Can. J. Math., Vol. XXVIII, No. 5, 1976, pp. 915–928

RINGS WITH INVOLUTION WHOSE SYMMETRIC UNITS COMMUTE

CHARLES LANSKI

In the last few years many results have appeared which deal with questions of how various algebraic properties of the symmetric elements of a ring with involution, or the subring they generate, affect the structure of the whole ring. If the ring has an identity, similar questions may be posed by making assumptions about the symmetric units or subgroup they generate. Little seems to be known about the special units which exist in rings with involution, although several questions of importance have existed for some time. For example, given a simple ring with appropriate additional assumptions, is the unitary group essentially simple? Also, what can be said about the structure of subspaces invariant under conjugation by all unitary or symmetric units (see [**7**])?

Since results about the special units in rings with involution are scarce and seem to be difficult to obtain, one way to begin a study of these units is to try to mimic known results for the symmetric elements. A fundamental result of this kind is a theorem of Amitsur [**1**] which states that if the symmetric elements satisfy a polynomial identity, then so does the whole ring. A condition analogous to satisfying an identity for the symmetric units would be that the group they generate is solvable. As a first step toward obtaining a structure theorem, with this assumption of solvability, one might assume that the symmetric units commute. It is this condition of commutativity of the symmetric units with which we shall be concerned in this paper. Even with this relatively strong hypothesis, it is surprisingly difficult to obtain a decent structure theorem.

Throughout the paper, R will denote a ring with identity having an involution, $*$, Z will be the center of R, and $S = \{x \in R | x^* = x\}$, the set of symmetric elements of R. Lastly, G is the group of units of R and $U = \{g \in G | gg^* = g^*g = 1\}$ is the subgroup of unitary units.

We begin our study with some very easy results describing G when the symmetric units happen to lie in the center of R.

PROPOSITION 1. *$U \lhd G$ if and only if U centralizes gg^* for all $g \in G$.*

Proof. For any $u \in U$ and $g \in G$, $g^{-1}ug \in U$ exactly when $(g^{-1}ug)^* = (g^{-1}ug)^{-1}$. Equivalently, $g^*u^{-1}(g^*)^{-1} = g^{-1}u^{-1}g$, which is the same as $gg^*u^{-1} =$

Received May 27, 1975. This research was supported in part by NSF Grant GP 38601.

https://doi.org/10.4153/CJM-1976-089-9 Published online by Cambridge University Press

$u^{-1}gg^*$. Hence $U \lhd G$ exactly when each $u \in U$ centralizes gg^* for each $g \in G$.

PROPOSITION 2. *If $G \cap S \subset Z$, then $(G \cap S)U = H \lhd G$ and G/H is an abelian 2-group.*

Proof. That $H \lhd G$ follows from Proposition 1. Since $gg^* \in Z$ for each $g \in G$, it is immediate that $gg^* = g^*g$. Consequently, $(g^*)^{-1}g \in U$, and so, $g^2 = gg^*(g^*)^{-1}g \in H$. Thus each element of G/H has order two, proving the proposition.

Our next result determines when $G = (G \cap S)U$, giving a "polar decomposition" which occurs in the theory of rings of operators [**11**, Theorem 65].

PROPOSITION 3. *Suppose that $G \cap S \subset Z$. Then $G = (G \cap S)U$ if and only if for each $g \in G$, gg^* has a symmetric square root.*

Proof. Assume that $G = (G \cap S)U$ and let $g = su$ for $s \in G \cap S$ and $u \in U$. Then $gg^* = suu^*s = s^2$, so gg^* has a symmetric square root. Furthermore, since $gg^* = sug^*$, it follows that $s^2 = sug^*$, or $s = ug^*$. Thus $g = us = u^2g^*$, so $g(g^*)^{-1} = u^2$.

Conversely, if $gg^* = s^2$ for $s \in G \cap S$, set $u = gs^{-1}$. Then $u^* = s^{-1}g^*$ and $uu^* = s^{-2}gg^* = s^{-2}s^2 = 1$. Hence $u \in U$ and $g = su \in (G \cap S)U$. Note that for this half of the proof, it suffices to know that gg^* has a symmetric square root which commutes with g.

Before attempting to determine the structure of R when $G \cap S$ is abelian, we shall continue with the stronger assumption that $G \cap S \subset Z$. Using the result of Amitsur mentioned above as a guide, one would hope to show, at least when R is semi-prime, that R satisfies S_4, the standard identity of degree four. This means that for the polynomial $\sum_{\sigma \in S_4}$ (sign $\sigma)x_{\sigma(1)}x_{\sigma(2)}x_{\sigma(3)}x_{\sigma(4)}$, in non-commuting indeterminates x_1, x_2, x_3 and x_4, any substitution for the x_i by elements of R, results in zero (see [**1**]). In this case, it is well-known that R is a subdirect product of orders in simple algebras four-dimensional or less over their centers. That such examples exist with $G \cap S \subset Z$ can be seen by considering the real quaternions with the usual involution, or $M_2(F)$ for F a field with char $F \neq 2$ and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^* = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Therefore, it might be that when R is semi-prime and $G \cap S \subset Z$, R must satisfy S_4. We present an example to show that this conclusion need not follow.

To construct the example desired, we require a result of Higman [**9**] which states that for any domain D and H any direct or free product of finitely many free groups, the group ring $D[H]$ is a domain with trivial units. Thus, each unit in $D[H]$ is the product of a unit of D with an element of H.

https://doi.org/10.4153/CJM-1976-089-9 Published online by Cambridge University Press

Example 1. Let K be the free group on the set X, with card $X > 1$. By the result of Higman, for any field F, $G(F[K]) \cong F^0 \oplus K$, where $F^0 = F - \{0\}$. Define an involution on $F[K]$ by setting $k^* = k^{-1}$ for $k \in K$ and $f^* = f$ for $f \in F$. With this involution, each element of K is unitary and $G \cap S = F^0$, so $G \cap S = \subset Z$ but $F[K]$ satisfies no polynomial identity. To see this, note that for any i, $M_i(F)$ can be generated as an algebra by two units and their inverses so is a homomorphic image of $F[K]$.

Observe in Example 1 that $U(F[K]) \cong K$ and $(fk)(fk)^* = f^2$ has the symmetric square root f. Of course, this follows from Proposition 3 since $G = (G \cap S)U$. We next construct a slightly more complicated example which will exhibit a ring in which $G \cap S \subset Z$ but gg^* need not have a symmetric square root. This example will serve later as a base for other examples when we assume $G \cap S$ is abelian.

Example 2. Let K be the free group on a set X, having more than one element, and let A be a free abelian group. Using the result of Higman once again, $F[A \oplus K]$ is a domain with trivial unit group, $G(F[A \oplus K]) \cong F^0 \oplus A \oplus K$, and satisfies no polynomial identity, as in Example 1. If "$-$" is an involution of A, as a group, define an involution $*$, on $F[A \oplus K]$ by extending $f^* = f$ for $f \in F$, $a^* = \bar{a}$ for $a \in A$, and $k^* = k^{-1}$ for $k \in K$. Then $G \cap S \subset F^0 \oplus A \subset Z(F[A + K])$. In the special case where A is generated by a_1 and a_2, $a_1^* = a_2$, and $a_2^* = a_1$, $a_1a_1^* = a_1a_2$ has no symmetric square root so $G \neq (G \cap S)U$.

As we have now seen, the assumption that $G \cap S \subset Z$ can hold for domains satisfying no polynomial identity, as well as for four-dimensional simple algebras. Clearly, direct and subdirect products of such examples can give rise to semi-prime rings with $G \cap S \subset Z$. Our next result shows that any such semi-prime ring must decompose into a product of domains and orders in 2×2 matrix rings.

THEOREM 1. *Let R be a semi-prime ring with $gg^* \in Z$ for all $g \in G$. Then R is a subdirect product of domains and orders in $M_2(F)$, for fields F.*

Proof. We begin by showing that any nilpotent element of R has index 2. Let $a \in R$ with $a^k = 0$ and either $a^* = a$ or $a^* = -a$. Then $(1 + ara^{k-1})(1 + ara^{k-1})^* = (1 + ara^{k-1})(1 \pm a^{k-1}r^*a) \in Z$, which implies that $y = ara^{k-1} \pm a^{k-1}r^*a \in Z$. But $y^3 = 0$ and R is semi-prime, so $y = 0$. Should $k > 2$, then $0 = a^{k-2}y = a^{k-1}ra^{k-1}$, or $a^{k-1}Ra^{k-1} = 0$, forcing $a^{k-1} = 0$. Thus, if $a^k = 0$ and $a^* = \pm a$, we may conclude that $a^2 = 0$.

Now choose any $a \in R$ with $a^k = 0$. Then $(1 + a)(1 + a^*) \in Z$ implies that $(1 + a)(1 + a^*) = (1 + a^*)(1 + a)$, and consequently, $aa^* = a^*a$. It follows that $t = a + a^*$ is nilpotent, and since $t^* = t$, by the first paragraph we must have $t^2 = 0$. By considering $(1 + trt)(1 + trt)^* \in Z$, one obtains $t(r + r^*)t = 0$ for every $r \in R$. But $rtr^* = rar^* + (rar^*)^*$, so $0 = t(rtr^*)t =$

$-trtrt$. Thus tR is a nil right ideal of R of index 3, so the semi-primeness of R together with Levitzki's Theorem [**5**, Lemma 1.1, p. 1] forces $t = a + a^* = 0$. Therefore $a^* = -a$, so by the earlier case, $a^2 = 0$. In addition, our argument shows that if $r + r^*$ has square zero, then $r + r^* = 0$. Hence for any $a^2 = 0$, since $a^* = -a$, $ara + (ara)^* = ara + ar^*a$ must be zero.

For any $r \in R$ and $a^2 = 0$, $a(r + r^*) + (a(r + r^*))^* = a(r + r^*) - (r + r^*)a$, and $(a(r + r^*) - (r + r^*)a)^3 = 0$, so $a(r + r^*) = (r + r^*)a$. Let V be the subring of R generated by $\{r + r^* | r \in R\}$. We have shown that if $a^2 = 0$, then $av = va$ for all $v \in V$. Should V be commutative, then a result of Amitsur [**2**, Theorem 1, p. 63] implies that R satisfies S_4. Since the prime images of R satisfy this same identity, R is a subdirect product of orders in simple rings each four-dimensional or less over its center [**5**, Theorem 5.6, p. 101; **4**, Theorem 6.3.1, p. 157]. If V is not commutative, then it contains the ideal $I = I^*$ of R generated by all $v_1v_2 - v_2v_1$ for $v_i \in V$ [see the proofs of **13**, Lemma 1.1, p. 581; **5**, Lemma 1.3, p. 4]. Now $av = va$ for all $v \in V$ clearly implies $ax = xa$ for all $x \in I$. It follows that for $r \in R$, $arx = rxa = rax$, and so $(ar - ra)I = 0$. Should $a \in I$, then $ar - ra \in I \cap \mathrm{Ann}(I) = 0$, putting $a \in Z$. But $a^2 = 0$, forces $a = 0$, and as a consequence, I has no non-zero nilpotent elements. Furthermore, $ax = xa$ for $x \in I$ implies that aI is a nilpotent ideal of R, so $a \in \mathrm{Ann}(I)$. So far then, we have proved that every nilpotent element of R has square zero and is contained in the annihilator of I.

Set $A = \mathrm{Ann}(I)$ and $B = \mathrm{Ann}(A)$. Then $A \cap B = 0$, from which it follows that R is the subdirect sum of R/A and R/B. Also, since $A^* = A$ and $B^* = B$, each quotient inherits the involution from R via $(r + A)^* = r^* + A$ and $(r + B)^* = r^* + B$. By definition, $I \subset B$, and since $(r + B) + (r + B)^* = (r + r^*) + B$, all such elements of R/B commute. The fact that B is a semi-prime ideal of R allows to use the result of Amitsur [**2**, Theorem 1, p. 63] again to conclude that R/B satisfies S_4, so is a subdirect product of orders in one and four dimensional simple algebras.

We claim that R/A has no nilpotent elements. Suppose $c \in R/A$ and $c^2 = 0$. Then $c(I + A)c$ consists of nilpotent elements in $I + A$. But $I \cap A = 0$ implies that the ideal $I + A$ of R/A is isomorphic to I, so has no nonzero nilpotent elements. Hence $c(I + A)c = 0$, forces $c = 0$ since R/A is a semi-prime ring. It is known that any ring without nilpotent elements is a subdirect product of domains [**3**, Theorem 2, p. 566]. Putting together the subdirect decompositions for R/A and R/B gives the required decomposition for R.

In case R is prime, we immediately obtain

COROLLARY 1. *Let R be a prime ring with $gg^* \in Z$ for each $g \in G$. Then R is a domain or an order in $M_2(F)$.*

Turning to the assumption that $G \cap S$ is abelian raises the question of whether the structure of R differs from the case when $G \cap S \subset Z$. We shall consider prime rings and first show that $G \cap S$ can be abelian without lying in Z. Such an example can be obtained easily by taking a free product of a field and a suitable polynomial algebra over the field. All one needs, is to have units be "scalars" not commuting with all the "indeterminates." However, since the condition we are interested in concerns units, it is not reasonable to presume that strong conditions will be forced on any object larger than the subring generated by the group of units. Since the examples just mentioned are not generated by units, they are not wholly convincing. To achieve a more desirable example, we modify Example 2.

Example 3. As in Example 2, let K be a free group on a set Y having more than one element, and let A be the free abelian group on $\{x_1, x_2, x_3, x_4\}$. Then the result of Higman implies that $D = F[A \oplus K]$ is a domain satisfying no polynomial identity and $G(D) \cong F^0 \oplus A \oplus K$. Define an automorphism σ on D by extending the actions: $(f)\sigma = f$ for all $f \in F$; $(k)\sigma = k$ for all $k \in K$; and σ acts on $\{x_i\}$ like the permutation $(13)(24)$. Using σ, let $R = D[t, \sigma]$, the twisted polynomial ring over D, defined as left polynomials with $td = (d)\sigma t$ for all $d \in D$. We wish to put an involution on R much like that in Example 2. In particular, set $t^* = -t$, $f^* = f$ for all $f \in F$, $k^* = k^{-1}$ for all $k \in K$, and $x_1^* = x_2$, $x_2^* = x_1$, $x_3^* = x_4$ and $x_4^* = x_3$. To check that * extends to a well-defined involution on R, it suffices to see that the defining relation $td = (d)\sigma t$ is preserved. One computes $(td)^* \doteq -d^*t$ and $((d)\sigma t)^* = -t((d)\sigma)^* = -((d)\sigma^*)\sigma t$. These are equal since the action of σ and * commute on D and σ has order 2. Finally, since $G(R) = G(D) \cong F^0 \oplus A \oplus K$, $G \cap S \subset F^0 \oplus A$ is abelian, but is not central since $x_1x_2 \in G \cap S$, but $x_1x_2t = tx_3x_4$. Of course, $G \cap S$ is contained in the center of the subring of R generated by G, so we have not yet arrived at the example we seek.

Let $V = \{t^{2k}\}$. V is a multiplicatively closed subset of $Z(R) \cap S$, since σ^2 is the identity on D. Hence, the localization, $R_1 = RV^{-1}$, at V is still a domain satisfying no polynomial identity, and it has the induced involution $(rt^{-2k})^* = r^*t^{-2k}$. Clearly $g \in G(R_1)$ exactly when $g = ht^i$ for $h \in G(R)$ and i any integer. It follows that $G(R_1) \cap S(R_1) = \{ht^{2i} | h \in G(R) \cap S(R)\}$ is abelian but still not central in R_1. Unlike R, R_1 is generated by its units, so provides the desired example.

Assuming that R is prime and $G \cap S$ is abelian, we will show that R is a domain or satisfies S_4 if G generates R. To do this requires results not dependent on the generation of R. We continue our investigation without yet assuming more than $G \cap S$ is abelian. As a notational convenience, for $x, y \in R$, denote by $[x, y]$ the commutator $xy - yx$.

LEMMA 1. *Let R be prime with $S \cap Z \neq GF(2)$ and assume that $G \cap S$ is abelian. If $a, b, s, t \in R$ are nilpotent and $s, t \in S$ then:*

i) $[s, t] = 0$

ii) $[s, a + a^*] = [s, aa^*] = 0$

iii) $[a + a^*, bb^*] = [a + a^*, b + b^*] = 0.$

https://doi.org/10.4153/CJM-1976-089-9 Published online by Cambridge University Press

Proof. Since $1 + t$, $1 + s \in G \cap S$, $0 = [1 + s, 1 + t] = [s, t]$. Using $(1 + a)(1 + a^*)$ instead of $1 + t$ yields $[s, a + a^* + aa^*] = 0$. Choose $z \in S \cap Z$, with $z^2 \neq z$, which is possible since $S \cap Z \neq GF(2)$. Then za is nilpotent, so a may be replaced by za to obtain $z[s, a + a^*] + z^2[s, aa^*] = 0$. It follows that $(z^2 - z)[s, a + a^*] = 0$ and $(z^2 - z)[s, aa^*] = 0$, so ii) holds since $z^2 - z$ is not a zero divisor in R. To prove iii), use $(1 + b)(1 + b^*)$ in place of $1 + s$ to get $[a + a^*, b + b^*] + [a + a^*, bb^*] + [aa^*, b + b^*] + [aa^*, bb^*] = 0$. Successively substituting zb for b, then za for a will give the result.

Note that the condition $S \cap Z \neq GF(2)$ is automatically satisfied if char $R \neq 2$ or if Z contains more than four elements. Our next result is important in what follows.

THEOREM 2. *Let R be prime with $S \cap Z \neq GF(2)$ and assume that $G \cap S$ is abelian. If $a, b \in R$ with $ab = 0$, then either $aa^* = 0$ or $b^*b = 0$.*

Proof. Since $ab = 0$, each element of bRa has square zero. Applying Lemma 1 to bxa and bya gives $[bxaa^*x^*b^*, bya + a^*y^*b^*] = 0$. Using $ab = b^*a^* = 0$, this expression reduces to $bxaa^*x^*b^*bya = a^*y^*b^*bxaa^*x^*b^*$. Right multiply by a^* to get $bxaa^*x^*b^*byaa^* = 0$. The fact that R is prime and $y \in R$ is arbitrary forces the conclusion that if $aa^* \neq 0$ then

(1) $bxaa^*x^*b^*b = 0$.

Taking * applied to (1) gives $b^*bxaa^*x^*b^* = 0$. Replace b by a^*, a by b^*, and x by x^* (these substitutions work because $ab = 0$ implies $b^*a^* = 0$, and $x \in R$ is arbitrary) to obtain

(2) $aa^*x^*b^*bxa = 0$.

Next, linearize (1) by setting $x = t + y$. The result of this, $btaa^*y^*b^*b + byaa^*t^*b^*b = 0$, multiplied on the right by ta and using (2) with t in place of x yields $btaa^*y^*b^*bta = 0$. Consequently, $b^*btaa^*Rb^*btaa^* = 0$, and so, $b^*btaa^* = 0$ for all $t \in R$. This implies that $b^*b = 0$ if $aa^* \neq 0$. Therefore, either $aa^* = 0$ or $b^*b = 0$ as required.

We record some special cases when Theorem 2 gives us the result which we desire on the structure of R.

COROLLARY 2. *Let R be prime with $S \cap Z \neq GF(2)$. Assume that $G \cap S$ is abelian and that R has no non-zero nilpotent symmetric elements. Then R is a domain or an order in $M_2(F)$.*

Proof. Using a result of Herstein [**6**, Theorem 1, p. 794], if R has no non-zero nilpotent symmetric elements, then R is either an order in $M_2(F)$ or $xx^* = 0$ implies $x = 0$. Assuming that R is not an order in $M_2(F)$, the other condition, in view of Theorem 2, forces R to be a domain.

https://doi.org/10.4153/CJM-1976-089-9 Published online by Cambridge University Press

Localizing our prime ring R at its central symmetric elements gives a new prime ring R_1 whose center is a field K. If $S \cap Z(R) \neq GF(2)$ then $S \cap K \neq GF(2)$. Furthermore, $G(R) \cap S(R)$ abelian implies the same for R_1. Lastly, R_1 is a domain or an order in $M_2(F)$ exactly when R is, so there is no loss of generality in assuming that $Z(R)$ is a field.

COROLLARY 3. *Let R be prime with $S \cap Z$ a field unequal to $GF(2)$. If $G \cap S$ is abelian and R is algebraic over $S \cap Z$, then R is a domain or $M_2(F)$.*

Proof. Choose $s \in S$ and suppose that $s \notin G$. Let $p(x)$ be the minimal polynomial for s over $S \cap Z$. Then $0 = p(s) = s^k g(s)$ where x does not divide $g(x)$. Since $g(s) \in S$, applying Theorem 2 forces either $s^{2k} = 0$ or $g^2(s) = 0$. But $s \notin G$ implies that x divides $p(x)$, which must divide $g^2(x)$ if $g^2(s) = 0$. As x does not divide $g(x)$, we must conclude that s is nilpotent. Hence, each symmetric element is nilpotent or invertible. If $J(R)$ is the Jacobson radical of R, then it is nil since R is algebraic, and satisfies S_4 by Amitsur's Theorem [**2**, Theorem 1] since it is a prime ring whose symmetric elements commute. Thus $J(R)$ is nilpotent [**5**, Lemma 5.4, p. 91], so $J(R) = 0$. Using a result of Herstein and Montgomery [**8**, Theorem 7, p. 398], it follows that R is a domain or $R = M_2(F)$ (note that regular elements of R must be invertible).

We remark that if it is assumed that R satisfies a polynomial identity, the localization of R at its central symmetric elements will also satisfy this identity. In this case it is known [**16**] that the localization is a simple algebra finite dimensional over its center. Hence we obtain the conclusion of Corollary 3 by assuming that R satisfies a polynomial identity, rather than assuming that R is algebraic.

We return to a general investigation of the properties of nilpotent elements of R.

THEOREM 3. *Let R be prime with $S \cap Z \neq GF(2)$ and assume that $G \cap S$ is abelian. If s and a are nilpotent elements of R with $s \in S$ and $s^2 = 0$, then $sas = 0$.*

Proof. Since $(1 + a)(1 + s)(1 + a^*) \in G \cap S$, it follows by assumption that $[1 + s, (1 + a)(1 + s)(1 + a^*)] = 0$. This reduces to $[s, as + sa^* + asa^*] = 0$ by using Lemma 1. Replacing a by za, for $z^2 - z \neq 0$ in Z, and combining with the last expression yields $[s, as + sa^*] = 0$. Using $s^2 = 0$ gives $sas = sa^*s$. This proves the result for char $R \neq 2$ because from $[s, a + a^*] = 0$, it follows that $sas = -sa^*s$. However we may as well ignore this fact since the remainder of the proof is independent of characteristic.

From Lemma 1, $[s, aa^*] = 0$, and so $0 = [s, aa^*]s = saa^*s$. Thus $(a^*sa)^2 = 0$, and $a^*sa \in S$ implies that $[s, a^*sa] = 0$, again using Lemma 1. Consequently, $0 = [s, a^*sa]s = sa^*sas = sasas$. For any $t \in S$, replace s by sts to get $stsastsasts = 0$. Set $y = sas$ and note that y is symmetric and $ytytyty = 0$ for

https://doi.org/10.4153/CJM-1976-089-9 Published online by Cambridge University Press

all $t \in S$. In particular $(tyt)^4 = tyt^2yt^2yt^2yt = 0$ since $t^2 \in S$. But $y^2 = 0$, so $y(tyt) = (tyt)y$, which implies that $ytyty = 0$. Linearize by setting $t = t_1 + t_2$ to obtain $yt_1yt_2y + yt_2yt_1y = 0$. Right multiplication by t_1y gives $yt_1yt_2yt_1y = 0$ for any $t_1, t_2 \in S$. Consequently $(yty)S(yty) = 0$ which implies [**12**, Lemma 3.1, p. 587] that $yty = 0$. For the same reason $y = sas = 0$, proving the theorem.

COROLLARY 4. *Let R be prime with $S \cap Z \neq GF(2)$ and assume that $G \cap S$ is abelian. If $s, t \in S$ and $s^2 = t^2 = 0$, then $st = 0$.*

Proof. Since $s^2 = 0$, any $y \in sRs$ has square zero. By Theorem 3, $tyt = tsrst = 0$. Now $ts = st$ by Lemma 1, so $stRst = 0$. The fact that R is prime forces $st = 0$.

Corollary 4 allows us to conclude that R is a domain or an order in $M_2(F)$ under hypotheses that guarantee a reasonable richness of units in R. Before stating our main result we require a definition.

Definition. An additive subgroup L of R is called a *Lie ideal* of R if $[x, r] \in L$ for all $x \in L$ and all $r \in R$.

THEOREM 4. *Let R be prime with $S \cap Z \neq GF(2)$ and assume that $G \cap S$ is abelian. If R satisfies any of the conditions:*

A) *G generates R as a ring,*

B) *the Z subalgebra generated by the quasi-regular elements of R contains a non-central Lie ideal of R,*

C) *R contains a non-zero, non-identity idempotent,*

then R is a domain or an order in $M_2(F)$.

Proof. Should R contain no non-zero nilpotent elements, the conclusion follows from Corollary 2. Thus, we may assume that there is $s \in S$ with $s^2 = 0$ and $s \neq 0$. For any $g \in G$, $[1 + s, gg^*] = 0$ by assumption, so $sgg^* = gg^*s$, and $sgg^*s = 0$. Consequently $(g^*sg)^2 = 0$, and since $g^*sg \in S$, we have by Corollary 4 that $(g^*sg)s = 0$, or simply, $sgs = 0$. Assuming Condition A, every element of R is a finite sum of units, so $sRs = 0$ forcing $s = 0$. This contradiction forces the conclusion that R cannot have non-zero nilpotent symmetric elements in the presence of Condition A.

Next assume that Condition B holds and that L is the Lie ideal. If q is any quasi-regular element of R, $1 + q \in G$, so by our argument above $s(1 + q)s = sqs = 0$. Proceeding by induction, suppose that $sq_1q_2 \ldots q_ks = 0$ for $\{q_i\}$ quasi-regular elements and $k \leqq n$. If $q_1, q_2, \ldots, q_{n+1}$ are quasi-regular, then $g = (1 + q_1)(1 + q_2) \ldots (1 + q_{n+1}) \in G$, so $sgs = 0$. The induction assumption now implies that $sq_1q_2 \ldots q_{n+1}s = 0$. Of course, the same relation holds for any q_i replaced by zq_i for any $z \in Z$. This shows that $sMs = 0$ where M is the Z-subalgebra generated by the quasi-regular elements of R. Clearly, the subring L' generated by L lies in M. It is well-known that the subring generated by a non-central Lie ideal must contain a non-zero ideal of R, unless R is an order in $M_2(F)$ [**5**, Lemma 1.3, p. 4; **13**, Theorem 4, p. 118].

Denoting this ideal by I, it follows that $sIs = 0$, and so, $s = 0$ by the primeness of R. Therefore, in the presence of Condition B, R cannot have non-zero nilpotent symmetric elements.

Lastly, assume Condition C. Let E be additive subgroup generated by the idempotents of R. For any idempotent e and any $r \in R$ $er - re = er(1-e) - (1-e)re = e + er(1-e) - (e + (1-e)re) \in E$. This shows that E is a (non-commutative) Lie ideal of R and that the Lie ideal $[E, R]$ is contained in the additive subgroup generated by the nilpotent elements of R. Note that $[E, R] \subset Z$ implies $[er(1-e) - (1-e)re, e] = 0$, from which it would follow that $eR(1-e) = 0$ forcing $e = 0$ or $e = 1$. Hence Condition C reduces to Condition B, completing the proof of the theorem.

Although the conditions in Theorem 4 are sufficient to imply the conclusion that R is a domain or an order in $M_2(F)$, it is not clear that any condition, in addition to the assumption $G \cap S$ is abelian, is necessary. To show that some other hypothesis is required we present another example.

Example 4. This example is attributed to Martindale [**15**, p. 136]. For any field F, let R be the quotient of the free algebra $F\{x, y\}$ by the ideal (x^2). Then R is a prime ring in which $ab = 0$ implies $a \in Rx$ and $b \in xR$. It follows that a unit in R has the form $f + gx$ or $f + xrx$ for $f,g \in F^0$ and $r \in R$. Consequently G is an abelian group, but not central. Define an involution on R by extending $f^* = f$, $x^* = x$, and $y^* = y$. Then $G \cap S$ is abelian, but not central, and R is neither a domain nor a subring of $M_n(K)$ for any positive integer n and field K. The last statement holds because R has as homomorphic images, all $M_n(F)$, so cannot satisfy any polynomial identity.

In view of the fact that in Example 4 $G \cap S$ is abelian, one might ask what conditions, other than those listed in Theorem 4, would serve to eliminate this example from consideration. One property of the example, which led to its use as a counter-example elsewhere [**15**], is its lack of left-right symmetry with respect to zero divisors. Although it has no obvious relation to the assumption about $G \cap S$, a hypothesis of such symmetry is enough to force R to be a domain or an order in $M_2(F)$. In the process of showing this, it will become clearer that a ring for which $G \cap S$ is abelian, but which is neither a domain nor an order in $M_2(F)$, must closely resemble Example 4.

Our next goal is to show that the usual conclusions for R will hold if it can be embedded nicely in a primitive ring. We prove a technical result about such rings.

LEMMA 2. *Let R be primitive with a minimal-right ideal and assume that $R \neq M_2(F)$. If R contains non-zero nilpotent symmetric elements then there exist non-zero $s, t \in R$ with $s^* = s$, $s^2 = t^2 = 0$, and $sts = s$.*

Proof. Using a result of Kaplansky [**10**, Theorem 2, p. 83], we may regard R as a ring of transformations on a self-dual vector space V, over a division

https://doi.org/10.4153/CJM-1976-089-9 Published online by Cambridge University Press

ring D, so that the elements of R are continuous with respect to a non-degenerate form $(\, , \,) : VxV \to D$. Furthermore, the involution on R is the adjoint with respect to this form, R contains all continuous transformations of finite rank, and $(\, , \,)$ is either Hermitian or alternate; in the second case $D = F$ and $*$ is the identity on F.

Assume that R contains non-zero nilpotent elements, and first consider the case when $(\, , \,)$ is Hermitian. For $x^* = x \in R$ with $x^2 = 0$, $(vx, vx) = (vx^2, v) = 0$ for all $v \in V$. Thus, there exist non-zero $v \in V$ with $(v, v) = 0$. Choose such a v and using non-degeneracy of the form, choose $w \in V$ with $(v, w) = 1$. If $(w, w) = d$, let $y = w - dv$, then $(y, w) = (w - dv, w) = d - d = 0$, and $(y, v) = (w - dv, v) = 1 - 0 = 1$. Set $s = (\, , v)v$ and $t = (\, , w)y$. It is easy to verify that $s^* = s$, and that $s^2 = t^2 = 0$. Furthermore

$$\begin{aligned} sts &= ((\, , \, v)v) \circ ((\, , \, w)y) \circ ((\, , v)v) \\ &= ((\, , \, v)y) \circ ((\, , v)v) \\ &= (\, , v)v = s. \end{aligned}$$

Therefore, this s and t satisfy the requirements of the lemma.

We turn now to the case when $(\, , \,)$ is alternate and $D = F$. Choose $u, v \in V$ independent over F with $(u, v) = 0$. This is possible unless $\dim_F V = 2$, in which case $R = M_2(F)$, since the annihilator of u has codimension one, for any $u \in V$. Choose $w \in V$ with $(w, v) = 1$. If $(w, u) \neq 0$, let $u_1 = u - (w, u)v$. Clearly $(u_1, v) = 0$ and $(w, u_1) = 0$ so we may assume that $(w, u) = 0$ to begin with. Next, choose $y \in V$ with $(y, u) = 1$. If necessary, we may replace v by a linear combination of v and u so that we may assume $(y, v) = 0$, without changing $(w, v) = 1$. Should $(y, w) \neq 0$, let $w_1 = w - (y, w)u$. Then $(y, w_1) = 0$, $(w_1, u) = 0$, and $(w_1, v) = 1$. In conclusion, $(v, w) = 1 = (y, u)$ and any other "products" of the four vectors is zero. Set $s = (\, , u)v - (\, , v)u$ and $t = (\, , w)y - (\, , y)w$. Then $s^* = s$ and $t^2 = s^2 = 0$. However,

$$\begin{aligned} sts &= ((\, , u)v - (\, , v)u) \circ ((\, , w)y - (\, , y)w) \circ ((\, , u)v - (\, , v)u) \\ &= ((\, , u)y + (\, , v)w) \circ ((\, , u)v - (\, , v)w) \\ &= (\, , u)v - (\, , v)u = s \end{aligned}$$

The elements s and t are those required, and the lemma is proved.

Combining Lemma 2 and Corollary 4 gives the result that if R is primitive with minimal one sided ideal and $G \cap S$ is abelian, then R is a division ring or $R = M_2(F)$.

Primitive rings with minimal right ideals arise from prime rings which satisfy a generalized polynomial identity. Recall that a prime ring with center Z is said to satisfy a *generalized polynomial identity* (*GPI*) if for some non-zero element $f(x_1, \ldots, x_n) \in R*_Z Z\{x_1, \ldots, x_n\}$, the free product of R with the free algebra in $\{x_1, x_2, \ldots, x_n\}$ over Z, $f(r_1, r_2, \ldots, r_n) = 0$ for all choices of $r_i \in R$. According to a theorem of Martindale [**14**, Theorem 3, p. 579], a

https://doi.org/10.4153/CJM-1976-089-9 Published online by Cambridge University Press

prime ring which is GPI is embedded in a primitive ring P with minimal right ideal, so that $P = RC$ where C is the center of P and a field containing Z. Moreover, the involution on R extends to P, and given $y \in P$ there exists an ideal W of R so that $yW \subset R$ and $y = 0$ exactly when $yW = 0$ for $W \neq 0$. [**14**, p. 577]. Using this result, we can prove our next theorem.

THEOREM 5. *Let R be prime with $S \cap Z \neq GF(2)$ and assume that $G \cap S$ is abelian. If R satisfies a GPI then R is a domain or an order in $M_2(F)$.*

Proof. By the discussion above, we can regard R as embedded in $P = RC$, a primitive ring with minimal right ideal. Suppose that $s, t \in P$ with $s^* = s$ and $s^2 = t^2 = 0$. From the construction of P [**14**] there exists a non-zero ideal W of R so that $W^* = W$ and sW, tW, and t^*W are non-zero right ideals of R. For $x \in W^2 \cap S$ and $y \in W^2$, sxs and tyt are elements of square zero in R and sxs is symmetric. Using Theorem 3, $sxstytsxs = 0$. Since P is prime, y is arbitrary in W^2, and W^2C is an ideal of P, it follows that $tsxst = 0$. For any $a \in W^4 \cap S$, $tat^* \in W^2 \cap S$, so $tstat^*st = 0$. Consequently, for any $y \in W^4$ we have $tst(y + y^*)t^*styt^*st = 0$. Since $y^*t^*sty \in W^4 \cap S$, this expression reduces to

$$(3) \quad tstyt^*styt^*st = 0.$$

Linearizing Equation (3) results in $tstyt^*stxt^*st + tstxt^*styt^*st = 0$. Multiply on the right by yt^*st^* and use (3) with the involution applied to get

$$tstyt^*stxt^*styt^*st^* = 0.$$

For any fixed $y \in W^4$, the primeness of P again implies that $tstyt^*st = 0$, and so, that $tst = 0$ or $t^*st = 0$.

Assume that R is not an order in $M_2(F)$. Then $P \neq M_2(F)$ and Lemma 2 implies that P has no non-zero nilpotent elements, or there exist $s, t \in P$ with $s^* = s$, $s^2 = t^2 = 0$, and $sts = s$. In the latter case, as we have seen, either $tst = 0$ or $t^*st = 0$. But $sts = s$ implies that $st^*s = s$, hence $stst = st = 0$ or $st^*st = st = 0$, contradicting $sts = s \neq 0$. Therefore, we must conclude that P has no non-zero nilpotent elements. Since the same holds for R, an application of Corollary 2 proves the theorem.

We use Theorem 5 first to indicate how close R must be to Example 4 if the usual conclusion does not follow from $G \cap S$ abelian.

COROLLARY 5. *Let R be prime with $S \cap Z \neq GF(2)$ and assume that $G \cap S$ is abelian. Then the nilpotent symmetric elements form a subring with trivial multiplication unless R is a domain or an order in $M_2(F)$.*

Proof. By Corollary 4 it suffices to show that $s^k = 0$ for $s \in S$ implies $s^2 = 0$. Suppose that $s^{k-1} \neq 0$, $s^k = 0$ and $k \geqq 3$. Let $y = srs^{k-1} + s^{k-1}r^*s \in S$. It is trivial that $y^3 = 0$, so by Lemma 1, $0 = [s, y] = s^2rs^{k-1} - s^{k-1}r^*s^2$. If $k \geqq 4$, multiply on the left by s^{k-3} to get $0 = s^{k-1}rs^{k-1}$, which implies

https://doi.org/10.4153/CJM-1976-089-9 Published online by Cambridge University Press

$s^{k-1} = 0$. This contradiction forces $k = 3$. Now we have $s^2rs^2 = s^2r^*s^2$ for all $r \in R$, and so, $s^2rs^2ws^2 = s^2w^*s^2r^*s^2 = s^2ws^2rs^2$. Should $s^2 \neq 0$, R satisfies a GPI and Theorem 5 implies the corollary.

One more lemma is required to enable us to exploit Theorem 5. The lemma will provide a setting in which a prime ring will satisfy a GPI.

LEMMA 3. *Let R be prime and assume that for some $x \in R$, $xSx^* = 0$. Then either $x = 0$ or R satisfies a GPI.*

Proof. First observe that for any $t \in S$, $x^*txSx^*tx = 0$. Since $x^*tx \in S$ it follows easily that $x^*tx = 0$ [**12**, Lemma 3.1, p. 587], and so, $x^*Sx = 0$. For any $r \in R$, $x(r + r^*)x^* = 0$. If $y = xrx^*$, then $y^* = -y$ and $ySy = xrx^*Sxrx^* = 0$. Repeating this procedure gives $y(a + a^*)y = 0$ for any $a \in R$; and so,

$$yayby = -yb^*y^*a^*y = -ybya^*y = ybyay$$

for any $a, b \in R$. Consequently, R satisfies a GPI unless $y = 0$. Equivalently, $xrx^* = 0$ for all $r \in R$, and $x = 0$ since R is prime.

Putting the last few results together allows us to obtain the usual conclusion for R if we ensure that Example 4 does not arise by assuming a suitable left-right symmetry for zero divisors. Note that the condition we state must hold in domains and in $M_2(F)$.

THEOREM 6. *Let R be prime with $S \cap Z \neq GF(2)$ and assume that $G \cap S$ is abelian. If $xx^* = 0$ implies that $x^*x = 0$, then R is a domain or an order in $M_2(F)$.*

Proof. We begin by assuming that $ab = 0$ for $a, b \in R$. By Theorem 2, either $aa^* = 0$ or $b^*b = 0$. Suppose that $aa^* \neq 0$. For any $s \in S$, $y = bsb^* \in S$ and $y^2 = 0$. Since $(ry)(ry)^* = ry^2r^* = 0$, the hypothesis implies that $(ry)^*(ry) = yr^*ry = 0$ for all $r \in R$. It follows that $ryr^* \in S$ and is nilpotent, so by Corollary 4 or Corollary 5, $ryr^*y = 0$. Linearizing gives $ryw^*y + wyr^*y = 0$, and multiplication on the right by ry yields $ryw^*yry = 0$. Now $w^* \in R$ is arbitrary, and R is prime, hence $yry = 0$, which implies, in turn, that $y = bsb^* = 0$. An application of Lemma 3 forces $b = 0$ or R to satisfy a GPI. If R satisfies a GPI, we are finished by Theorem 5, so $b = 0$. Consequently, unless R is a domain, whenever $ab = 0$, it must be that $aa^* = 0$. A similar argument shows that $b^*b = 0$, as well.

Let $a, b \in R$ be any zero-divisors. From $aa^* = b^*b = 0$, it follows that a^*Sa and bSb^* consist of symmetric nilpotent elements. As we have observed in Lemma 1, such elements commute. Therefore, $a^*sabtb^* = btb^*a^*sa$ for any $s, t \in S$. Multiply on the right by a^* to get $a^*sabtb^*a^* = 0$, and set $y = abtb^*a^*$. Clearly, $y^* = y$ and $ySy = 0$. It follows, as in the proof of Lemma 3, that $y = 0$. This is equivalent to $abS(ab)^* = 0$, and using Lemma 3 again yields that $ab = 0$ or R satisfies a GPI. As we have seen, the proof is complete

https://doi.org/10.4153/CJM-1976-089-9 Published online by Cambridge University Press

if R satisfies a GPI. Hence, $ab = 0$ for any zero divisors a and b. But if a is a zero divisor, then ra is also, for any $r \in R$. Therefore $ara = 0$, which implies that $a = 0$, forcing R to be a domain and completing the proof.

Our final result is a somewhat different approach, since it does not involve nilpotent elements. The assumption we make comes from the property of C^*-algebras that $1 + xx^*$ is invertible for each $x \in R$.

THEOREM 7. *Let R be prime and assume that $G \cap S$ is abelian. If $1 + x \in G$ for each x satisfying $x + x^* = 0$, then R is a domain or an order in $M_2(F)$.*

Proof. If char $R = 2$ then $1 + s \in G$ for each $s \in S$, so the symmetric elements commute, which implies that R satisfies S_4 by the result of Amitsur [**2**, Theorem 1]. As in the proof of Theorem 1, it follows that R is an order in a simple algebra at most four-dimensional over its center. Hence, we may assume that char $R \neq 2$.

Let $k = \{x \in R | x^* = -x\}$. Each $k \in K$ is quasi-regular in R, and k_1k_2 is in the Z-subalgebra generated by K. It is easy and well-known that K^2, the additive subgroup generated by all k_1k_2 is a Lie ideal of R [**5**, p. 28]. If $K^2 \not\subset Z$, then an application of Theorem 4 finishes the proof. Therefore, assume that $K^2 \subset Z$. In particular $k_1k_2 \in Z$, so $[k_1k_2, k_2] = [k_1, k_2]k_2 = 0$. But $[k_1, k_2] = k_1k_2 - k_2k_1 \in Z$ whose non-zero elements are not zero-divisors in R. Consequently, $[k_1, k_2] = 0$ for all $k_1, k_2 \in K$, which implies $[x - x^*, y - y^*] = 0$ for any $x, y \in R$. Using the result of Amitsur [**2**, Theorem 1] again, yields the fact that R satisfies S_4, so is an order in a simple algebra at most four-dimensional over its center.

REFERENCES

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

2. ——— *Identities in rings with involutions*, Israel J. Math. *7* (1969), 63–68.

3. V. A. Andrunakievic and M Rjabuhin, *Rings without nilpotent elements, and completely simple ideals*, Soviet Math. Dokl. *9* (1968), 565–567.

4. I. N. Herstein, *Non-commutative rings*, The Carus Mathematical Monographs *15* (The Mathematical Assn. of America, 1968).

5. ——— *Topics in ring theory* (The University of Chicago Press, Chicago, 1969).

6. ——— *On rings with involution*, Can. J. Math. *26* (1974), 794–799.

7. ——— *A unitary version of the Brauer-Cartan-Hua theorem*, J. of Algebra *32* (1974), 554–560.

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

9. G. Higman, *The units of group-rings*, Proc. Lond. Math. Soc. *46* (1940), 231–248.

10. N. Jacobson, *Structure of rings*, Amer. Math. Soc. Coll. Pub. *37* (American Mathematical Society, Providence, 1964).

11. I. Kaplansky, *Rings of operators* (W. A. Benjamin, Inc., New York, 1968).

12. C. Lanski, *On the relationship of a ring and the subring generated by its symmetric elements*, Pacific J. Math. *44* (1973), 581–592.

13. C. Lanski and S. Montgomery, *Lie structure of prime rings of characteristic 2*, Pacific J. Math. *42* (1972), 117–136.

14. W. S. Martindale, *Prime rings satisfying a generalized polynomial identity*, J. of Algebra *12* (1969), 576–584.

15. S. Montgomery, *Rings with involution in which every trace is nilpotent or regular*, Can. J. Math. *26* (1974), 130–137.

16. L. Rowen, *Some results on the center of a ring with polynomial identity*, Bull. Amer. Math. Soc. *79* (1974), 219–223.

University of Southern California,
Los Angeles, California

https://doi.org/10.4153/CJM-1976-089-9 Published online by Cambridge University Press