Can. J. Math., Vol. XXX, No. 1, 1978, pp. 85–94

INVARIANT SUBRINGS IN RINGS WITH INVOLUTION

CHARLES LANSKI

The purpose of this paper is to consider, in rings with involution, the structure of those subrings which are invariant under Lie commutation with $[K, K]$. Our goal is to find conditions which force such subrings to contain a noncentral ideal of the ring. Of course, the subring itself may lie in the center. Orders in 4×4 matrix rings over fields are known to provide examples of invariant subrings which are not central and contain no ideal (see [**1**, 40] or [**5**]). Except for subdirect products of these two kinds of "counter-examples", we show that in semi-prime rings, invariant subrings do contain noncentral ideals. This generalizes work of Herstein [**4**] in two directions by considering semi-prime rings rather than simple rings, and by using $[K, K]$ instead of K. Also, the work here is a natural extension of that in [**5**], where similar results are obtained for subrings generated by elements of K. Our hope is that these results will prove useful, in the same way that [**4**] was used in [**3**], for the study of the unitary group and subrings invariant under the unitary group.

Throughout the paper, R will denote a 2-torsion free semi-prime ring with involution, $*$, and center, Z. Set $S = \{r \in R | r^* = r\}$ and $K = \{r \in R | r^* = -r\}$. More generally, for any ring A with involution, we write $Z(A)$, $S(A)$, and $K(A)$, for the subsets corresponding to those above. The notation $[x, y] = xy - yx$, for $x, y \in R$, will be used extensively, and $[A, B]$ will denote the additive subgroup generated by all $[a, b]$ for $a \in A$ and $b \in B$. If A is an additive subgroup then A' will be the subring generated by A. Lastly, let $V = [K, K]$.

In order to shorten many statements, in both our theorems and proofs, which must take into account the finite dimensional matrix example mentioned above, we follow the notation in [**5**]. Therefore, we will say that a prime ring satisfies S_{2n} if it is an order in a simple algebra of dimension at most n^2 over its center, and a semi-prime ring satisfies S_{2n} if it is a subdirect product of prime rings, each of which satisfies S_{2n}. One thinks of this condition in the semi-prime case as corresponding to a finite dimensional restriction for simple rings. Of course, the notation comes from the theory of polynomial identities, although results from this area are not explicitly used here.

Overall, the techniques employed are those that have become fairly standard in treating rings with involution, and the computations, while involved, are initially similar to those used in [**4**] and earlier works in the subject (see [**1**]). Our first result is a technical lemma about nilpotent elements which will be useful in Theorem 1.

Received September 10, 1976. This research was supported by N.S.F. Grant MPS73-08746.

https://doi.org/10.4153/CJM-1978-007-8 Published online by Cambridge University Press

LEMMA 1. *Let A be a subring of R contained in S and satisfying $[A, V] \subset A$. Then the following hold:*

1) *If $a \in A$ and $a^2 = 0$, then $aKa = 0$.*
2) *If $N = \{a \in A | a^t = 0\}$, then $N^3 = 0$.*

Proof. First note that A is commutative, since $xy = (xy)^* = yx$, for $x, y \in A$. Let $a \in A$ with $a^2 = 0$, and let $v \in V$. Then $[a, v] \in A$, so the commutativity of A implies that $0 = [a, [a, v]] = a(av - va) - (av - va)a = -2ava$. The 2-torsion freeness of R gives $aVa = 0$. Consequently, if $k \in K$, then $(aka)V(aka) = 0$ and we have $aka \in K$ with $(aka)^2 = 0$. It follows [**5**, Lemma 7] that $aka = 0$. Therefore $a(r - r^*)a = 0$ for any $r \in R$, or equivalently, $ara = ar^*a$. Now let $b \in N$ and let t be minimal with $ab^t = 0$. Should $t > 1$, then $a(b^{t-1}r)a = a(b^{t-1}r)^*a = ar^*b^{t-1}a$. Right multiplying by b, using the commutativity of A, yields $ab^{t-1}rab = 0$. Since R is semi-prime, one may conclude that $ab^{t-1} = 0$, contradicting the minimality of t. Thus $aN = 0$ if $a^2 = 0$. In particular, if $b \in N$ with $b^n = 0, b^{n-1} \neq 0$ and $n > 3$, then $(b^{n-2})^2 = 0$, so by what we have already shown, $b^{n-2}b = b^{n-1} = 0$. Hence, every element of N has cube equal to zero. Now for $a, b \in N$, since $(a^2)^2 = 0$, we have $a^2b = 0$, and so $(ab)^2 = 0$, using the commutativity of A once again. Consequently, $abN = 0$. Therefore, $N^3 = 0$, completing the proof of the lemma.

The next result is implicit in [**5**] and is used to obtain another technical lemma required in Theorem 1. Recall that * is said to be of the *first kind* if $Z \subset S$, and of the *second kind* otherwise.

LEMMA 2. *If R is a prime ring, then V' contains a nonzero ideal of R, unless R satisfies S_4.*

Proof. Applying [**5**, Lemma 3 and Sublemma], either V' contain a nonzero ideal of R or $x^2 \in Z$ for all $x \in V$. If * is of the second kind then [**5**, Lemma 6] implies that R satisfies S_4 or $K \subset Z$, which in turn implies that R is commutative, since $2tR \subset K + tK$ for any $t \in Z \cap K$. Finally, if * is of the first kind, then the proof of [**5**, Lemma 9] shows that R satisfies S_4 or else one may reduce to the case where R is simple and $Z \neq 0$. Now an examination of [**1**, 36-40] shows that when R is simple V must be 3-dimensional over Z and have a nonzero centralizer in K, disjoint from V and contained in V! This absurdity shows that R must satisfy S_4.

LEMMA 3. *Let R be a prime ring and L any nonzero additive subgroup of R satisfying $[L, V] \subset L$. If either $Lx = 0$ or $xL = 0$, then $x = 0$ unless R satisfies S_4.*

Proof. Assume that $xL = 0$. Since $xyv = 0$ for $y \in L$ and $v \in V$, it follows that $0 = x[y, v] = xvy$. Repeating the argument gives $xV'L = 0$. If R does not satisfy S_4, then V' contains a nonzero ideal by Lemma 2. Hence $x = 0$, since R is prime and $L \neq 0$. Clearly, a similar argument works if $Lx = 0$.

https://doi.org/10.4153/CJM-1978-007-8 Published online by Cambridge University Press

In obtaining a structure theorem for subrings invariant under commutation by V, our approach generally parallels that used in [**4**]. Since information is available from [**5**] if the subring contains elements of K, one must eventually consider the possibility that the subring is contained in S. Eliminating this case, as in [**4**], is perhaps the most difficult part of the investigation, and is accomplished in our first theorem.

THEOREM 1. *Let A be a (commutative) subring of R contained in S, and satisfying $[A, V] \subset A$. Then R is a subdirect sum of semi-prime, *-homomorphic images R_1 and R_2 so that R_1 satisfies S_6, and the image of A in R_2 is central. Furthermore, if R is 6-torsion free, then R_1 satisfies S_4.*

Proof. We first note that since R is 2-torsion free, the intersection of all the prime ideals P of R satisfying $2R \not\subset P$, is zero. For the remainder of this proof, *all* prime ideals considered will be of this type. Our goal is to show, for each such prime P, that either R/P satisfies S_6 or $A + P \subset Z(R/P)$. Should this dichotomy hold, we let I be the intersection of all such primes with R/P satisfying S_6 and J the intersection of the others. If necessary, let the empty intersection equal R. Then $R_1 = R/I$ and $R_2 = R/J$ satisfy the conditions of the theorem. Observe that $I^* = I$ and $J^* = J$ since R/P satisfies S_6 exactly when R/P^* does.

Suppose that P is a prime ideal of R, $2R \not\subset P$, and $P^* \neq P$. Then $P^* + P$ is a nonzero ideal of R/P and $P^* + P \subset K + P$ since $x^* + P = x^* - x + P$ for any $x \in P$. Consequently, $[A, [P^*, P^*]] + P \subset [A, [K, K]] + P \subset A + P$. Now $[P^*, P^*] + P$ is a Lie ideal of R/P (see [**1**]), so using a result of Herstein [**2**, Theorem 3, p. 566] we have that either $A + P$ contains a nonzero ideal of R/P or that $A + P$ commutes with $[P^*, P^*] + P$. In the first case, the commutativity of A would force R/P to be commutative, and so R/P satisfies S_t for all $t \geqq 2$. If we assume that $A + P$ commutes with the Lie ideal $[P^*, P^*] + P$, then [**6**, Lemma 8, p. 120] implies that $A + P \subset Z(R/P)$, or $[P^*, P^*] + P \subset Z(R/P)$. Another application of this same result to the second possibility yields $P^* + P \subset Z(R/P)$, or that R/P is commutative. Therefore if $P^* \neq P$, then R/P is commutative or $A + P \subset Z(R/P)$.

Turning to prime ideals P with $2R \not\subset P$ and $P^* = P$, note that R/P has the induced involution $(r + P)^* = r^* + P$. The first difficulty we face, is that $A + P$ may not be invariant under commutation with $V(R/P)$ since $K(R/P)$ may contain elements not in $K + P$. To eliminate this problem, consider $(R/P) \otimes_J J[1/2]$, where J is the ring of integers. Since R/P is 2-torsion free, R/P is embedded inside this new prime ring, R/P satisfies S_{2n} exactly when $(R/P) \otimes J[1/2]$ does, and $A + P \subset Z(R/P)$ exactly when $(A + P) \otimes J[1/2] \subset Z(R/P) \otimes J[1/2]$. The advantage of this new ring, is that with the involution $((r + P)/2^t)^* = (r^* + P)/2^t$, one has $K((R/P) \otimes J[1/2]) = (K + P) \otimes J[1/2]$, so that $(A + P) \otimes J[1/2]$ is invariant under commutation with $[L, L]$ for $L = K((R/P) \otimes J[1/2])$. To simplify notation we shall go

https://doi.org/10.4153/CJM-1978-007-8 Published online by Cambridge University Press

back to using R and A, but may now assume that R is prime and $2R = R$. We must show that $A \subset Z$ or R satisfies S_6.

Next we consider what happens when $Z \not\subset S$. There must be $t \in K \cap Z$, and since $2tr = t(r + r^*) + t(r - r^*)$ for $r \in R$, we have $tr \subset K + tK$. It follows that $t^2[R, R] \subset Z[K, K]$, and so $[AZ, t^2[R, R]] \subset [AZ, Z[K, K]] \subset AZ$. Therefore, t^2AZ is a subring of R invariant under commutation with $[R, R]$. The same argument as above, in the case when $P^* \neq P$, allows us to conclude that R is commutative or that $t^2AZ \subset Z$. The second possibility, together with the primeness of R, forces $A \subset Z$. It remains to consider involutions of the first kind, when $Z \subset S$, and henceforth we assume that this is the case.

If $a \in A$, set $d(x) = ax - xa$ for any $x \in R$. Note that $d(\quad)$ is a derivation on R; that is, $d(\quad)$ is an additive map and $d(xy) = xd(y) + d(x)y$. For $v \in V$ and $k \in K$, $[k, v] \in V$ so $d([k, v]) \in A$. The commutativity of A implies that $d^2([k, v]) = 0$. Expanding this expression, using the fact that $d(\quad)$ is a derivation, and that $d^2(v) = 0$, gives $[d^2(k), v] + 2[d(k), d(v)] = 0$. Now $A \subset S$ means $d^2(k) \in K$, so $[d(k), d(v)] \in [K, K]$. As a consequence, $0 = d^2([d(k), d(v)]) = [d^3(k), d(v)]$. Also, $0 = d^2([d^2(k), v]) = [d^4(k), v] + 2[d^3(k), d(v)] = [d^4(k), v]$. Clearly, $d^4(k)$ commuting with V forces $d^4(k)$ to commute with V'. But by Lemma 2, unless R satisfies S_4, V' certains a nonzero ideal. Therefore, assuming that R does not satisfy S_4 implies that $d^4(k) \in Z$. It is immediate that $d^4(k) \in K$. Since $Z \subset S$, we must conclude that $d^4(k) = 0$ for all $k \in K$. But $[A, S] \subset K$, so $d^4([a, s]) = d^5(s) = 0$ for all $s \in S$. Consequently, unless R satisfies S_4, $d^5(R) = d^5(S + K) = 0$. We assume to end the proof that R does not satisfy S_4.

Suppose that char $R \neq 3, 5$. For $v \in V$, one can easily show that $0 = d^5(v^5) = 60d(v)^5$, and so $d(v)^5 = 0$. Setting $N = \{b \in A | b^t = 0\}$, we have shown that $d(v) \in N$. Apply Lemma 1 to get $N^3 = 0$. Now $[a, v] \in N$ for any $a \in A$ and $v \in V$, so, in particular, $[N, V] \subset N$. We may now use Lemma 3 to get $N^2 = 0$, and then use it again to get $N = 0$. However, $[A, V] \subset N = 0$ means that A commutes with V', and so, $A \subset Z$ follows from Lemma 2.

It remains to show that when R does not satisfy S_4 and when char R is 3 or 5, then $A \subset Z$. The procedure at this point is to prove that some power of each element of A is central and then reduce the situation to the case when R is simple. If char $R = 5$, then expanding the expression $d^5(x) = 0$, for all $x \in R$, shows that $a^5 \in Z$ for each $a \in A$. If char $R = 3$ we want that $a^3 \in Z$, but the proof is somewhat more involved. For $x \in R$ and $v \in V$, $0 = d^5(xv) = 5d^4(x)d(v)$, and similarly $d(v)d^4(x) = 0$. Hence, for v, w, $y \in V$, $0 = d(v)d^4(xw)d(y) = 4d(v)d^3(x)d(w)d(y) = d(v)d^3(x)d(w)d(y)$ for all $x \in R$. Since $d^2(u) = 0$ for $u \in V$, and $3x = 0$ for all $x \in R$, it follows that $d^3(xu) = d^3(x)u$. Therefore, repeated substitutions of this kind for $x \in R$ in the expression $d(v)d^3(x)d(w)d(y) = 0$ show that $d(v)d^3(x)V'd(w)d(y) = 0$. Applying Lemma 2 again, and using the primeness of R, forces either $d(u)d^3(x) = 0$ or $d(w)d(y) = 0$. Should the second possibility occur, then $d(w)^2 = 0$, so $[a, v]$ is

https://doi.org/10.4153/CJM-1978-007-8 Published online by Cambridge University Press

nilpotent for each $a \in A$ and $v \in V$. The same argument as above, in the case char $R \neq 3, 5$ shows that $A \subset Z$. Therefore, we may assume that $d(v)d^3(x) = 0$. Now use substitutions of the form ux for x, with $u \in V$, to obtain $d(v)V'd^3(x) = 0$. Once again, by Lemma 2, we may conclude that $d(v) = 0$, and so, $A \subset Z$, or that $d^3(x) = 0$ for all $x \in R$. Expanding this last expression shows that $a^3 \in Z$. Thus if char $R = t$ for $t = 3$ or $t = 5$, then $a^t \in Z$ for all $a \in A$.

For either characteristic, if it should happen that $a^t = 0$ for all $a \in A$, then by using Lemma 1 and Lemma 3 as above, we could conclude that $N = \{a \in A | a^t = 0\} = A$ must be zero, and so $A \subset Z$ as required. Therefore, assume that $a^t \neq 0$ for some $a \in A$, and so, that $Z \neq 0$. Let $T = Z - (0)$ and consider RT^{-1}, the localization of R at its center. This new ring is prime, its center is a field F, and it possesses the involution $(rz^{-1})^* = r^*z^{-1}$. It is trivial to verify that $K(RT^{-1}) = KT^{-1}$. Consequently, replacing A by $AF + F$ leaves all of our hypotheses and assumptions unchanged, since A is commutative and char $R = t$. Furthermore, RT^{-1} satisfies S_{2n} exactly when R does, and $AF + F \subset Z(RT^{-1})$ implies that $A \subset Z(R)$. Therefore, we may keep the same notation as before but can now assume that Z is a field and that A is a Z subspace of R. We wish to extend Z to an algebraic closure, but the resulting tensor product might not be a prime ring. To eliminate this difficulty, we show that one may assume that R is a simple ring.

If R is not simple, let $I = I^*$ be a nonzero ideal of R, and set $I_K = I \cap K$ and $I_V = [I_K, I_K]$. Then $[A, I_V] \subset A \cap I = B$, and $[B, V] \subset V$. Now since $a^t \in Z$ for all $a \in A$, where $t = 3$, or $t = 5$ is the characteristic of R, it is immediate that $b^t \in Z \cap I$ for all $b \in B$. But Z is a field, so either $I = R$, or I is a proper ideal and $b^t = 0$. Applying Lemma 1 to B gives $B^3 = 0$, and so $B = 0$ by Lemma 3. Thus A commutes with I_V'. The fact that I is *-invariant implies that $I_K = K(I)$, so using Lemma 2 we may conclude that I_V' contains a nonzero ideal J of I, or that I satisfies S_4. In the first case, IJI is a nonzero ideal of R centralizing A, so $A \subset Z$. In the second case, it is easy and well-known, that R is an order in the same 4-dimensional simple algebra that is the quotient ring of I. Therefore, when R does not satisfy S_4, either R is simple or $A \subset Z$.

Assuming that R is a simple ring, let L be an algebraic closure of Z and consider the simple algebra $R \otimes_Z L$. Using the involution induced by $(r \otimes 1)^* = r^* \otimes 1$, one can show easily that $K(R \otimes L) = K \otimes L$, that $A \otimes L$ satisfies all the conditions we are assuming for A, and that $A \otimes L \subset Z(R \otimes L)$ implies that $A \subset Z$. Consequently, we may keep the same notation as before, but assume that Z is an algebraically closed field.

The proof can now be completed when char $R = 5$. With this assumption we have $a^5 \in Z$ each $a \in A$. Since Z is algebraically closed, there is $z \in Z$ with $(a - z)^5 = 0$. By Lemma 1, we have $(a - z)^3 = 0$. Suppose that some $a \in A$ is not nilpotent. It is still true that for some $z \in Z$, $0 = (a - z)^3 = a^3 - 3a^2z + 3az^2 - z^3$. For any $v \in V$, $0 = [(a - z)^3, v] = [a^3, v] - 3z[a^2, v] + 3z^2[a, v]$. The commutativity of A gives $[a^2, v] = 2a[a, v]$ and $[a^3, v] = 3a^2[a, v]$.

https://doi.org/10.4153/CJM-1978-007-8 Published online by Cambridge University Press

Using these in the expression above yields $3a^2[a, v] - 6za[a, v] + 3z^2[a, v] = 0$. Since it is in A, $[a, v]$ is either nilpotent or invertible. Should $[a, v]$ be invertible, then $3a^2 - 6za + 3z^2 = 0$ results, and commutating this with v again gives $0 = 3[a^2, v] - z[a, v] = 6a[a, v] - z[a, v] = (a - z)[a, v]$. Thus $a - z = 0$, $a \in Z$ and $[a, v] = 0$, so is not invertible. Consequently, when $a \in A$ is not nilpotent, then $[a, v]$ must be nilpotent for every $v \in V$. If $b \in A$ is nilpotent, then $(a + b)^5 = a^5$. Therefore, $a + b$ is not nilpotent, which implies that $[a + b, v] = [a, v] + [b, v]$ is nilpotent. But $[b, v] = [a + b, v] - [a, v]$ and A is commutative, so $[b. v]$ is nilpotent. Hence $[A, V] \subset N = \{a \in A | a^t = 0\}$, and so, $[N, V] \subset N$. Repeating the argument we have used before, employing Lemma 1 and Lemma 3, we may conclude that $N = 0$. However, if A has no nilpotent elements, but $(a - z)^3 = 0$ for each $a \in A$, then we are forced to conclude that $A \subset Z$.

At this point we note that if the original semi-prime ring under consideration were 6-torsion free, then all primes P satisfying $6R \not\subset P$ have been accounted for, and either R/P satisfies S_4 or $A + P \subset Z(R/P)$. Therefore, the second conclusion of the theorem would be proved, as explained in the first paragraph of this proof.

Finally, assume char $R = 3$. Since $a^3 \in Z$ for all $a \in A$, and Z is algebraically closed, either $A \subset Z$ or A contains nilpotent elements, just as in char $R = 5$ case. Let $b \in A$ with $b^2 = 0$. As in Lemma 1, $bkb = 0$ and so $bxb = bx^*b$ for all $x \in R$. In particular $bxbyb = by^*bx^*b = bybxb$. Exactly as in [**4**, proof of Lemma 2, p. 631], this relation forces R to be finite dimensional over Z. Since R is more than 4-dimensional by assumption, a direct computation shows the well known fact that $V = K$. Thus $[A, K] \subset A$, and the same argument as given at the end of [**4**, Lemma 2, p. 631] shows that dim ${}_ZR \leqq 9$, so that R satisfies S_6. Therefore, either $A \subset Z$ or R satisfies S_6, completing the proof of the theorem.

Our next theorem is quite easy, uses Theorem 1 and isolates a special case of the general result which it will be convenient to have.

THEOREM 2. *Let R be a prime ring and $A = A^*$ a subring of R which satisfies $[A, V] \subset A$. Then either R satisfies S_8, $A \subset Z$, or A contains $I = I^*$ a nonzero ideal of R.*

Proof. Should $A \cap K = 0$, then as $A^* = A$, we would have $A \subset S$. It follows that A is commutative, so Theorem 1 gives either $A \subset Z$ or R satisfies S_6. Consequently, we may assume that $A \cap K \neq 0$. Now $[A \cap K, V] \subset A \cap K$. Using [**5**, Theorem 1 and Theorem 2] either $(A \cap K)'$ contains $I = I^*$, a nonzero ideal of R, $A \cap K \subset Z$, or R satisfies S_8. Clearly $A \supset (A \cap K)'$, so we are finished unless $A \cap K \subset Z$. If $A \cap S = 0$, then $A \subset A \cap K \subset Z$, so assume $A \cap S \neq 0$. But $(A \cap S)(A \cap K) \subset A \cap K \subset Z$, $A \cap K \neq 0$, and the primeness of R, combine to yield $A \cap S \subset Z$. Therefore $2A \subset A \cap S + A \cap K \subset Z$, which implies that $A \subset Z$, since R is 2-torsion free, establishing the theorem.

https://doi.org/10.4153/CJM-1978-007-8 Published online by Cambridge University Press

Before extending Theorem 2 to arbitrary subrings of semi-prime rings, we require a few more technical results about subgroups of R invariant under commutation with V.

LEMMA 4. *Let R be a prime ring and W an additive subgroup of R satisfying $[W, W^*] = 0$ and $[W, V] \subset W$. Then either R satisfies S_8 or $W \subset Z$.*

Proof. Let A be the subring generated by W. Then $[A, V] \subset A$ follows by induction and the identity $[ab, c] = a[b, c] + [a, c]b$. It is also trivial that $[A, A^*] = 0$. Consequently, we may as well assume that W is a subring of R. For $a, b \in W$, $[ab^* - a^*b, a - a^*] = a^*[a, b] + a[a^*, b^*] \in V$. Therefore, $[a, a^*[a, b] + a[a^*, b^*]] = a^*[a, [a, b]] \in W$. Replace b by bc to obtain $a^*[a, b[a, c] + [a, b]c] \in W$. Expanding yields $a^*b[a, [a, c]] + 2a^*[a, b][a, c] + a^*[a, [a, b]]c \in W$, and so, using $a^*[a, [a, b]] \in W$ and $[W, W^*] = 0$ gives $2a^*[a, b][a, c] \in W$. For any $d \in W$, $0 = [2a^*[a, b][a, c], d^*] = 2[a^*, d^*][a, b][a, c]$. Clearly, $0 = W[a^*, d^*][a, b][a, c] = [a^*, d^*]W[a, b][a, c]$ and $0 = [a^*, d^*][a, b][a, c]W^* = [a^*, d^*]W^*[a, b][a, c]$. Consequently, $[a^*, d^*](W + W^* + WW^*)[a, b][a, c] = 0$. Now $T = W + W^* + WW^*$ is a subring of R and $[T, V] \subset T$, so using Theorem 2 we may conclude that R satisfies S_8, $T \subset Z$, or T contains a nonzero ideal of R. Since either of the first two cases prove the lemma, assume that T contains a nonzero ideal of R. The primeness of R forces either $[a^*, d^*] = 0$ or $[a, b][a, c] = 0$. Since the first of these implies the second, it is always true that $[a, b][a, c] = 0$ for any $a, b, c \in W$. Replacing c by cd for $d \in W$ shows that $[a, b]W[a, d] = 0$. Since $0 = W^*[a, b][a, d] = [a, b]W^*[a, d]$, we have again that $[a, b](W + W^* + WW^*)[a, d] = 0$. As above, the lemma holds unless $[a, b] = 0$. But if $[W, W] = 0$, then W commutes with $T = W + W^* + WW^*$. A final application of Theorem 2 demonstrates that unless the lemma is valid, W commutes with a nonzero ideal of R, forcing $W \subset Z$.

In the proof of our main result, we will apply Lemma 4 to subgroup of the form $[W, W]$. Our next result, together with Lemma 4, will enable us to restrict our attention to involutions of the first kind.

LEMMA 5. *Let R be a prime ring with * of the second kind; that is, $Z \cap K \neq 0$. If W is an additive subgroup of R satisfying $[W, W] \subset Z$ and $[W, V] \subset W$, then $W \subset Z$.*

Proof. We may assume that W is a Z module, since $W + WZ$ satisfies the same hypotheses as W. Since the involution is of the second kind, $Z \neq 0$, so we may localize R at $T = Z \cap S - \{0\}$. As in Theorem 1, RT^{-1} is a prime ring whose center is a field. The involution $(rt^{-1})^* = r^*t^{-1}$ on RT^{-1} is of the second kind, $K(RT^{-1}) = KT^{-1}$, and WT^{-1} satisfies the hypotheses on W. Finally, $WT^{-1} \subset Z(RT^{-1})$ exactly when $W \subset Z$, so we may as well keep our original notation and now assume that Z is a field and W is a Z-subspace of R. If $v \in K \cap Z$, then $S = vK$ and $K = vS$. Consequently, $W \supset [W, [K, K]] =$

https://doi.org/10.4153/CJM-1978-007-8 Published online by Cambridge University Press

$[W, [vS, K]] = [vW, [S, K]] = [W, [S, K]]$, and similarly $W \supset [W, [S, S]]$. It follows easily that $[W, [R, R]] \subset W$, and so, using [**2**, Theorem 5, p. 570] we conclude that either $[W, [R, R]] = 0$, or $W \supset [M, R] \neq 0$ for M an ideal of R. If $[W, [R, R]] = 0$, then $W \subset Z$ by [**2**, Lemma 2, p. 562]. On the other hand, if $[M, R] = L \subset W$, then $[L, L] \subset Z$, since $[W, W] \subset Z$, forcing $L \subset Z$ [**6**, Lemma 7, p. 120]. But now $[M, R] \subset Z$, so as we have just seen, $M \subset Z$, giving rise to the contradiction $[M, R] = 0$. Therefore, $W \subset Z$ as required.

One more result is required before our main theorem.

LEMMA 6. *Let R be a prime ring and A a subring which satisfies $[A, V] \subset A$. If $[x, [A, V]] = 0$, then $[x, A] = 0$ unless R satisfies S_4.*

Proof. For $a \in A$, $b \in [A, V]$, and $v \in V$, $0 = [x, [ab, v]] = [x, a[b, v]] + [x, [a, v]b] = [x, a][b, v]$, using $[b, v] \in [A, V]$. Since a, b, and v are arbitrary, $[x, A][[A, V], V] = 0$. Now $[[A, V], V]$ is an additive subgroup of R and is invariant under commutation with V, by the identity $[[a, b], c] = [[a, c], b] + [a, [b, c]]$. Thus, Lemma 3 implies that R satisfies S_4 or that $[x, A] = 0$, provided that $[[A, V], V] \neq 0$.

If R does not satisfy S_4 but $[[A, V], V] = 0$, then it follows from Lemma 2 that $[A, V] \subset Z$. Let $a \in A$ and $v \in V$. Since $a^2 \in A$, $[a^2, v] = a[a, v] + [a, v]a = 2a[a, v] \in Z$. The primeness of R and $[a, v] \in Z$ together imply that $a \in Z$ unless $[a, v] = 0$. Another application of Lemma 2, in the case where $[a, V] = 0$, shows that $a \in Z$ anyway. Consequently, $A \subset Z$ and $[x, A] = 0$ always holds.

We are now able to prove our main result about subrings of R invariant under commutation by V.

THEOREM 3. *Let R be a 2-torsion free semi-prime ring and A a subring of R satisfying $[A, V] \subset A$. Then A contains $I = I^*$, a noncentral ideal of R, unless R is the subdirect sum of semi-prime *-homomorphic images R_1 and R_2 with R_1 satisfying S_8 and the image of A central in R_2.*

Proof. Consider $A \cap K$, an additive subgroup of K satisfying $[A \cap K, V] \subset A \cap K$. Using the results in [**5**], we may conclude that $(A \cap K)'$ contains a noncentral ideal $I = I^*$ of R, or that for each prime ideal P of R with $2R \not\subset P$ either R/P satisfies S_8, or $A \cap K + P \subset Z(R/P)$. Assuming that $A \supset (A \cap K)'$ does not contain a noncentral *-ideal of R, to complete the proof of the theorem it suffices to show, as in Theorem 1, that for each prime ideal P of R with $2R \not\subset P$, either R/P satisfies S_8 or $A + P \subset Z(R/P)$. Henceforth, for any prime ideal P of R under consideration, we assume that $2R \not\subset P$, that R/P does not satisfy S_8, and that $A \cap K + P \subset Z(R/P)$.

Let P be such a prime ideal of R and suppose that $P^* \neq P$. We argue much as in Theorem 1. Recall that $P^* + P$ is a non-zero ideal in R/P and $P^* + P \subset K + P$. Therefore $[A, [P^*, P^*]] + P \subset A \cap [P^*, P^*] + P \subset A \cap K + P \subset Z(R/P)$. Consequently, for each $x \in A$, $[x, [x, [P^*, P^*]]] \subset P$ which implies that $[x, [P^*, P^*]] \subset P$ by [**2**, Theorem 1, p. 563], and so that $[x, P^*] \subset P$

https://doi.org/10.4153/CJM-1978-007-8 Published online by Cambridge University Press

[**2**, Lemma 2, p. 562]. Since P is a prime ideal of R, $x + P \in Z(R/P)$ results. Thus, when $P^* \neq P$, we have $A + P \subset Z(R/P)$.

For prime ideals P with $P^* = P$, R/P has the involution $(r + P)^* = r^* + P$, and if necessary by tensoring with $J[1/2]$, as in the proof of Theorem 1, we may assume that R is a prime ring with $2R = R$ and $2A = A$. Our situation is that R does not satisfy S_8, $A \cap K \subset Z$, and we want to show that $A \subset Z$.

Next suppose that $A^* = A$. Then Theorem 2 implies that $A \subset Z$ or A contains a nonzero ideal $I = I^*$. But $A \cap K \subset Z$, so the second possibility means that $[I \cap K, I \cap K] = 0$. Now I is a prime ring and $I^* = I$ gives $K(I) = I \cap K$, so [**5**, Lemma 2] forces I to satisfy S_4. As in Theorem 1, R itself must satisfy S_4, a contradiction. Thus, if $A^* = A$, then $A \subset Z$. In any event $(A \cap A^*)^* = A \cap A^*$, $A \cap A^* \cap K \subset Z$, and $[A \cap A^*, V] \subset A \cap A^*$, so the subring $A \cap A^* \subset Z$.

Let $a, b \in A$ and $v \in V$. Then $[a, [b - b^*, v]] \in [A, V] \subset A$, and so $[a, [b, v]] - [a, [b^*, v]] \in A$. Since $[a, [b, v]] \in [A, A] \subset A$, we have $[a, [b^*, v]] \in A$. Now a, b, and v are arbitrary, so $[A, [A^*, V]] \subset A$. Set $B = [A, V]$ and note that $[B, V] \subset B$, and $B^* = [A^*, V]$. Consequently, $[B, B^*] \subset [A, B^*] \subset A$ and $[B, B^*] = [B, B^*]^* \subset A^*$, so $[B, B^*] \subset A \cap A^* \subset Z$. It follows that $[[B, B], B^*] = 0$, and so, that $[[B, B], [B, B]^*] = 0$. Applying Lemma 4 with $W = [B, B]$ results in $[B, B] \subset Z$. If * is of the second kind, then $B \subset Z$ by Lemma 5, so $A \subset Z$ follows from Lemma 6. Therefore, we may assume that * is of the first kind, so that $K \cap Z = 0$.

Now let $b \in B$ and $v \in V$. Then $b^2 \in A$, so $[b^2, v] \in B$ and so, $[b, [b^2, v]] \in Z$. Rewriting this gives $[b, b[b, v] + [b, v]b] = b[b, [b, v]] + [b, [b, v]]b \in Z$. But $[b, [b, v]] \in Z$, so we obtain $2b[b, [b, v]] \in Z$. Should $[b, [b, v]] \neq 0$, then because R is prime, we must have $b \in Z$, implying that $[b, [b, v]] = 0$. Thus for any $b \in B$ and $v \in V$, $[b, [b, v]] = 0$. Replacing b by $b + c$ for $c \in B$ gives $[c, [b, v]] + [b, [c, v]] = 0$. Now $[c, [b, v]] = [[c, b], v] + [b, [c, v]]$ and $[c, b] \in [B, B] \subset Z$, so $[c, [b, v]] = [b, [c, v]]$, and it follows that $[b, [c, v]] = 0$. Therefore, $[B, [B, V]] = 0$. Using Lemma 6 allows the conclusion that $[A, [B, V]] = 0$.

The goal of our next computation is to show that $[B, B] = 0$. Note that for all $b, c \in B$ and $v \in V$, since $bc \in A$, $[bc, v] \in B$, and so $[A, [[bc, v], V]] = 0$. Expanding gives

$$\begin{aligned} 0 &= [A, [b[c, v] + [b, v]c, V]] \\ &= [A, b[[c, v], V]] + [A, [b, V][c, v]] + [A, [b, v][c, V]] \\ &\qquad + [A, [[b, v], V]c] \\ &= [A, b][[c, v], V] + [[b, v], V][A, c] \end{aligned}$$

where we have let A and V stand for representative elements of themselves, and have used $[A, [B, V]] = 0$. Now if $c \in [B, V]$, then $[A, c] = 0$, so finally we obtain $[A, B][[[B, V], V], V] = 0$. Since R does not satisfy S_8 and since each of the factors in this product are invariant under commutation with V, it follows from Lemma 3, that either $[A, B] = 0$ or $[[[B, V], V], V] = 0$.

https://doi.org/10.4153/CJM-1978-007-8 Published online by Cambridge University Press

Assume that the second possibility holds and let $b \in B$ and $u, v, w \in V$. Applying * to the resulting expression yields $[[[b^*, u], v], w] = 0$, and so $[[[b - b^*, u], v], w] = 0$. Because $w \in V$ is arbitrary, $[[[b - b^*, u], v], V] = 0$. Using Lemma 2 and the primeness of R allows us to conclude that $[[b - b^*, u], v] \in Z$. But $[[b - b^*, u], v] \in K$ and * is of the first kind. Hence $[[b - b^*, u], v] = 0$. Repeating this argument leads to $b - b^* = 0$, or $B \subset S$. Consequently, $[B, B] \subset Z \cap [S, S] \subset Z \cap K = 0$. Had we assumed the first possibility above, namely that $[A, B] = 0$, we would have the same conclusion. Therefore, we may assume that $[B, B] = 0$, and recall that $[B, B^*] \subset Z$ also holds.

Using $[B, B^*] \subset Z \subset S$, we have $[a, b^*] = [a, b^*]^* = [b, a^*]$ for $a, b \in B$. Equivalently, $[a, b^*] + [a^*, b] = 0$. But now for $a, b \in B$, $[a - a^*, b - b^*] = -[a, b^*] - [a^*, b] = 0$, since $[B, B] = 0$. Set $L = \{a - a^* | a \in B\}$ and note that we have just shown $[L, L] = 0$. It is easy to verify that L is an additive subgroup of K and that $[L, V] \subset L$. Applying [**5**, Theorem 3] yields either $L \subset Z$ or L contains a noncommutative Lie ideal of V. Since $[L, L] = 0$, we are forced to conclude that $L \subset Z \cap K = 0$. The outcome is that $a = a^*$ for all $a \in B$. Thus B' the subring generated by B, is commutative, *-invariant, and $[B', V] \subset B'$. Consequently, $B \subset Z$ by Theorem 1, and so, $A \subset Z$ using Lemma 6, which completes the proof of the theorem.

To see how the subdirect sum in Theorem 3 may arise, it suffices to take a direct or subdirect product of suitable prime rings. The prime rings in which A can be taken to lie in the center need no further elaboration. For completeness, we present an example of a prime ring satisfying S_8, which contains an invariant subring not in the center and not containing an ideal (see [**1**, 40] or [**5**]). Let $R = M_4(D)$, the complete 4×4 matrix ring over a commutative domain D with identity and char $D \neq 2$. Take the usual matrix transpose as the involution on R. If $\{e_{ij}\}$ are the standard matrix units, set $v_{ij} = e_{ij} - e_{ji}$. Then the D submodule A generated by the identity matrix I_4 together with $v_{12} + v_{34}$, $v_{13} - v_{24}$, and $v_{14} + v_{23}$ is invariant under commutation with K, and is, in fact, a subring. Clearly, A is not in the center of R and cannot contain a nonzero ideal of R, since the extension of A to a subalgebra of $M_4(F)$, for F the quotient field of D, is not all of $M_4(F)$.

References

1. I. N. Herstein, *Topics in ring theory* (University of Chicago Press, Chicago, 1969).

2. ——— *On the Lie structure of an associative ring*, J. Algebra *14* (1970), 561–571.

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

4. ——— *Certain submodules of simple rings with involution II*, Can. J. Math. *27* (1975), 629–635.

5. C. Lanski, *Lie structure in semi-prime rings with involution*, Comm. in Alg. *4* (1976), 731–746.

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

University of Southern California,
Los Angeles, California

https://doi.org/10.4153/CJM-1978-007-8 Published online by Cambridge University Press