UNITARY INVARIANCE IN ALGEBRAIC ALGEBRAS¹

RY

CHARLES LANSKI

ABSTRACT. A structure theorem is obtained for subspaces invariant under conjugation by the unitary group of a prime algebraic algebra over an infinite field. For an invariant subalgebra W, it is shown that either W is central, W contains an ideal, or the ring satisfies the standard identity of degree eight. Also, for prime algebras not satisfying such an identity, the unitary group is not solvable.

In the study of the unitary group in rings with involution, two main questions have been examined. The first concerns the structure of the unitary group itself, particularly for simple rings. A result of R. V. Kadison [5] shows that the unitary group modulo its center is topologically simple (has no closed normal subgroups) in certain simple rings of operators. The general question of the algebraic simplicity of this quotient, or of related groups, as for example the same quotient for the commutator subgroup, remains open [6, p. 136]. The second question asks about the structure of subsets invariant under conjugation by the unitary group. Some of these, put forward by I. N. Herstein can be found in [10]. For division rings with involution, the structure of invariant subdivision rings has been settled by I. N. Herstein [3]. Recent results of M. Chacron [1], obtained concurrently with those presented here, determine the structure of invariant subalgebras of simple artinian rings with involution when either the underlying division ring is algebraic over its center, or when the subalgebra satisfies a polynomial identity. Our investigation concerns invariant subspaces of algebraic algebras with involution. The main technical result shows that such subspaces are invariant under Lie commutation with the skew-symmetric elements of the ring. Using previous work [8], [9] which describes this situation, we obtain results for algebraic algebras over infinite fields which include those mentioned above for such algebras. Although we can make no real progress on the question of the simplicity of the unitary group, we do show that this group cannot be solvable.

Received by the editors September 2, 1977.

AMS (MOS) subject classifications (1970). Primary 16A28; Secondary 16A12, 16A48.

Key words and phrases. Unitary group, skew-symmetric elements, Lie commutation, invariant subspace, invariant subring, solvable normal subgroup.

¹This research was supported by NSF Grant MCS76-07240A01.

[©] American Mathematical Society 1979

Throughout the paper, R will denote an algebraic algebra over an infinite field F, with char $F \neq 2$. We assume that $1 \in R$ and that R has an involution, *. Let $K = \{r \in R | r^* = -r\}$ and $U = \{x \in R | xx^* = x^*x = 1\}$. If $S(F) = \{a \in F | a^* = a\}$, then since [F: S(F)] = 2, R is algebraic over S(F) and S(F) is infinite, so without loss of generality we may assume that F = S(F). The assumptions that R is algebraic and that F is infinite imply that for any $x \in R$, both 1 + tx and 1 - tx are invertible for all but finitely many $t \in F$. In particular, when such a choice of $t \in F$ is made for $k \in K$, set $C(tk) = (1 - tk)(1 + tk)^{-1}$ and observe that $C(tk) \in U$, and that $C(tk)^{-1} = C(-tk)$. An additive subgroup A of R is called an invariant subspace, if A is a vector space over F, and if for each $a \in A$, $k \in K$ and all but finitely many $t \in F$, $C(tk)aC(-tk) \in A$.

Our first objective is to use the assumption that R is algebraic to obtain a formula for $(1 + tk)^{-1}$ as a polynomial in k. We begin with an easy lemma about the degree of $(1 + tk)^{-1}$ as such a polynomial.

LEMMA 1. Let $y \in R$ have minimal polynomial $m(x) \in F[x]$ with $\deg m(x) = n + 1$. If $z \in F - (0)$ and 1 + zy is invertible, there is $p(x) \in F[x]$ of degree n so that $(1 + zy)^{-1} = p(y)$. Should $(1 + zy)^{-1} = f(y)$ for $f(x) \in F[x]$, then $\deg f(x) > n$.

PROOF. Since $m((x-1)z^{-1})$ is a polynomial of degree n+1 which is satisfied by 1+zy, the existence of p(x) is immediate. Should $(1+zy)^{-1} = f(y)$ for deg f(x) = d < n, then g(x) = f(x)(zx+1) - 1 has degree d+1 < n+1 and g(y) = 0, contradicting the choice of m(x). Thus deg f(x) > n and the lemma is proved.

As a consequence of Lemma 1, if $y \in R$ is of degree n + 1 and $R(y) = \{z \in F - (0)|1 + zy \text{ is invertible}\}$, then for $z \in R(y)$ we can write $(1 + zy)^{-1} = \sum a_i(z)y^i$, for $0 \le i \le n$, the $a_i(z)$ functions from R(y) to F, and $a_n(z) \ne 0$ for all $z \in R(y)$. The next result gives a description of the functions $a_i(z)$.

LEMMA 2. Let $y \in R$ with minimal polynomial $m(x) = \sum b_j x^j$ where $0 \le j \le n+1$ and $b_{n+1} = 1$. If $z \in F - (0)$ and 1 + zy is invertible, then $(1 + zy)^{-1} = \sum a_i(z)y^i$ for $0 \le i \le n$ where

$$A(z)a_{i}(z) = (-z)^{i}b_{n+1} + (-z)^{i+1}b_{n} + \cdots + (-z)^{n}b_{i+1}$$
 for $A(z) \in F - (0)$.

PROOF. Throughout the proof, the subscript i will satisfy $0 \le i \le n$. Set $u_i(z) = (-z)^i b_{n+1} + (-z)^{i+1} b_n + \cdots + (-z)^n b_{i+1}$ and let $u_{-1}(z) = u_{n+1}(z) = 0$. Consider

$$G(x) = \left(\sum u_i(z)x^i\right)(1+zx) = u_0(z) + \sum (u_{i+1}(z) + zu_i(z))x^{i+1}.$$

It follows from the definitions that $u_{i+1}(z) + zu_i(z) = z(-z)^n b_{i+1}$, and so,

 $G(x) = u_0(z) + (-z)^{n+1}b_0 + z(-z)^n m(x)$. Since m(x) is the minimal polynomial for y, $G(y) = u_0(z) + (-z)^{n+1}b_0 = A(z)$. Thus $(\sum u_i(z)y^i)(1 + zy) = A(z)$. Should A(z) = 0 the invertibility of 1 + zy would force $\sum u_i(z)y^i = 0$, and this in turn gives $0 = u_n(z) = (-z)^n$, from the choice of m(x). But $z \neq 0$, so we may write $(1 + zy)^{-1} = \sum A(z)^{-1}u_i(z)y^i$, and setting $a_i(z) = A^{-1}(z)u_i(z)$ completes the proof.

Using the computations in Lemma 2, we can now prove the main technical result of the paper. Denote xy - yx by [x, y] for $x, y \in R$, and for additive subgroups A and B of R, let [A, B] stand for the subgroup generated by all [a, b] for $a \in A$ and $b \in B$.

THEOREM 1. If W is an invariant subspace of R then $[W, K] \subset W$.

PROOF. Let $k \in K$ so that 1 + k and 1 - k are invertible, and for all $w \in W$,

$$(1-k)(1+k)^{-1}w(1+k)(1-k)^{-1} \in W.$$

We repeat here the lemma from [3, Lemma 1, p. 555] by noting that

$$(1+k)^{-1}(1+k-2k)w(1-k+2k)(1-k)^{-1} \in W$$

and so,

$$w + (1+k)^{-1}(-2kw) + 2wk(1-k)^{-1} + (1+k)^{-1}(-4kwk)(1-k)^{-1} \in W.$$

Since W is a subspace, we can delete the w to obtain

$$(1+k)^{-1}(-2kw(1-k)+(1+k)2wk-4kwk)(1-k)^{-1} \in W.$$

Simplifying gives $(1+k)^{-1}[w,k](1-k)^{-1} \in W$. Our earlier remarks show that for any $k \in K$ and all but finitely many $z \in F - (0)$, one has both 1-zk and 1+zk invertible, where of course $zk \in K$. Furthermore, from the definition of invariant, for all but finitely many of these z, one has $C(zk)WC(-zk) \subset W$. For any of these $z \in F$, we may write $(1+zk)^{-1} = \sum a_i(z)k^i$ for $0 \le i \le n$, from Lemma 1. Consequently, for $0 \le i, j \le n$, we have

$$\left(\sum a_i(z)k^i\right)\left[w,zk\right]\left(\sum a_j(-z)k^j\right)\in W.$$

Using again that W is a subspace and that $z \neq 0$ yields first that $\sum a_i(z) \cdot a_j(-z)k^i[w, k]k^j \in W$, and then that $\sum B_{ij}(z)k^i[w, k]k^j \in W$, where $B_{ij}(z) = A(z)a_i(z)A(-z)a_i(-z)$.

Using Lemma 2 one finds that each $B_{ij}(z)$ is a polynomial in z of degree at most 2n whose coefficients are functions of the b_k which depend only on i and j. Also, z^{i+j} is the smallest power of z which appears with nonzero coefficient. Therefore, one can rearrange the sum above into an expression of

the form $\sum f_m(w, k)z^m \in W$ for $0 \le m \le 2n$, where $f_m(w, k)$ is independent of z. Since W is a subspace and all but finitely many elements of F can be used as a choice for z, a Vandermonde determinant argument shows that $f_m(w, k) \in W$ for each m. In particular, $f_0(m, k) = [w, k] \in W$, completing the proof of the theorem.

Applying Theorem 1 and the results in [8] and [9] enables us to obtain the structure theorems we seek. For the case of invariant subalgebras of simple rings it would suffice to use Theorem 1 and [4]. Although the following theorems can be stated for semiprime rings, we consider *-prime rings only, for the sake of some simplicity. Also, we abbreviate the statement "R satisfies the standard polynomial identity of degree eight" to "R is (or satisfies) S_8 ." Recalling that in a ring with involution, $S = \{r \in R | r^* = r\}$, we proceed to an immediate consequence of Theorem 1.

THEOREM 2. Let R be a *-prime ring and W an invariant subspace of R. One of the following must hold: (i) there is a nonzero *-ideal I of R so that either $W \supset [I \cap K, K]$, a noncommutative Lie ideal of [K, K], or $W \supset [I \cap K, S] + [I \cap S, K]$, a noncommutative K submodule of S; (ii) R is S_8 ; or (iii) $W \cap S + W \cap K \subset Z$, the center of R. If in addition $W^* = W$, then (iii) becomes $W \subset Z$.

PROOF. Applying Theorem 1 gives $[W, K] \subset W$. The theorem follows at once from [8, Theorems 1 and 2].

Invariant subsets of interest include the subset of symmetric idempotents and subsets of nilpotent symmetric elements. We state a corollary of Theorem 2 for these sets.

COROLLARY 2.1. Let R be a *-prime ring and set $N_0 = \{e \in S | e^2 = e, \text{ and } e \neq 0, 1\}$ and for $i \geq 1$, $N_i = \{x \in S | x^{i+1} = 0 \text{ but } x^i \neq 0\}$. Assume that R is not S_8 and that some given N_t is not empty. Then $[N_t]_F$, the subspace spanned by N_t contains $[I \cap K, S] + [I \cap S, K]$, a noncommutative K submodule of S, for $I^* = I$ an ideal of R. When R is *-simple with center Z, $[N_t]_Z \supset [K, S]$ and if $Z \not\subset S$, $[N_t]_Z \supset [R, R]$.

PROOF. Clearly, if N_t is not empty it is closed under conjugation by all elements of U, so $[N_t]_F$ is an invariant subspace of R and is contained in S. Because R is a *-prime ring, $N_t \not\subset Z$ and so, it follows from Theorem 2 that $[N_t]_F \supset [K \cap I, S] + [S \cap I, K]$ as claimed. When R is *-simple we must have I = R, so $[N_t]_Z \supset [K, S]$. If $Z \not\subset S$, then there is $z \in Z \cap K - (0)$ and one has K = zS and S = zK. Thus $[N_t]_Z \supset [S, K] = [S, zS] = z[S, S]$, so as a Z-vector space $[N_t]_Z \supset [S, S]$. Consequently, $[N_t]_Z \supset [S, K] + [S, S] = [S, R]$ and the same argument used again shows $[N_t]_Z \supset [R, R]$.

The statements of the last two results for subalgebras follow as easily by

using Theorem 1 and [9, Theorem 3], so we omit the proofs.

THEOREM 3. Let R be a *-prime ring and W an invariant subalgebra of R. Then either $W \subset Z$, the center of R, $W \supset I$ a nonzero *-ideal of R, or R is S_8 .

COROLLARY 3.1. Let R be a *-prime ring and N_i as in Corollary 2.1. If R is not S_8 and some given N_t is not empty then M_t , the subalgebra generated by N_t over F, contains a nonzero *-ideal of R. When R is *-simple, $M_t = R$.

We isolate one further case of Theorem 3.

COROLLARY 3.2. If R is a *-prime ring and W is an invariant subalgebra of R which satisfies a polynomial identity, then either $W \subset Z$ or R satisfies a polynomial identity. When W is commutative, either $W \subset Z$ or R is S_8 .

Our next goal is to show that the unitary group cannot be solvable when R is a *-prime ring. First we note that when $u \in U$ and 1 + u is invertible, then $(u-1)(1+u)^{-1} = k \in K$, $1-k=1-(u-1)(1+u)^{-1} = ((1+u)-(u-1))(1+u)^{-1} = 2(1+u)^{-1}$ is invertible, and $(1+k)(1-k)^{-1} = u$. Similarly, if 1-k is invertible, then $u=(1+k)(1-k)^{-1} \in U$ and 1+u is invertible. Consequently, $U_0 = \{u \in U | 1+u \text{ is invertible}\} = \{u \in U | u = (1+k)(1-k)^{-1} \text{ for some } k \in K\}$. Note that U_0 is not a subgroup of U. The crucial step in showing the nonsolvability of U is an extension of Theorem 2 to subspaces invariant under conjugation by subgroups of U normalized by U_0 . The proof is like those of Theorems 1 and 2, but somewhat more involved.

THEOREM 4. Let R be a *-prime ring, Z the center of R, $W = W^*$ an F-subspace of R, and V a subgroup of U normalized by U_0 . If $vwv^* \in W$ for each $w \in W$ and $v \in V$, then one of the following must hold: (i) R is S_8 ; (ii) $V \subset Z$; (iii) $W \subset Z$; or (iv) there is a nonzero *-ideal I of R so that $W \supset [K \cap I, K]$ which is noncommutative, or $W \supset [K \cap I, S \cap I]$ which is noncommutative. When W is a subalgebra of R, the last possibility above can be replaced by: $W \supset I$ a nonzero *-ideal of R.

PROOF. Consider $C(zk) = (1 - zk)(1 + zk)^{-1}$, which exists for each $k \in K$ and all but finitely many $z \in F - (0)$. By Lemma 2, we may write $(1 + zk)^{-1} = \sum a_i(z)k^i$, for $0 \le i \le n$, so that $C(zk) = (1 - zk)\sum a_i(z)k^i = \sum (a_i(z) - za_{i-1}(z))k^i$ where we allow $0 \le i \le n+1$ and set $a_{-1}(z) = a_{n+1}(z) = 0$. Also from Lemma 2, write $A(z)C(zk) = \sum B_i(z)k^i$ for $B_i(z) = A(z)(a_i(z) - za_{i-1}(z))$. Now make the computations:

$$B_0(z) = A(z)a_0(z) = 1 - zb_n + \dots + (-1)^n z^n b_1,$$

$$B_{n+1}(z) = A(z)(-za_n(z)) = (-1)^{n+1} z^{n+1}$$
(1)

and for $1 \le i \le n$,

$$B_{i}(z) = A(z)(a_{i}(z) - za_{i-1}(z))$$

$$= ((-z)^{i} + (-z)^{i+1}b_{n} + \cdots + (-z)^{n}b_{i+1})$$

$$-z((-z)^{i-1} + (-z)^{i}b_{n} + \cdots + (-z)^{n}b_{i}),$$

SO

$$B_i(z) = 2((-z)^i + (-z)^{i+1}b_n + \cdots + (-z)^n b_{i+1}) + (-z)^{n+1}b_i. \quad (2)$$

Consequently, $B_i(z)$ is a polynomial in z of degree at most n+1, the coefficients are functions of the b_k and depend only on i, and z^i is the smallest power of z appearing in $B_i(z)$ with nonzero coefficient.

Since V is normalized by U_0 , $C(zk)vC(-zk) \in V$ for each $v \in V$, $k \in K$, and all but finitely many $z \in F - (0)$. Therefore, for each $w \in W$, $C(zk)vC(-zk)wC(zk)v^*C(-zk) \in W$. Now W is a subspace, so we can multiply by $A(z)^2A(-z)^2$ and rewrite the result as

$$\left(\sum B_i(z)k^i\right)v\left(\sum B_j(-z)k^j\right)w\left(\sum B_p(z)k^p\right)v^*\left(\sum B_q(-z)k^q\right)\in W \quad (3)$$

where i, j, p, and q range between 0 and n + 1. Using our comment above about the $B_i(z)$ as polynomials, rewrite the summation (3) as $\sum f_d(k, v, w)z^d \in W$ for $0 \le d \le 4n + 4$. As in the proof of Theorem 1, we may use a Vandermonde determinant argument to obtain $f_d(k, w, v) \in W$, and in particular $f_1(k, w, v) \in W$. Consideration of the summation (3) together with formulas (1) and (2) shows that the terms of $f_1(k, w, v)$ arise either by taking all $B_i(z) = B_0(z)$ in (3), or by taking one $B_i(z) = B_1(z)$ and the others equal to $B_0(z)$. Explicitly computing the eight terms in $f_1(k, v, w)$ shows that the coefficient of vwv^* is zero, leaving $f_1(k, v, w) = -2(kvwv^* - vkwv^* + vwkv^* - vwv^*k)$. Consequently W contains $(-1/2)v^*f_1(k, v, w)v = v^*kvw - kw + wk - wv^*kv = [w, k - v^*kv]$.

Let T be the F-subspace spanned by $\{k-v^*kv|k\in K \text{ and } v\in V\}$. It is easy to see that $T\subset K$ and that $uTu^*\subset T$ for all $u\in U_0$. Therefore, Theorem 2 can be applied to T and one obtains either $T\subset Z$, R is S_8 , or $T\supset [K\cap I,K]$ for I a nonzero *-ideal of R. Since there is nothing more to prove if R is S_8 , we assume henceforth that R is not S_8 . Should the first possibility for T hold, that is $T\subset Z$, then $k-v^*kv\in Z$ and it follows that $vk-kv=[v,k]\in Zv$. Hence, for each $v\in V$, the subring Z[v] generated by Z and v is invariant under Lie commutation with K. In this situation, it is immediate from [9, Theorem 3] that $Z[v]\subset Z$, and so $V\subset Z$, which would prove the theorem. As a result, we may assume that the third possibility above, $T\supset [K\cap I,K]$ holds. Note that for any *-ideal I of R, $K\cap I=K(I)=\{x\in I|x^*=-x\}$. Set $L=[W,[K(I),K]]\subset [W,T]\subset W$, and observe that $L=L^*$ is a subspace of the *-prime algebra I, and that $[L,[K(I),K(I)]]\subset L$. We can assume that I is not S_8 , since if it were, it

would force R to be S_8 . Therefore, applying [8, Theorem 2] to I and L gives rise to two possibilities: either $L \subset Z(I)$, the center of I; or for a nonzero *-ideal M of I, $L \supset [K(M), K(I)]$ or $L \supset [K(M), S(M)]$ and the appropriate one of these sets is not commutative.

First consider the case $L \subset Z(I)$. Clearly $[W, J] \subset L$ where J = [K(I), K(I)], and it follows that [W, [J, J]] = 0. Since J is invariant under Lie commutation with K(I), we must have $[7, \text{proof of Theorem 3}] J \subset Z(I)$ or that the subring generated by [J, J] contains a nonzero *-ideal P of I. The first possibility forces I to be S_8 [7, Lemma 2], and the second means that W commutes with IPI, forcing $W \subset Z$. The theorem would be proved in either case, so we may now assume $L \not\subset Z$ and L contains either [K(M), K(I)] or [K(M), S(M)]. We continue with assumption $L \supset [K(M), S(M)]$ and omit the argument in the other case because it is very similar and is less difficult.

Given that $L \supset [K(M), S(M)]$ for M a nonzero *-ideal of I, we have $L \supset [K(IMI), S(IMI)] = Y$. Now $Y \subset S(IMI)$ and $[Y, K] \subset Y$. If $Y \subset Z$, then [[K(IMI), K(IMI)], S(IMI)] = 0 and the argument used in the preceding paragraph shows that the subring generated by [K(IMI), K(IMI)] contains a nonzero *-ideal of IMI, or that $K(IMI) \subset Z(IMI)$ [7, proof of Theorem 3]. As above, we must conclude from these possibilities that $S(IMI) \subset Z(IMI)$, since IMI cannot satisfy S_8 . But this condition on S(IMI) forces IMI to be S_8 [2, proof of Theorem 1.6]. Therefore, assume that $Y \not\subset Z$, apply [8, Theorem 2] to Y, and obtain the conclusion that $Y \supset [K(P), S(P)]$, a noncommutative set, for P a *-ideal of R. Since $W \supset L \supset Y \supset [K(P), S(P)]$, the first statement of the theorem is proved.

When W is a subalgebra of R, the initial arguments above are still valid and we obtain $L' \subset W$, where L' is the subalgebra generated by L. Since $[L', [K(I), K(I)]] \subset L'$ also holds, if follows from [9, Theorem 3] that $L' \subset Z(I) \subset Z$ or that $L' \supset M$, a nonzero *-ideal of I. In the first case, $L \subset Z$ so as shown above, either R is S_8 or $W \subset Z$. In the second case, $IMI \subset M \subset L' \subset W$ shows that the other possible conclusion of the theorem holds, completing the proof of the theorem.

Using Theorem 4, our final result, showing that $U/(U \cap Z)$ has no solvable normal subgroups, is easy.

THEOREM 5. Let R be a *-prime ring which is not S_8 . If V is a subgroup of U normalized by U_0 , then V is solvable if and only if $V \subset Z$.

PROOF. Let $V \supset V^{(1)} \supset \cdots \supset V^{(n+1)} \supset 1$ be the derived series for $V \not\subset Z$, showing V to be solvable. Clearly, each $V^{(i)}$ is normalized by U_0 . If W is the subspace spanned by $V^{(n+1)}$, then W is a commutative subalgebra of R and is invariant. Thus, by Corollary 3.2, $W \subset Z$. Hence, for $v, w \in V^{(n)}$, $vwv^*w^* \in Z$, so $vwv^* \in Z[w]$, the subalgebra generated by Z and w. Since

 $v(Z[w])v^* \subset Z[w]$ for all $v \in V$, Theorem 4 forces either $V^{(n)} \subset Z$ or $Z[w] \subset Z$. In either case $V^{(n)} \subset Z$, and the contradiction $V^{(n+1)} = (1)$ results.

The author wishes to thank the referee for suggestions which helped to clarify and simplify parts of this paper. In particular, the proof of Lemma 2 was suggested by the referee as a replacement for the longer proof originally submitted by the author.

REFERENCES

- 1. M. Chacron, Unitaries in simple Artinian rings (preprint).
- 2. I. N. Herstein, Topics in ring theory, Univ. of Chicago Press, Chicago, Illinois, 1969.
- 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, Canad. J. Math. 27 (1975), 629-635.
 - 5. R. V. Kadison, Infinite unitary groups, Trans. Amer. Math. Soc. 72 (1952), 386-399.
 - 6. I. Kaplansky, Rings of operators, Benjamin, New York, 1968.
- 7. C. Lanski, Lie structure in semi-prime rings with involution, Comm. Algebra 4 (1976), 731-746.
- 8. _____, Invariant submodules in semi-prime rings with involution, Comm. Algebra 6 (1978), 75-96.
 - 9. ____, Invariant subrings in rings with involution, Canad. J. Math. 30 (1978), 85-94.
- 10. K. McCrimmon and S. Montgomery, Open questions on rings with involution, Ring Theory Conf., Univ. of Chicago, Chicago, Illinois, July 1973.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CALIFORNIA 90007