A Structure Theorem and a Positive-Definiteness Condition in Rings with Involution

SUSAN MONTGOMERY

Department of Mathematics, University of Southern California,
Los Angeles, California 90007

Communicated by I. N. Herstein

Received August 28, 1975

INTRODUCTION

There has been a series of works recently describing the structure of a ring \( R \) with involution \( * \) when various subsets of its symmetric or skew symmetric elements are assumed to be regular or invertible, or nilpotent \([4, 6, 9, 13-15]\). In particular, if all the symmetric elements are regular or nilpotent, and \( R \) is prime with no nil right ideals, then a necessary and sufficient condition for \( R \) to be "well behaved" is a certain left-right symmetry condition. Specifically, with the above hypotheses on \( R \), \( R \) is a domain or an order in a four-dimensional simple algebra if and only if the following holds: For any \( x \in R \), \( xx^* = 0 \) implies \( x^*x = 0 \) \([13]\). The same condition has also arisen in studying symmetric units \([10, \text{Theorem 6}]\). The work in this paper was motivated by a desire to examine this condition by itself.

There are two obvious ways in which a ring could satisfy the desired condition. First of all, it may happen that \( xx^* \) is never 0, for any \( x \neq 0 \) in \( R \). This is a kind of "positive-definiteness" assumption about the involution, and has been studied by Herstein in \([6]\). The other trivial possibility is that \( xx^* = x^*x \) for all \( x \in R \). Such "normal" rings have also been studied. Maxwell has considered such algebras of matrices \([12]\), and more generally, Amitsur has studied identities in rings with involution of the form \( p(x_1, \ldots, x_n; x_1^*, \ldots, x_n^*) \), where \( p \) is a polynomial in \( 2n \) indeterminates \([1]\). Clearly \( p(x; x^*) = xx^* - x^*x \) is a special case, and it is an immediate consequence of Amitsur's results that a prime ring satisfying \( p(x; x^*) = 0 \) must be an order in a four-dimensional simple algebra.

\( ^\dagger \) This research was supported by NSF Grant GP-38601 at the University of Southern California.

Copyright © 1976 by Academic Press, Inc.
All rights of reproduction in any form reserved.
It is proved in this paper that, if $R$ is prime satisfying $xx^* = 0$ implies $x^*x = 0$, then the only two possibilities for $R$ are the two just described: $xx^*$ is never 0 or $R$ is “normal.”

The method of proof is of independent interest, as it relies on a structure theorem for prime rings with involution whose central closures have a minimal one-sided ideal. The theorem is a kind if infinite-dimensional Faith–Utumi theorem, and extends to rings with involution a recent result of Smith [16, Lemma 6, and Corollary 1]. Smith proved that if the central closure of $R$ acts on the minimal one-sided ideal $V$ with commuting ring $D$, then for every positive integer $n \leq \dim_D V$, there exists a subring $E$ of $D$ such that $R$ contains a subring isomorphic to the $n \times n$ matrices over $E$. Moreover $EC = D$, where $C$ is the extended centroid of $R$. The difficulty when $R$ has an involution is to produce appropriate subrings which are closed under the involution. The proof given here is based on Smith’s method, but also uses the relationship between primitive rings with involution and Hermitian and alternate scalar products.

Using the structure theorem, we are also able to obtain more straightforward proofs of some of the results on regular and nilpotent elements mentioned above. The advantage is that it enables one to work entirely within the prime ring itself, and avoids the difficulty of showing that hypotheses on $R$ are inherited by the central closure.

In all that follows, $R$ will denote a ring with involution $\ast$. An element $x \in R$ is symmetric if $x^* = x$, and skew-symmetric if $x^* = -x$. The traces are the set $T = \{x + x^* | x \in R\}$, and the skew-traces are defined by $K_T = \{x - x^* | x \in R\}$.

By a $\ast$-subring of $R$, we will mean a subring which is closed under the involution. We will say that the involution is positive-definite if $xx^* \neq 0$ for all $x \neq 0$ in $R$, and we will say that $R$ is normal if $xx^* = x^*x$, for all $x \in R$.

Finally, if $R$ is any ring, $R_n$ will mean the ring of all $n \times n$ matrices over $R$, and an element of $R$ will be called regular if it is not a zero divisor.

1. The Structure Theorem

Before beginning the proof of the theorem, we summarize some needed facts about the relationship between dense rings of linear transformations, involutions, and scalar products.

Let $V$ be a left vector space over a division ring $D$, and assume that $D$ has an involution $\alpha \rightarrow \bar{\alpha}$. Let $\langle \cdot , \cdot \rangle : V \times V \rightarrow D$ denote a nondegenerate Hermitian or alternate scalar product on $V$. $L(V)$ will denote the ring of all continuous linear transformations on $V$ (that is, those transformations which have an adjoint re $\langle \cdot , \cdot \rangle$), and $F(V)$ will denote the subring of all transforma-
tions in $L(V)$ of finite rank. The adjoint mapping $T \rightarrow T^*$, for $T$ a linear transformation, is an involution on the rings $L(V)$ and $F(V)$.

If the scalar product is Hermitian, then for any nondegenerate finite-dimensional subspace $V_0$ of $V$, we may find an orthogonal basis $\{v_1, \ldots, v_n\}$ for $V_0$, that is $\langle v_i, v_j \rangle = \delta_{ij} d_i$ where $d_i = d_i \in D$, $i = 1, \ldots, n$. Write $V_0^\perp$ for the orthogonal complement of $V_0$ in $V$; $V = V_0 \oplus V_0^\perp$. Now, for any matrix $A = (a_{ij}) \in D_n$, define a linear transformation $T_A$ on $V$ by $T_A: v_i \rightarrow \sum a_{ij} v_j$ and $T_A^*: v \rightarrow 0$ for $v \in V_0^\perp$. Clearly $T_A \in F(V)$, and thus $F(V)$ contains a subring $R(n) \cong D_n$. Moreover, the adjoint is an involution on $D_n$, and is given simply by $A^* = y A^t y^{-1}$, where $A^t$ is the conjugate transpose of $A$ and $y$ is the matrix of the scalar product. We will refer to such an involution as an involution of transpose type.

In the alternate case, $D$ is a field, and the mapping $\alpha \rightarrow \bar{\alpha}$ on $D$ is the identity. If $V_0$ is any nondegenerate finite-dimensional subspace of $V$ (necessarily of even dimension $2m$), then there exists a basis $\{u_1, v_1, u_2, v_2, \ldots, u_m, v_m\}$ of $V_0$ such that $\langle u_i, v_i \rangle = 1$, $\langle v_i, u_i \rangle = -1$, and all other inner products are zero. Using this basis and $V_0^\perp$, we may define linear transformations as in the Hermitian case to see that $F(V)$ contains a subring $R(2m) \cong D_{2m}$. The involution corresponding to the adjoint in this case is just the symplectic involution. That is, $A^* = y A^t y^{-1}$, where $y$ is the matrix of the scalar product and where, if $A = (a_{ij})$ is written as an $m \times m$ matrix of $2 \times 2$ blocks, $A^t = (A_{ji})$, transpose on the blocks [8, p. 0.10].

We will use in a crucial way a result of Kaplansky [7, p. 83] which states that if $R$ is a primitive ring with involution and a minimal one-sided ideal, then for some vector space $V$ over a division ring $D$, there exists a nondegenerate Hermitian or alternate form on $V$ such that $*$ on $R$ is the adjoint with respect to the scalar product, and such that $F(V) \subseteq R \subseteq L(V)$. From the previous discussion, it follows that for every $n$ (or $2m$) $\leq \dim_D V$, $R$ contains a complete matrix ring $D_n$ (or $D_{2m}$) which is invariant under $*$. We next need a few properties of the central closure $RC$ of a prime ring $R$. Each element of $RC$ is an equivalence class $[U, f]$, where $U$ is an ideal of $R$ and $f: U \rightarrow R$ is a right $R$-module homomorphism, and $[U, f] = [V, g]$ if and only if $f$ and $g$ agree on some nonzero ideal $W \subseteq U \cap V$. $C$, the extended centroid of $R$, is the center of the ring of all such equivalence classes, and is a field. Also, given any $x \in RC$, there exists an ideal $U$ of $R$ such that $0 \neq xU \subseteq R$ [3, pp. 1–2]. One more fact we will need is that if $R$ has an involution, this involution can be extended to $RC$ in a natural way [2].

Now assume that $R$ is a prime ring whose central closure $Q = RC$ has a minimal right ideal. Since $Q$ is prime, it is primitive, and so if $e$ is a primitive idempotent, $D = eQe$ is the commuting ring of $Q$ acting on the right ideal $eQ$. Moreover, since the centroid of $Q$ is just $C$ [3], the center of $D$ is isomorphic to $C$. 

RINGS WITH INVOLUTION 183
**Lemma 1.** Let \( R, Q = RC, e, \) and \( D \) be as above. Then for any nonzero ideal \( I \) of \( R \), such that \( Ie \subseteq R \), the ring \( E = eIe \) is an order in \( D \) and satisfies \( EC = D \).

**Proof.** First note that \( E \neq 0 \) since \( RC \) is prime. Now \( EC = eICe \supseteq eIRCe \supseteq eIeDe = D \), and thus \( D = EC \).

Now for any \( c_1, \ldots, c_k \in C \), there exists an ideal \( U \) of \( R \) such that \( 0 \neq c_i U \subseteq R \), for all \( i \). Thus \( c_i eUIe = e(c_i U)e \subseteq eRIe \subseteq eIe = E \), and so \( U' = eUIe \) is an ideal of \( E \) such that \( c_i U' \subseteq E \), for all \( i = 1, \ldots, k \). It follows that there exists some \( u \in U' \) such that \( c_i u = a_i \in E \), or that \( c_i = a_i u^{-1} \), for \( i = 1, \ldots, k \). Now choose any \( d \in D \). Since \( D = EC \), \( d = \sum e_i c_i \), where \( e_i \in E \) and \( c_i \in C \). By the above remarks, \( d = \sum e_i a_i u^{-1} = (\sum e_i a_i) u^{-1} \), where \( \sum e_i a_i \) and \( u \) are both in \( E \). Thus \( E \) is an order in \( D \).

The proof of Lemma 1 is based on the proof of [3, Corollary 3, p. 71] in which it is proved (although not stated explicitly) that if \( RC \) is simple Artinian, then \( R \) is an order in \( RC \).

We also remark that, by Lemma 1, the subrings \( E \) in Smith's theorem are actually orders in \( D \).

We can now prove the structure theorem.

**Theorem 1.** Let \( R \) be a prime ring with involution * such that the central closure \( Q = RC \) has a minimal one-sided ideal, and extend * to \( Q \). Let \( Q \) act densely on the vector space \( V \) over \( D \), where \( V \) has a nondegenerate Hermitian or alternate scalar product. Then either Case 1 or Case 2 occurs:

**Case 1 (The Hermitian case).** For every positive integer \( n \leq \dim_D V \), there exists a *-*subring \( R^{(n)} \) of \( R \) and an order \( E^{(n)} \) in \( D \) such that

1. \( R^{(n)} \) is an order in \( D_n \), and \( (E^{(n)})_n \subset R^{(n)} \subset D_n \),
2. * on \( R^{(n)} \) coincides with an involution of transpose type on \( D_n \).

**Case 2 (The alternate case).** For every positive even integer \( n = 2m \leq \dim_D V \), there exists a *-*subring \( R^{(n)} \) of \( R \) and an order \( E^{(n)} \) in \( D \) such that

1. \( R^{(n)} \simeq (E^{(n)})_n \),
2. * on \( R^{(n)} \) coincides with the symplectic involution on \( (E^{(n)})_n \).

Moreover, in either case, if \( V_0 \) is any nondegenerate subspace of \( V \) of dimension \( n \), then \( R^{(n)} \) can be chosen so that \( V_0 \cdot R^{(n)} \subset V_0 \) and \( V_0^\perp \cdot R^{(n)} = (0) \).

**Proof.** In order to relate elements in \( Q \) to those in \( R \), we need an explicit representation of the scalar product as multiplication in \( Q \). We separate the two cases.
Case 1. In this case, $Q$ contains a primitive symmetric idempotent $e = e^* = e^2$. Let $V = eQ$, $W = V^* = Qe$, and $D = eQe$. $Q$ acts by right multiplication on $V$, and the scalar product can be defined by $\langle v, w \rangle = vw^* \in D$, where $v, w \in V$. Let $V_0$ be a nondegenerate subspace of $V$ of dimension $n$, and let $\{v_1, \ldots, v_n\}$ be an orthogonal basis for $V_0$. If $\langle v_i, v_i \rangle = d_i$, let $w_i = d_i^{-1}v_i$, $i = 1, \ldots, n$. Then the $\{v_i\}$ and $\{w_i\}$ are dual bases in the sense that $\langle v_i, w_j \rangle = \delta_{ij}$, all $i, j$. One then has a set of elements $e_{ij} \in Q$, which behave like matrix units, by defining $v \cdot e_{ij} = \langle v, w_i \rangle v_j$, for all $v \in V$.

We can now mimic Smiths construction [16, Lemma 6]. For any $d \in D$, the linear transformation $e_{ij} \cdot d$ is defined as follows:

$$v \cdot (e_{ij} \cdot d) = \langle v, w_i \rangle dw_j$$

for all $v \in V$.

By taking appropriate intersections of ideals, we may find an ideal $U = U^*$ of $R$ such that $0 \neq v_i^* U \subseteq R, 0 \neq eU \subseteq R, 0 \neq Uv_i \subseteq R$, and $0 \neq Ue \subseteq R$, all $i = 1, \ldots, n$. Then let $I = U^2 \neq 0$, and let $E(n) = eIe$. By Lemma 1, $E(n)$ is an order in $D$.

Now for any $\alpha \in E(n)$, we claim that $e_{ij} \cdot \alpha \in R$, for all $i, j$. It will suffice to show this when $\alpha$ is of the form $e_{xy}$, where $x, y \in U$. Choose $v \in V$. Then

$$\langle e_{ij} \cdot \alpha \rangle = \langle v, w_i \rangle \alpha w_j = vw_i^* \alpha w_j = vw_i^* e_{xy} w_j = vw_i^* xy w_j.$$ 

That is, $e_{ij} \cdot \alpha$ is just right multiplication by $w_i^* xy w_j$, which is in $R$ by construction. Thus, $R$ contains a subring isomorphic to $(E(n))_n$.

Now let $R(n) = \{r \in R | r = \sum_{i,j} e_{ij} \cdot \alpha_{ij}, \text{ where } \alpha_{ij} \in D\}$. From the discussion preceding Lemma 1, it is clear that the adjoint on $D_n$ is an involution of transpose type, which coincides with $^*$ in $R$. Thus, if $r \in R(n)$, $r^*$ is again an element of the same form, and so $R(n)$ is a $^*$-subring of $R$. Since $R(n) \supseteq (E(n))_n$, and $E(n)$ is an order in $D$, $R(n)$ is an order in $D_n$.

Case 2. In this case, $Q$ contains no primitive symmetric idempotents. It is not difficult to show, using this fact, that there exists a minimal right ideal $\rho = eQ$ such that $xx^* = 0$, for all $x \in \rho$. Let $V = eQ$, $W = V^* = Qe$, and $D = eQe$. Now since $Q$ is prime, $eQe^* \neq 0$ so we may choose $v_0 = ebe^* \neq 0$. Using the minimality of $Qe^*$, we have $Qv_0 = Qe^*$. Now for any $x, y \in Q$ with $exy^* e^* \neq 0$, we also have $Qexy^* e^* = Qe^* = Qv_0$, and so $exy^* e^* \in eQv_0 = Dv_0$. We may therefore define the scalar product as follows: For any $v, w \in V$, let $\langle v, w \rangle = \alpha$, where $vw^* = \alpha v_0 \in Dv_0$. This is a nondegenerate, alternate scalar product on $V$.

Note also that if $\alpha \in D$, then $\alpha v_0 = v_0 \alpha^*$ (this can be shown by using the fact that $xx^* = 0$, for all $x \in eQ$).

Let $V_0$ be a nondegenerate subspace of $V$ of dimension $n = 2m$. We may choose a basis

$$\{u_1, v_1; u_2, v_2; \ldots; u_m, v_m\}$$
of \( V_0 \) such that \( \langle u_i, v_i \rangle = 1, \langle v_i, u_i \rangle = -1, \) and all other scalar products are zero. By appropriate renaming, we can find dual bases \( \{z_1, \ldots, z_{2m}\} \) and \( \{w_1, \ldots, w_{2m}\} \) in \( V \) such that \( \langle z_i, w_i \rangle = \delta_{ij} \) (for example, let \( z_1 = u_1, \)
\( z_2 = v_1, w_1 = v_1 \) and \( w_2 = u_1 \)). Then, as in the Hermitian case, we can construct matrix units \( e_{ij}, i, j = 1, \ldots, 2m \) in \( Q \) given by \( v \cdot e_{ij} = \langle v, w_i \rangle x_j \), for all \( i, j \). For any \( d \in D \), the linear transformation \( e_{ij} \cdot d \) is defined as before.

Now, using \( v_0 = ebe^* \) and the minimality of \( eQ \), we have \( eQ = v_0 Q = v_0 e^* Q \). Thus we may write \( x_i = v_0 x_i \), where \( x_i \in e^* Q \), for each \( i = 1, \ldots, 2m \).

By taking appropriate intersections of ideals, there exists an ideal \( U \) of \( R \) such that \( 0 \neq x_i^* U \subseteq R, 0 \neq eU \subseteq R, 0 \neq U w_i \subseteq R, \) and \( 0 \neq U e \subseteq R \), for all \( i = 1, \ldots, 2m \). As before let \( I = U^2 \) and let \( E^{(n)} = eIe \). Then \( E^{(n)} C = D = C \) and \( E^{(n)} \) is an order in \( C \) by Lemma 1.

We claim that for any \( \alpha \in E^{(n)}, e_{ij} \cdot \alpha \in R \). Choose any \( v \in V \). Then
\[
\psi(e_{ij} \cdot \alpha) = \langle v, w_i \rangle \alpha x_j = \langle v, w_i \rangle \alpha x_i^* x_j
\]
\[
= \langle v, w_i \rangle v_0 x_i^* x_j = v_0 x_i^* \alpha \alpha^* x_j.
\]
By construction, \( x_i^* \alpha x_i \in R \), and thus \( (x_i^* \alpha x_i)^* = w_i^* \alpha^* x_i \in R \). That is, \( e_{ij} \cdot \alpha \) is just right multiplication by an element of \( R \). Thus \( R \) contains a subring \( R^{(n)} \cong (E^{(n)})_n \). Since the adjoint on \( (E^{(n)})_n \) is just the symplectic involution, which involves no scalars in \( D \), \( R^{(n)} \) itself is a \(*\)-subring of \( R \). Thus the theorem is proved.

**Corollary 1.** Let \( R \) be a prime ring with \(*\) whose central closure has a minimal one-sided ideal. Then either \( R \) is a Goldie ring, or for every positive integer \( n \), \( R \) contains a \(*\)-subring \( R^{(n)} \) which is a prime Goldie ring of Goldie dimension \( \geq n \).

**Proof.** Immediate from Theorem 1 and Kaplansky's theorem. The \( R^{(n)} \) are Goldie rings of Goldie dimension \( n \) since they are orders in \( D_n \).

**Corollary 2.** Let \( R \) be a prime ring with \(*\) satisfying a generalized polynomial identity. Then either \( R \) satisfies a polynomial identity (PI), or for every positive integer \( n \), \( R \) contains a \(*\)-subring \( R^{(n)} \) which is a prime PI ring of PI degree \( \geq n \).

**Proof.** By a theorem of Martindale on generalized polynomial identities [11], \( RC \) is primitive one-sided ideal \( V_i \), and the commuting ring \( D \) (of \( RC \) on \( V \)) is finite-dimensional over its center \( C \). If \( \dim_C V < \infty \), then \( R \) satisfies a polynomial identity. If not, then we may apply Theorem 1 to construct the rings \( R^{(n)} \) for arbitrarily large \( n \). Since \( R^{(n)} \) has the same PI degree as \( D_n \), and \( \dim_C D_n = n^2 (\dim_C D) \), \( R^{(n)} \) will have PI degree \( \geq n \).
2. Rings in Which $xx^* = 0$ Implies $x^*x = 0$

In this section we prove the theorem mentioned in the Introduction: If $R$ is a prime ring in which $xx^* = 0$ implies $x^*x = 0$, for any $x \in R$, then either $R$ is normal or the involution is positive definite.

In order to apply Theorem 1, we will show that the central closure of $R$ has a minimal one-sided ideal. Although this could be done by applying Martindale's theorem on generalized polynomial identities, the identity that arises here is so special that a direct proof is quite easy. Also a direct proof provides the additional information (needed later) that the commuting ring is a field. The proof of the lemma is due to Herstein and will appear in [5]. We give it here for completeness.

**Lemma 2** [5]. Let $R$ be a prime ring with $a \neq 0$ in $R$ such that $ax_ay = ayax$, for all $x, y \in R$. Then $Q = RC$ is a primitive ring with minimal right ideal $V$, and the commuting ring of $Q$ on $V$ is $C$. Moreover, considered as a linear transformation on $V$, $a$ has rank 1.

**Proof.** Fixing $x$, we have $(axa)y = ay(axa)$, for all $y \in R$, and thus for all $y \in Q = RC$. By a lemma of Martindale ([11] or [3, p. 2]), $axa$ and $a$ are linearly dependent over $C$. Thus $axa = \lambda(x)a$, where $\lambda(x) \in C$, for all $x \in R$. Using $Q = RC$, we see that $aQa \subseteq Ca$.

Since $Q$ is prime, $ay_0a \neq 0$ for some $y_0 \in Q$, and so $ay_0a = \lambda a$ where $\lambda \neq 0$. Letting $x_0 = \lambda^{-1}y_0$, $ax_0a = a$, and hence $e = ax_0a$ is an idempotent.

Also, $eQe = ax_0Qax_0 = Cax_0 = Ce \cong C$, a field, and thus $V = eQ$ is a minimal right ideal of $Q$. The commuting ring is just $eQe \cong C$, and clearly $Q$ is primitive, since it is prime. Since $Va = eQe = eQea \subseteq Cea$, where $ea \in V$, $a$ must have rank 1.

**Lemma 3.** Let $R = F_n$, where $F$ is a field. Assume that $R$ has an involution $\ast$ and satisfies the condition $xx^* = 0$ implies $x^*x = 0$, for any $x \in R$. Then if $\ast$ is not positive definite on $R$, $R$ is normal and $R = F_2$ with the symplectic involution.

**Proof.** We first show that $\ast$ cannot be of transpose type. For the sake of simplicity, the proof is only given for $n = 2$, but the same proof works for $n > 2$. Let $\alpha \rightarrow \tilde{\alpha}$ be an automorphism of period $\leq 2$ on $F$. Then for any

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in F_2, \quad A^* = \begin{pmatrix} \tilde{a} & \alpha^{-1} \tilde{c} \\ \alpha \tilde{b} & \tilde{d} \end{pmatrix},$$

where $\alpha = d_2^{-1}d_1$. Now if $\ast$ is not positive definite, $AA^* = 0$ for some $A \neq 0$. $AA^* = 0$ gives that $aa + \alpha bb = 0 = \alpha^{-1}c\tilde{c} + \tilde{d}\tilde{d}$. If $A \neq 0$, then either $a \neq 0$ or $c \neq 0$ (otherwise $b = d = 0$ also). Say that $a \neq 0$ and let
B = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}. Then B^* = \begin{pmatrix} \bar{a} & 0 \\ a b & 0 \end{pmatrix}, and so BB^* = 0. However, BB^* = \begin{pmatrix} a\bar{a} & * \\ * & * \end{pmatrix} \neq 0, which is a contradiction.

We may thus assume that * is symplectic. Here we wish to show that n = 2. If not, say that n = 4. The proof in this case works for all n \geq 4. Let

\[
A = \begin{pmatrix}
0 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 \\
& & \circ & \\
& & \circ & 
\end{pmatrix}
\]

Then

\[
A^* = \begin{pmatrix}
0 & -1 & & \\
-1 & 0 & & \\
& & \circ & \\
& & \circ & 
\end{pmatrix}
\]

One can easily check that AA^* \neq 0 but that A^*A \neq 0. Thus it must be that n \leq 2. Also, it can be easily verified that if n = 2, R is normal in this case.

**Theorem 2.** Let R be a prime ring with * such that xx^* = 0, for any x \in R, implies that x^*x = 0 also. Then either

1. * is positive definite (xx^* \neq 0, for all x \neq 0), or
2. R is normal (xx^* = x^*x, for all x) and R is an order in F_2, the 2 \times 2 matrices with symplectic involution.

**Proof.** We assume that R is not an order in F_2 with the symplectic involution. Now since R^2 is an ideal of R, if R^2 were an order in F_2, R would be also. Thus we may assume that R^2 is not an order in F_2, with the symplectic involution.

Now assume also that * is not positive definite, and so there exists x \neq 0 in R such that xx^* \neq 0. Note that since Rx \neq 0, we may actually choose x \in R^2. Since R^2 is a prime ring with *, by [4, Theorem 1], R^2 must contain a symmetric nilpotent element unless R^2 is an order in F_2 and all symmetric elements are central. This can happen only in the symplectic case, which we are excluding. Thus, R^2 must contain an element a = a^* \neq 0 such that a^2 = 0.

Now for any r \in R, ra \cdot ar^* = 0, and thus by the hypothesis on R, ar^*ra = 0. Linearizing on R, we see that a(x^*y + y^*x)a = 0, for all x, y \in R; that is, a(z + z^*)a = 0, for all z \in R^2. Thenaza = -az^*a. Let
RINGS WITH INVOLUTION

$z = w a y$, where $w, y \in R^2$. Then $(a w a y) a = -a (w a y)^* a = -a y * a a * a a = -a y w a$, for all $w, y \in R^2$.

If the characteristic of $R$ is not $2$, we may let $y = w$ to see that $a w a w a = -a w a w a = 0$. Using this fact, by multiplying the equation $a w a y = -a y w a$ on the right by $w a$, we see that $a w a y w a = 0$, for all $y, w \in R^2$. Since $R^2$ is a prime ring, $a w a = 0$ for all $w \in R^2$, and so $a = 0$, a contradiction.

Therefore, we may assume from now on that $R$ has characteristic $2$. In this case, $a w a y = a y w a$ for all $w, y \in R^2$. By applying Lemma 2, we see that $Q = R^2 C$ has a minimal right ideal $V$, with commuting ring $C$, a field, and $a$ has finite rank. Let $V_0$ be any finite-dimensional nondegenerate subspace of $V$ such that $V a \subseteq V_0$ and $V_0^* a = 0$. Since $a^2 = 0$, we must have $n = \dim_C V_0 \geq 2$. Now let $a$ be represented by a matrix in $C_n$ which acts on $V_0$.

By Theorem 1, there exists an order $E$ in $C$ such that $E_n \subseteq R^2$, where $E_n$ acts on $V_0$. Thus, given any $x \in C_n$, there exists some $\alpha \neq 0$ in $C$ such that $x x \in E_n \subseteq R^2$. If for $x \in C_n$, $x x^* = 0$, then $(x x)(x x)^* = x x^* x x^* = 0$, and so since $x x \in R$, we must have $(x x)^* x x = 0 = \bar{\alpha} x x^* x x = 0$. Thus $x x = 0$, and $C_n$ satisfies the hypothesis on $R$. But now, by Lemma 3, either $*$ is positive definite on $C_n$ (an impossibility since $a \in C_n$) or $n = 2$ and $C_2$ has the symplectic involution. Thus $\dim_C V_0 = 2$, for any $V_0$, which can only happen if $\dim_C V = 2$, and $R^2 C \cong C_2$. But then $R^2$ is an order in $C_2$ (see the remark following Lemma 1), which is a contradiction. Thus, the theorem is proved.

One would hope that some version of Theorem 2 would be true when $R$ is only assumed to be semiprime; for example, that $R$ must be a subdirect product of prime rings with $*$ which are either positive definite or normal. However, this is not the case, as is seen by the following example. Let $D$ be a noncommutative division ring, and let $R = D \oplus D^6$, where $D^6$ is the opposite ring of $D$. Give $R$ the exchange involution; that is, $(a, b^0)^* = (b, a^0)$. Then $R$ satisfies the condition $x x^* = 0$ implies $x^* x = 0$, for if $x = (a, b^0)$, then $x x^* = 0$ implies $a b = 0$, and so either $a = 0$ or $b = 0$. But then certainly $x^* x = 0$. However, since $(a, 0) \cdot (a, 0)^* = 0$ for any $a \in D$, $*$ is not positive definite, and $R$ is not normal since $D$ is not commutative. $R$ has no proper homomorphic images with $*$ at all, and so cannot be a subdirect sum of "better behaved" rings with $*$.

3. Applications

In this section we apply Theorems 1 and 2 to obtain more straightforward proofs of the results on regular and nilpotent skew and symmetric elements mentioned in the Introduction [6, 13]. The next theorem was stated in [13] only for the traces, and with the additional assumption of no nil right ideals.
Theorem 3. Let $R$ be a prime ring with $\ast$ whose central closure has a minimal one-sided ideal. If every trace (or, every skew trace) is nilpotent or regular in $R$, then $R$ is a domain or an order in $\mathbb{F}_2$, for a field $F$.

Proof. First, apply Theorem 1 to get that $R$ contains subrings isomorphic to $E_n$, for any $n \leq \dim_D V$. If the scalar product is alternate, then $D = C$ is a field and the involution is symplectic. If $n > 2$, we may let

$$x = \begin{pmatrix} \alpha & 0 & \circ & \circ \\ 0 & 0 & \circ & \circ \\ \circ & \circ & \circ & \circ \end{pmatrix},$$

for any $\alpha \in E$. Then $a = x \pm x^\ast$ is a trace (skew trace) in $R$ which is neither regular nor nilpotent, a contradiction. Thus $n = 2 = \dim_D V$, and $R$ is an order in $C_2$. If $n > 2$, let

$$x = \begin{pmatrix} 0 & \alpha & \circ & \circ \\ 0 & 0 & \circ & \circ \\ \circ & \circ & \circ & \circ \end{pmatrix}$$

for any $\alpha \neq 0$ in $E$. Then for some $d_1, d_2 \in D$,

$$x^\ast = \begin{pmatrix} 0 & 0 & \circ & \circ \\ d_1\bar{\alpha}d_2^{-1} & 0 & \circ & \circ \\ \circ & \circ & \circ & \circ \end{pmatrix}.$$

Then $a = x \pm x^\ast$ is in $R$ and is neither regular nor nilpotent. Thus $n = 2$ in this case also, and so $Q = RC \cong D_2$.

Now if $D$ is not a field, then since $E$ is an order in $D$, $E$ is not commutative. Thus there exist $\alpha, \beta \in E$ such that $\alpha \beta \neq \beta \alpha$. It follows that if $x = \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} \in E_2$, then for some $\alpha \in E$, we have $x^\ast \neq x$. For,

$$x^\ast = \begin{pmatrix} d_1\bar{\alpha}d_1^{-1} & 0 \\ 0 & 0 \end{pmatrix},$$

for some $d_1 \in D$, so if $x^\ast = x$ for all $\alpha \in E$, we would have that $d_1\bar{\alpha}d_1^{-1} = \alpha$, for $\alpha \in E$. But then $d_1\bar{\beta}d_1^{-1} = \beta$ so $\alpha \beta = d_1\bar{\alpha}\bar{\beta}d_1^{-1} = d_1\bar{\alpha}d_1^{-1} = \beta \alpha$, a contradiction. Thus, for some $\alpha, a = x - x^\ast \neq 0$ and is a skew trace in $R$ which
is neither regular nor nilpotent, a contradiction. A similar argument shows that if every such \( x^* = -x \), then \( \alpha \beta = -\beta \alpha \) for all \( x \in E \), which is also impossible. Thus for some such \( x \), \( a = x + x^* \neq 0 \) is a trace in \( R \) which is neither regular nor nilpotent, again a contradiction. Thus \( D \) must be a field, so \( RC \cong C_2 \) and \( R \) is an order in \( C_2 \).

**Corollary 2** [6, Theorem 4]. Let \( R \) be a prime ring in which every nonzero skew trace (or every trace) is regular in \( R \). Then \( R \) is a domain or an order in \( F_2 \), where \( F \) is a field.

**Proof.** If every symmetric element in \( R \) is regular, then the desired conclusion holds by a theorem of Lanski [9] (for the characteristic 2 case, see [4]). Thus, we may assume that some \( s = s^* \neq 0 \) is a zero divisor.

If the traces \( T \) are regular, then since \( sTs \subseteq T \), \( sTs = 0 \). Thus \( s(x + x^*)s = 0 \), or \( sxs = -sx^*s \), for all \( x \in R \). Then \( s(xy)s = -s(y^sx^*)s = -syxys \). Thus \( R \) satisfies the generalized polynomial identity \( p(x, y) = sxys + syxys \), so by Martindale's theorem [11] \( RC \) has a minimal one-sided ideal. We are now done by Theorem 3.

An analogous argument works for the skew-traces \( K_T \).

The last corollary is related to [13, Theorem 2], where a similar result was proved for the traces only, with the additional assumption of no nil right ideals.

**Corollary 3.** Let \( R \) be a prime ring with \( * \) in which every trace (or every skew trace) is nilpotent or regular in \( R \), and assume that \( R \) is not an order in \( F_2 \), for \( F \) a field. Then \( R \) is a domain if and only if for any \( x \in R \), \( xx^* = 0 \) implies that \( x^*x = 0 \).

**Proof.** If \( R \) is a domain, then \( xx^* = 0 \) only when \( x = 0 \), and then \( x^*x = 0 \) also. Thus, we may assume that \( R \) satisfies the condition that \( xx^* = 0 \) implies \( x^*x = 0 \). By Theorem 2, \( * \) must be positive-definite on \( R \); that is, \( xx^* \neq 0 \) for any \( x \neq 0 \) in \( R \). It follows that no trace or skew trace can be nilpotent, and we are thus back into the situation of Corollary 2.

**References**