence U is commutative. It follows that $A_\alpha = U \oplus U^*$, U a field.

Note. Since the announcement of our results in this paper, I. N. Herstein has proved the following striking theorem: if A is a simple algebra with involution such that S satisfies a polynomial identity, then A is finite-dimensional over its centre. It appears very likely that his result will hold, more generally, for primitive algebras. In that event our Theorem 7 will, of course, be a special case of his theorem.

REFERENCES

1. I. N. Herstein, *Lie and Jordan Systems in simple rings with involution*, Amer. J. Math., *78* (1956), 629–649.
2. ——— *Lie and Jordan structures in simple, associative rings*, Bull. Amer. Math. Soc., *67* (1961), 517–531.
3. ——— *Theory of rings* (Univ. of Chicago Math. Lecture Notes, 1961).
4. ——— *Topics in algebra* (Blaisdell, 1964).
5. N. Jacobson, *Structure of rings*, Amer. Math. Soc., Colloquium Publications, *37* (1956).
6. ——— *Structure theory for a class of Jordan algebras*, Proc. Nat. Acad. Sci. U.S.A., *55* (1966), 243–251.
7. N. Jacobson and C. E. Rickart, *Homomorphisms of Jordan rings of self-adjoint elements*, Trans. Amer. Math Soc., *72* (1952), 310–322.
8. W. S. Martindale III, *Primitive algebras with involution*, Pacific J. Math., *11* (1961), 1431–1441.

University of Delaware, and
University of Massachusetts

https://doi.org/10.4153/CJM-1968-043-6 Published online by Cambridge University Press