Pacific Journal of Mathematics

LIE STRUCTURE OF PRIME RINGS OF CHARACTERISTIC 2

CHARLES PHILIP LANSKI AND SUSAN MONTGOMERY

Vol. 42, No. 1 January 1972

PACIFIC JOURNAL OF MATHEMATICS
Vol. 42, No. 1, 1972

LIE STRUCTURE OF PRIME RINGS OF CHARACTERISTIC 2

CHARLES LANSKI AND SUSAN MONTGOMERY

In this paper the Lie structure of prime rings of characteristic 2 is discussed. Results on Lie ideals are obtained. These results are then applied to the group of units of the ring, and also to Lie ideals of the symmetric elements when the ring has an involution. This work extends recent results of I. N. Herstein, C. Lanski and T. S. Erickson on prime rings whose characteristic is not 2, and results of S. Montgomery on simple rings of characteristic 2.

1. Prime rings. We first extend the results of Herstein [5]. Unless otherwise specified, all rings will be associative. If R is a ring, R has a Lie structure given by the product $[x, y] = xy - yx$, for $x, y \in R$. A Lie ideal of R is any additive subgroup U of R with $[u, r] \in U$ for all $u \in U$ and $r \in R$. By a commutative Lie ideal we mean a Lie ideal which generates a commutative subring of R.

Denote the center of R by Z. We recall that if R is prime, then the nonzero elements of Z are not zero divisors in R. In this case, if $Z \neq 0$ and F is the quotient field of R, then $R \otimes_Z F$ is a prime ring, every element of which can be written in the form $r \otimes a^{-1}$ for $a \in Z$, $a \neq 0$. Thus $R \otimes_Z F$ is naturally isomorphic to RZ^{-1}, the localization of R at Z. We will consider R imbedded in RZ^{-1} in the usual way (see [2]).

We begin with some easy lemmas.

LEMMA 1. *If R is semi prime and U is a Lie ideal of R with $u^2 = 0$ for all $u \in U$, then $U = 0$.*

Proof. Let $u \in U$, $x \in R$ then $0 = (ux - xu)^2 = uxux - ux^2u + xuxu$. Right multiply by ux to obtain $(ux)^3 = 0$. Thus uR is a nil right ideal of index 3. Since R is semi prime, by Levitzki's Theorem [6; Lemma 1.1] $u = 0$.

LEMMA 2. *Suppose $2R = 0$ and U is a commutative Lie ideal of R. Then $u^2 \in Z$ for all $u \in U$.*

Proof. Let $u \in U$, $x \in R$. Then $ux + xu \in U$ so $uxu + u^2x = xu^2 + uxu$. Hence $u^2 \in Z$.

LEMMA 3. *Let R be prime and I a nonzero ideal of R. If $[x, I] = 0$,*

then $x \in Z$.

Proof. If $r \in R$, then for $y \in I$, $ry \in I$ and so $0 = [x, ry] = [x, r]y$. Thus $[x, R]I = 0$. Since R is prime $[x, R] = 0$, so $x \in Z$.

THEOREM 4. *Let R be prime and U a commutative Lie ideal of R. Then $U \subset Z$ unless char $R = 2$, $Z \neq 0$ and RZ^{-1} is a simple ring 4-dimensional over its center.*

Proof. If char $R \neq 2$, then $U \subset Z$ by the proof of Lemma 1.3 of [6]. Hence we can assume char $R = 2$. By Lemma 2 $u^2 \in Z$ for all $u \in U$. If $Z = 0$ then by Lemma 1 $U = 0 \subset Z$. Thus we can assume $Z \neq 0$. Let F be the center of RZ^{-1}. If $\bar{U} = UZ^{-1}$, then $\bar{U}$ is still a commutative Lie ideal of RZ^{-1} and is not contained in F unless $U \subset Z$. Suppose I is a proper ideal of RZ^{-1}. Let $A = [\bar{U}, I]$. A is a Lie ideal of RZ^{-1} and is commutative since $A \subset \bar{U}$. Also $A \subset I$ so can contain no units. But Lemma 2 implies that every element of A squared is in F, hence must be zero. By Lemma 1, $A = 0$, and so $\bar{U} \subset F$ by Lemma 3 unless $I = 0$. If $U \not\subset Z$ then $I = 0$. Thus RZ^{-1} is simple. But it is well known in this case [6] that $\dim_F RZ^{-1} \leqq 4$.

We indicate two standard examples to show that prime rings of characteristic 2 can have noncentral commutative Lie ideals.

EXAMPLE 1. Let D be any commutative domain of characteristic 2, and D_2 the complete 2×2 matrix ring over D. Then

$$U = \left\{ \begin{pmatrix} ab \\ ba \end{pmatrix} a, b \in D \right\}$$

is a noncentral commutative Lie ideal of D_2.

EXAMPLE 2. Let F be any field of characteristic 2 with K a normal extension of degree 2. Let α be the generator of the Galois group of K over F. Let $R = K[x, \alpha]$ be the twisted polynomial ring over K where addition is as usual but multiplication is given by the rule $xk = k^\alpha x$ for $k \in K$. R is a domain, not simple, and $U = F[x]$ is a commutative subring of R which properly contains $Z = F[x^2]$. U is also a Lie ideal, for

$$[x^i, kx^j] = [x^i, k]x^j = (x^i k + kx^i)x^j = (k^{\alpha^i} + k)x^{i+j} .$$

If i is even then $k^{\alpha^i} = k$ and $k^{\alpha^i} + k = 0$ where as if i is odd $k^{\alpha^i} = k^\alpha$ and $k^{\alpha^i} + k = k^\alpha + k$ is the trace of k, so is in F.

If one wishes to consider the case for semi-prime rings there is immediate difficulty arising from taking various direct products of prime rings. Of course every semi prime ring is a subdirect sum of its prime images. If the given ring contains a non central commutative Lie ideal U, one can write the ring as a subdirect sum of two images A and B where the image of U in A is central and where B is a subdirect sum of prime rings of characteristic 2 each of which is an order in a simple ring of dimension at most 4 over its center. This decomposition does not seem very useful and we offer the following example which seems to indicate that one cannot say very much in the semi-prime case, even if the ring contains an idempotent and its center is a domain, which eliminates the difficulties arising from direct products.

EXAMPLE 3. Let S be the prime-ring of Example 2 and consider $R' = S[y]\{w, t\}$, the free ring with 1 generated by w and t over a polymonial ring over S. Let I be the ideal of R' generated by xw, yt, and w^2-w and let $R = R'/I$. By examining degrees of elements of R with respect to x, y, w, and t, one can show that $rtr = 0$ implies $r = 0$ for $r \in R$, and so, R is semi-prime. The center of R is $Z = F[x^2, y]$ a domain. Let U be the set of polynomials over F in $x^i y^j$ for $i, j, \geqq 1$. U is a commutative subring and can be shown to be a Lie ideal as in Example 2.

This example can be made "larger" by beginning with $S[Y]\{W\}$ where Y is a finite set, making sure that I contains $y_i w$ for each $w \in W$ and some $y_i \in Y$, and letting U be all polynomials over F in x and Y where x and each $y \in Y$ appears in every monomial.

There is one special case in which we can obtain a generalization.

THEOREM 5. *Let R be semi-prime and Z a field. If U is a commutative Lie ideal of R then $U \subset Z$ unless char $Z = 2$, R is simple and* $\dim_z R = 4$.

Proof. As in Theorem 4 we can dispense with the case that char $Z \neq 2$. Also as in Theorem 4 we can obtain that U commutes with every proper ideal of R. We may assume that R is not simple for otherwise we are done. If $I \neq 0$ is a proper ideal of R then $0 = [U, RI] = [U, R]I$, and so $0 = [U, R]RI$. If P is a prime ideal of R then either $I \subset P$ or $[U, R] \subset P$. If $[U, R] \subset P$ for all prime ideals, then since R is semi-prime $[U, R] = 0$ which says that $U \subset Z$. If $[U, R] \not\subset P_0$ for some prime P_0, then $I \subset P_0$ for every proper ideal I. Thus P_0 is the unique maximal ideal of R. If P is any other prime of R then $[U, R] \subset P$. But $\bigcap_{P \neq P_0} P = 0$, so again $U \subset Z$.

We proceed now to obtain results like those in [5] for prime rings. As one may expect our results are a bit stronger since we are dealing with prime rings. Our proofs are generally characteristic free and so throughout this section we will assume only that R is prime and if both char $R = 2$ and $Z \neq 0$, then dim RZ^{-1} over its center exceeds four. Hence by Theorem 4 we may always assume that any commutative Lie ideal of R must lie in Z.

LEMMA 6. *If U is a Lie ideal of R then either $U \subset Z$ or $C(U) \subset Z$ where $C(U) = \{x \in R \mid [x, U] = 0\}$.*

Proof. If $C(U)$ is commutative it is in Z by Theorem 4. If $C(U)$ is not commutative, since it is a subring and Lie ideal, it contains a nonzero ideal I of R [6; Lemma 1.3]. Hence $[U, I] = 0$ and $U \subset Z$ by Lemma 3.

LEMMA 7. *Let U_1, U_2 be Lie ideals of R with $[U_1, U_2] \subset Z$. Then either $U_1 \subset Z$ or $U_2 \subset Z$.*

Proof. If $[U_1, U_2] = 0$ then we have $U_1 \subset Z$ or $U_2 \subset Z$ by Lemma 6. Thus we can assume $Z \neq 0$. Let $V_1 = U_1 Z^{-1}$ and $V_2 = U_2 Z^{-1}$ in RZ^{-1}. Then V_1 and V_2 are still Lie ideals of RZ^{-1} and $[V_1, V_2] \subset F$, the center of RZ^{-1}. Let $u \in V_1$, $v \in V_2$ and $s \in RZ^{-1}$. Then $[u, [v, vs]] \in F$, and so, $[u, v[v, s]] = v[u, [v, s]] + [u, v][v, s] \in F$. If $[u, v] = 0$ for all $u \in V_1$ then $v \in F$ or $V_1 \subset F$ by Lemma 6. If $V_1 \subset F$, then $U_1 \subset Z$ and we are done. Suppose $U_1 \not\subset Z$ and $v \notin F$. Then there is $u \in V_1$ with $[u, v] = a \in F$ and $a \neq 0$. Thus $[v, s] \in F + Fv = W$ for all $s \in RZ^{-1}$. Hence W is a commutative Lie ideal of RZ^{-1}, so $W \subset F$ by Theorem 4. But then $v \in F$. Thus we must have $V_2 \subset F$, so $U_2 \subset Z$.

LEMMA 8. *If U is a Lie ideal of R and $[t, U] \subset Z$, then either $t \in Z$ or $U \subset Z$.*

Proof. Let $T = \{x \in R \mid [x, U] \subset Z\}$. T is clearly an additive subgroup of R. If $y \in R$ and $x \in T$, then $[[x, y], u] = [[x, u], y] + [x, [y, u]] \in Z$ for any $u \in U$. Thus T is a Lie ideal of R. By Lemma 7 either $T \subset Z$ or $U \subset Z$.

LEMMA 9. *If U is a Lie ideal of R, $x \in R$, $x^2 = 0$ and $xUx = 0$, then either $x = 0$ or $U \subset Z$.*

Proof. Let $u \in U$ and $r \in R$. Then we have $0 = x[u, r]x = xurx - xrux$. Replace r by $u_1 xr$ for $u_1 \in U$. Then $xuu_1xrx - xu_1xrux = xuu_1xrx = 0$. Since R is prime, either $x = 0$ or $xuu_1x = 0$ for $u, u_1 \in U$.

If $x \neq 0$, then using $x[u, r]x = 0$ again and replacing r by u_1u_2xr for $u_1u_2 \in U$, yields $xuu_1u_2x = 0$. Continuing we obtain $x\bar{U}x = 0$ where $\bar{U}$ is the subring generated by U. If $U \not\subset Z$ we must have $\bar{U}$ not commutative by Theorem 4. Hence $\bar{U}$ contains a nonzero ideal I of R [6; Lemma 1.3], thus $xIx = 0$. Since R is prime we must have $x = 0$, contradicting $x \neq 0$. Thus if $x \neq 0$ we must have $U \subset Z$.

LEMMA 10. *Let $U \not\subset Z$ be a Lie ideal of R and V an additive subgroup of R with $[U, V] \subset V$. If $v^2 = 0$ for all $v \in V$, then $V = 0$.*

Proof. Let $r \in R$, $u \in U$, and $v \in V$. Then $[u, r] \in U$, so $[v, [u, r]]^2 = 0$. That is $(vur - vru - urv + ruv)^2v = 0$. Expanding yields $vurvurv - vurvruv - vruvurv + vruvruv = 0$. Replacing r by rv give $vrvuvrvuv = 0$, and so, $(vuvr)^3 = 0$. Since R is prime $vuv = 0$. By Lemma 9, $v = 0$.

LEMMA 11. *$U \not\subset Z$ be a Lie ideal of R, and V an additive subgroup of R with $[V, U] \subset V$. If $[V, V] \subset Z$, then $V \subset Z$.*

Proof. Suppose first that $[V, V] = 0$. If char $R = 2$ then $0 = [v, [v, u]] = [v^2, u]$ for $v \in V$, $u \in U$. Thus since $U \not\subset Z$, $v^2 \in Z$ by Lemma 6. If $Z = 0$ then $V = 0$ by Lemma 10. If char $R \neq 2$ let $K = [V, U]$ and note that $[K, K] = 0$. If $v \in K$, $u \in U$ and $r \in R$ then $u[u, r] = [u, ur] \in U$, so

$$\begin{aligned} 0 = [v, [v, u[u, r]] &= [v, u[v, [u, r]]] + [v, [v, u][u, r]] \\ &= [v, u][v, [u, r]] + [v, u][v, [u, r]] . \end{aligned}$$

Since char $R \neq 2$ we have $[v, u][v, [u, r]] = 0$.

Let $r = vu$. Then

$$0 = [v, u][v, [u, vu]] = [v, u][v, [u, v]u] = [v, u][u, v][v, u] .$$

Thus for $v \in K$, $u \in U[v, u]^3 = 0$, and also $0 = [v, [v, u]] = v^2u - 2vuv + uv^2$. If $v \in K$ and $v^3 = 0$, then $0 = v^3uv - 2v^2uv^2 + vuv^3$ which implies $v^2uv^2 = 0$. Since $U \not\subset Z$, Lemma 9 says that $v^2 = 0$. But now, using $0 = [v, [v, u]]$, we have $vuv = 0$, so again by Lemma 9, $v = 0$. Since $[v, u]^3 = 0$ for any $v \in K$ we conclude that $[v, u] = 0$. By Lemma 6, $K = [V, U] \subset Z$. Thus $V \subset Z$ by Lemma 8. Thus if $[V, V] = 0$ we are done if char $R \neq 2$, so regardless of char R we are done if $Z = 0$. Therefore we may assume $Z \neq 0$.

Now assume that R is simple. Since $U \not\subset Z$ we have $U \supset [R, R]$ [6, Theorem 1.5]. Thus $W = V \cap [R, R]$ is a Lie ideal of $[R, R]$, so is $[R, R]$ or is in Z [6, Theorem 1.13]. But $[W, W] \subset Z$, so $W \neq [R, R]$ by repeated applications of Lemma 7. Hence $W \subset Z$, and so, $[V, [R, R]] \subset Z$. By Lemma 7 we have $V \subset Z$.

We may now assume that R is not simple. Let $V_1 = VZ^{-1}$ and $U_1 = UZ^{-1}$. U_1 is a Lie ideal of RZ^{-1} not contained in F, the center of RZ^{-1}, V_1 is an additive subgroup of RZ^{-1}, $[V_1, U_1] \subset V_1$, and $[V_1, V_1] \subset F$. If RZ^{-1} is simple we are done as above. Let $I \neq 0$ be a proper ideal of RZ^{-1}. Set $J = [U_1, I]$, J is a Lie ideal of RZ^{-1} and is contained in $U_1 \cap I$. Let $W = [V_1, J] \subset V_1 \cap J$. Now $[W, W] \subset F \cap J \subset F \cap I$. Since I is proper we must have $[W, W] = 0$. But $[W, U_1] \subset W$ so as above, if char $R \neq 2$ then $W \subset F$ while if char $R = 2$ then the square of every element of W is in F. But again $W \subset J \subset I$, a proper ideal containing no units, so in either case the square of very element in W is zero. By Lemma 10, $W = 0$. Thus $[V_1, J] = 0$. Since J is a Lie ideal of RZ^{-1}, by Lemma 6 either $J \subset F$ or $V_1 \subset F$. If $V_1 \subset F$ then $V \subset Z$. If $J \subset F$ then $[U_1, I] \subset F$. Using Lemma 7 we conclude $U_1 \subset F$ or $I \subset F$, both of which are impossible. Thus we must have $V \subset Z$.

THEOREM 12. *Let W be a subring of R, U a Lie ideal of R and $[W, U] \subset W$. Then either $U \subset Z$, $W \subset Z$ or $W \supset M \neq 0$ an ideal of R.*

Proof. The first half of the proof is almost the same as that of Theorem 3 of [5]. We repeat it here for convenience. Let $V = [W, U]$. If $V = 0$ then $U \subset Z$ or $W \subset Z$ by Lemma 6. Assume $V \neq 0$. Let $t \in V$, $w \in W$, and $r \in R$. Since $V \subset W \cap U$ we have $[t, tr] \in U$, and so $[w, [t, tr]] \in W$. Thus $[w, t[t, r]] \in W$. Now $[w, t[t, r]] = t[w, [t, r]] + [w, t][t, r] \in W$. Since $t \in W$ and $[w, [t, r]] \in W$, we obtain

$$(A) \qquad [w, t][t, r] \in W .$$

Replacing r by yr with $y \in W$ yields

$$(B) \qquad [w, t][t, yr] = [w, t]y[t, r] + [w, t][t, y]r \in W .$$

Since $t \in V \subset U$, $[t, r] \in U$, so $[y, [t, r]] \in W$. Thus $y[t, r] = [t, r]y + k$ for some $k \in W$. Hence $[w, t]y[t, r] = [w, t][t, r]y + [w, t]k$. By (A) $[w, t][t, r] \in W$, hence $[w, t]y[t, r] \in W$. Thus (B) implies $[w, t][t, r]R \subset W$. Commutating repeatedly with U gives $\bar{U}[w, t][t, y]R \subset W$, where $\bar{U}$ is the subring generated by U. If U is commutative then $U \subset Z$ by Theorem 4. If $U \not\subset Z$ then $\bar{U}$ containes a nonzero ideal I of R by Lemma 1.3 of [6]. But then $M = I[w, t][t, y]R$ is an ideal of R in W. We are done if $M \neq 0$, so suppose $M = 0$. Since R is prime we have

$$(C) \qquad [w, t][t, y] = 0 \text{ for } t \in V \text{ and } w, y \in W .$$

In particular, if $w = y \in V$, then $[w, t]^2 = 0$. Let $K = [V, V]$. K is a Lie ideal of U contained in V, and if $v_1, v_2, v_3 \in K$ with $v_i^2 = 0$ then

by (C) we have $[v_1, v_2][v_1, v_3] = 0$. Expanding gives $v_1v_2v_1v_3 - v_1v_2v_3v_1 + v_2v_1v_3v_1 = 0$. Right multiplication by v_1 gives

$$(D) \qquad v_1v_2v_1v_3v_1 = 0 .$$

Now $[v_3, u] \in K$ for any $u \in U$, hence $[v_3, [u, v_1]] \in K$. Thus $v_1v_2v_1[v_3, [u, v_1]]v_1 = 0$. Expanding this expression yields $v_1v_2v_1(v_3uv_1 - v_3v_1u - uv_1v_3 + v_1uv_3)v_1 = 0$. Using (D) we obtain $v_1v_2v_1uv_1v_3v_1 = 0$. Since $v_1^2 = 0$, by Lemma 9 we conclude that $v_1Kv_1 = 0$ if $U \not\subset Z$. Suppose now that $v_1, v_2 \in K$ with $v_1^2 = v_2^2 = 0$. First we conclude that $(v_1v_2)^2 \in v_1Kv_1v_2 = 0$. If $u \in U$ then we also have $0 = v_1[v_2u]v_1v_2 = v_1v_2uv_1v_2$. Lemma 9 again implies that $v_1v_2 = 0$ if $U \not\subset Z$. But if $t_1, t_2 \in V$ then $[t_1, t_2] \in K$ and has square zero by (C). Since K is additively generated by such elements, by what we have just shown, every element in K has square zero. By Lemma 10, $K = 0$ if $U \not\subset Z$. But now we have $[V, V] = 0$ which implies $V \subset Z$ if $U \not\subset Z$, by Lemma 11. Since $V = [W, U] \subset Z$, Lemma 8 says that either $W \subset Z$ or $U \subset Z$. Thus assuming W contains no ideals leads to the conclusion that either $W \subset Z$ or $U \subset Z$, which establishes the theorem.

THEOREM 13. *Let U be a Lie ideal of R and V an additive subgroup of R with $[V, U] \subset V$. Then either $V \subset Z$, $U \subset Z$,* or *$V \supset [M, R] \neq 0$ for M an ideal of R.*

Proof. Following the proof of Theorem 5 of [5], let $A = [U, V]$, $T = \{x \in R \mid [x, R] \subset A\}$, and T_0 be the subring of T generated by $[A, A]$. Then, as in the proof in [5], $[T_0, U] \subset T_0$, so by Theorem 12 either $T_0 \subset Z$, $U \subset Z$, or T_0 contains $M \neq 0$ an ideal of R. If $T_0 \subset Z$, then $[A, A] \subset Z$ so $A \subset Z$ by Lemma 11. But $[U, V] \subset Z$ implies either $U \subset Z$ or $V \subset Z$ by Lemma 8. If $M \subset T_0 \subset T$, then $[M, R] \subset A \subset V$ and we are done.

II. **The group of units in a prime ring.** We now turn to results concerning normal subgroups and conjugates in prime rings Again R will always be assumed to be prime, now with identity, and if char $R = 2$ then dim RZ^{-1} over its center must exceed four. The proofs are similar to those in [7] and [8] but will be repeated, without going into detail, for convenience. We call a subset W of R G-normal for $G \subset U$, the group of units of R, if W is invariant under conjuation by all elements of G. If $G = U$ we just say that W is normal. The notation $L \subset S$ will mean that the subgroup S generated by all elements of square zero contains a noncentral Lie ideal L of R. See [7] for a discussion of this condition and for examples when R has no idempotents. Finally $|A|$ denotes the cardinality of A.

THEOREM 14. *Let $L \subset S$, $|Z| > 2$, and W a normal Z-submodule of R. Then $W \subset Z$ or $W \supset [M, R] \neq 0$ for M an ideal of R. If W is a subring, then $W \subset Z$ or $W \supset M$.*

Proof. For $a^2 = 0$ and $w \in W$, $(1 + a)w(1 - a) = w + aw - wa - awa \in W$. Using the fact that W is a Z-submodule, $|Z| > 2$, and $(za)^2 = 0$ for $z \in Z$, we obtain $[w, za] \in W$ for $z \neq 0 \in Z$ and independent of $w \in W$ and "a". Thus $[W, zL] \subset W$. Since zL is a noncentral Lie ideal of R, we have $W \subset Z$ or $W \supset [M, R]$ by Theorem 13. If W were a subring and $[M, R] \subset W$, then Lemma 1.3 of [6] implies that W contains an ideal unless $[M, R]$ is commutative. But then Theorem 4 says $[M, R] \subset Z$, and so $M \subset Z$ by Lemma 8, which is impossible in a prime ring.

THEOREM 15. *Let $L \subset S$, $|Z| > 4$ and W a G-normal Z submodule of R where $G \lhd U$. Then $G \subset Z$, $W \subset Z$, or $W \supset [M, R] \neq 0$ for M an ideal of R. If W is a subring, then $G \subset Z$, $W \subset Z$ or $W \supset M \neq 0$.*

Proof. If $a^2 = 0$, $g \in G$, and $w \in W$, then $h = (1 - a)g(1 + a)g^{-1} \in G$, so $hwh^{-1} \in W$. Expanding gives $w + f_1(a) + \cdots + f_4(a) \in W$ where $f_i(za) = z^i f_i(a)$ for $z \in Z$. Using $|Z| > 4$ and the fact that W is a Z submodule (See Lemma 4.4 in [7]) we obtain $cf_1(a) = [w, c(a - gag^{-1})] \in W$, where $c \neq 0 \in Z$ is independent of w, g, and "a". Let T be the Z submodule generated by all $c(a - gag^{-1})$ for $a^2 = 0$ and $g \in G$. Since T is normal, Theorem 14 implies that $T \subset Z$ or $T \supset [K, R] \neq 0$ for K an ideal of R. Suppose first that $T \subset Z$. Then $ac(a - gag^{-1})a = -cagag^{-1}a = 0$, so $agag^{-1}a = 0$. This implies that $(c(a - gag^{-1}))^3 = 0$. But a central element in a prime cannot be nilpotent unless it is zero. Hence $a = gag^{-1}$. The result is that $[G, L] = 0$. Since $L \not\subset Z$ we have $G \subset Z$ by Lemma 6.

Now consider the possibility that $[K, R] \subset T$. Then $[W, [K, R]] \subset W$, so Theorem 13 implies that $W \subset Z$, $[K, R] \subset Z$ or $W \supset [M, R] \neq 0$. But $[K, R] \subset Z$ is impossible since it would say $K \subset Z$, by Lemma 7, and so $[K, R] = 0$. If W is a subring we proceed as Theorem 14.

LEMMA 16. *Let $L \subset S$ and $|Z| > 2$. If $N \lhd U$ and N is abelian, then $N \subset Z$.*

Proof. Let $W = ZN$. Then W is a normal Z module so by Theorem 14 either $W \subset Z$ or $W \supset [M, R] \neq 0$. If $W \subset Z$ then clearly $N \subset Z$. If $W \supset [M, R]$, then since $[M, R]$ is a commutative Lie ideal, $[M, R] \subset Z$ by Theorem 4. But then $M \subset Z$, Lemma 7, which is impossible in a prime ring.

THEOREM 17. *Let* $L \subset S$ *and* $|Z| > 4$. *If* $N \lhd U$ *and is solvable then* $N \subset Z$.

Proof. Let the derived series for N be $1 \lhd N^{(k)} \lhd \cdots \lhd N$. If $k = 1$ then N is abelian so $N \subset Z$ by Lemma 16. In any event $N^{(k)}$ is normal and abelian so $N^{(k)} \subset Z$. Suppose $k > 1$. Let $x, y \in N^{(k-1)}$. Then $yxy^{-1} = zx$ for $z \in Z$. Thus $Z[x]$, the ring generated by x over Z is $N^{(k-1)}$-normal, so by Theorem 15 either $Z[x] \subset Z$, which says that $x \in Z$, or $Z[x] \supset M \neq 0$ an ideal of R. But prime rings cannot have commutative ideals (note that $L \not\subset Z$ says R is not commutative) so $x \in Z$. Thus $N^{(k-1)} \subset Z$, a contradiction. We must conclude that $k = 1$ and so $N \subset Z$.

As in [7] and [8] the last three results can be extended to normal subgroups of normal subgroups by assuming $|Z| > 8$. The proofs use the same techniques presented here and so will not be given. For details see Theorem 23 in [8].

Given $x \in R - Z$ and $G \lhd U$ what does the set of G-conjugates of x look like? In [8] it was shown that if $L \subset S$ and char $R \neq 2, 3$ then the set must be infinite unless R is finite. Here we eliminate the characteristic assumptions on R but still assume that R is prime with 1 and if char $R = 2$ then $\dim RZ^{-1}$ over its center exceeds four.

LEMMA 18. *Let* $L \subset S$, $|Z| > 2$ *and* $x \in R - Z$. *Then* x *has infinitely many conjugates unless* R *is finite.*

Proof. Let $K = \{y \in U \mid yx = xy\}$. If x has only a finite number of conjugates then K is a subgroup of finite index in U, K has only finitely many conjugates, and each conjugate is finite index. If G is the intersection of the conjugates of K, then $G \lhd U$, G is of finite index, and $[x, G] = 0$. Since GZ is a normal Z submodule of R, Theorem 14 implies that $GZ \subset Z$ or $GZ \supset [M, R] \neq 0$. If $GZ \supset [M, R]$ then $[x, [M, R]] = 0$, so $x \in Z$ or $[M, R] \subset Z$ by Lemma 6. But $x \notin Z$ and $[M, R] \subset Z$ implies $M \subset Z$ by Lemma 7, so $[M, R] = 0$, a contradiction. Thus we must have $GZ \subset Z$, and so $G \subset Z$. That is, $Z \cap U$ is of finite index in U.

Suppose $a^2 = 0$. Then $1 + za$ is a unit for any $z \in Z$, and $1 + z_1a$ and $1 + z_2a$ are in the same coset of $Z \cap U$ exactly when $1 + (z_1 - z_2)a \in Z$. But this implies $(z_1 - z_2)a \in Z$. Since Z contains no divisors of zero and $a^2 = 0$, we must have $z_1 = z_2$. Since $Z \cap U$ is of finite index in U, Z must be finite, so $Z^* = Z - 0$ is a multiplicative group. Hence $Z \cap U = Z^*$, and so, U must be finite. Since $1 + a$ a unit for any "a" of square zero, there can only be a finite number of elements of

square zero. Thus S, the subgroup they generate must be finite. Since $L \subset S$, L must be finite. As $L \not\subset Z$, $[L, R] \neq 0$. By Lemma 13 of [8] $R[L, R]R$ is a nonzero ideal of R which is finitely generated as a module over the integers. But char R is finite, so $R[L, R]R$ is finite. Since R is prime and contains a finite ideal, R itself must be finite.

THEOREM 19. *Let $L \subset S$, $|Z| > 4$, $x \in R - Z$, and $G \lhd U$. Then x has infinitely many G conjugates unless $G \subset Z$ or R is finite.*

Proof. As in Lemma 18, if x has only finite many G conjugates, then the intersection, say N, of the G conjugates of the centralizer of x in G has the properties that $N \lhd G$, N is of finite index in G, and $[x, N] = 0$. Now NZ is a G-normal Z submodule of R and a subring, so by Theorem 15 either $G \subset Z$, $NZ \subset Z$, or $NZ \supset M \neq 0$. If $G \subset Z$ we are done. If $M \subset NZ$, then $[x, M] = 0$ so $x \in Z$ by Lemma 3. Thus we can assume $N \subset Z$. If Z is finite then G is finite, since N is of finite index in G. But then, if $g \in G$, g has only a finite number of conjugates in R, so either $g \in Z$ or R is finite by Lemma 18. In either case we are done. We may therefore assume that Z is infinite.

Let $g_1, \cdots, g_k$ be a complete set of coset representatives of N in G. Since G is normal, if $a^2 = 0$ and $c \in Z$, then since $(ca)^2 = 0$ we have for any $g \in G$ that $(1 + ca)g(1 - ca) = g_i s$ for some $s \in N$. Since Z is infinite there must be an infinite subset P_1 of Z so that if $k \in P_1$ then $(1 + ka)g(1 - ka) = g_j s_k$ where j is fixed and $s_k \in N$. Given $z \in Z$ there is an infinite subset P_2 of Z so that $k \in P_2$ implies $(1 + k(za))g(1 - k(za)) = g_i t_k$ where g and "a" are the same as above, i is fixed and $t_k \in N$. Thus given some $g \in G$, $a \in R$ with $a^2 = 0$ and $c_1, \cdots, c_m \in Z$ we can find an infinite subset P_m of Z with every $k \in P_m$ satisfying

$$(1 + k(c_i a))g(1 - k(c_i a)) = g_j \eta_k$$

where j depends only on i and not on k.

If $k_1, k_2 \in P_m$ then

$$h = (1 + k_1(c_i a))g(1 - k_1(c_i a))(1 + k_2(c_i a))g^{-1}(1 - k_2(c_i a)) \in N$$

for *each* $i = 1, \cdots, m$. Thus $[x, h] = 0$. Expanding gives

$$[x, 1 + (k_1 - k_2)(c_i a - g c_i a g^{-1}) - k_1(k_1 - k_2)c_i^2 a g a g^{-1} + k_2(k_1 - k_2)c_i^2 g a^{-1} g a + k_1 k_2 (k_1 - k_2) c_i^3 a g a g^{-1} a] = 0 .$$

If we use a sufficient number of c_i then by combining the relations obtained, as in Lemma 4.4 of [6], we can conclude that $[x, (k_1 - k_2)c(a - gag^{-1})] = 0$ where $c \neq 0 \in Z$. Thus $[x, a - gag^{-1}] = 0$

for any $g \in G$ and $a \in R$ with $a^2 = 0$. Let T be the Z module generated by all $a - gag^{-1}$. Since T is a normal set either $T \subset Z$ or $T \supset [M, R] \neq 0$ by Theorem 14. If $T \supset [M, R]$, then $[x, [M, R]] = 0$ and we are led to a contradiction as we have seen in Lemma 18. If $T \subset Z$ then just as in the proof of Theorem 15 we get $G \subset Z$. Having exhausted all possibilities, the Theorem is established.

An immediate consequence of Theorem 19 is

COROLLARY 20. *Let $L \subset S$, $|Z| > 4$ and $N \lhd G \lhd U$. Suppose that $N \not\subset Z$ and that R is not finite. Then*

(i) *N is infinite*

(ii) *If S is any finite G-normal subset of R then $S \subset Z$.*

(iii) *If $f(x) \in Z[x]$ has a noncentral root in a G-normal subset S, then $f(x)$ has infinitely many roots in S.*

III. Rings with involution. In this section we examine the Lie structure of prime rings with involution of characteristic 2, applying the results of §I. These results generalize theorems in [10] which describe the Lie structure of the symmetric elements of a simple ring with involution of characteristic 2. Analogous results for the skew-symmetric elements in characteristic not 2 have been obtained by T. S. Erickson [3]. There appears to be little hope of extending the results further, even to semi-prime rings, because of Example 3.

Let R denote a prime ring of characteristic 2, with an involution*, and center Z. Let $S = \{x \in R \mid x^* = x\}$ denote the symmetric elements of R; S is a Lie subring of R under the product $[x, y] = xy + yx$. The involution is said to be of the *first kind* if $Z \subset S$, and of the *second kind* if $Z \not\subset S$.

We consider first the case when the involution is of the first kind; so, assume from now through Theorem 37 that $Z \subset S$. Let $V = \{x + x^* \mid x \in R\}$, a Lie subring of S. As in [10], to study the Lie structure of S we will actually work with V. If I is a*-ideal of R (that is, an ideal closed under*), define $V_I = \{x + x^* \mid x \in I\}$. Now $V_I \subseteqq V \cap I$, and in our results V_I will assume the position of $K \cap I$ (where K denotes the skew-symmetric elements) in the theorems of Erickson.

If R is simple, it was shown in [10] that V, S and $[V, V]$ were essentially simple as Lie rings, unless $\dim_z R \leqq 16$ (in which case the conclusions are false). In the prime case, our theorems will hold unless R is an order in a simple ring Q (that is, Q is a right or left quotient ring of R) which is of dimension $\leqq 36$ over its center C. Though $\dim_c Q \leqq 16$ should be the appropriate condition, the methods of [10] do not apply to the smaller dimensions.

Before proceeding, we point out that any nonzero ideal of R contains a *-ideal. For, let I be any nonzero ideal of R. Then $I^* = \{i^* | i \in I\}$ is also an ideal of R, and $I \cap I^*$ is a *-ideal of R contained in I. $I \cap I^* \neq (0)$, since R is a prime ring (for more on *-ideals, see [9]). Finally, if A is any subset of R, let A' denote the subring of R generated by A. We first prove:

THEOREM 21. *V' contains a nonzero *-ideal of R, unless R is an order in a simple ring Q, with center C, such that* $\dim_C Q \leqq 4$.

Proof. By Lemma 1 of [10], V' is a Lie ideal of R. Thus by Theorem 12, either V' contains a nonzero ideal of R or $V' \subset Z$. If V' contains an ideal of R, then V' contains a nonzero *-ideal of R by the above remarks. We may therefore assume that $V' \subset Z$. Then $[V, V] = (0)$ and so V satisfies a polynomial identity of degree 2. By a theorem of Amitsur [1], this implies that R satisfies a polynomial identity of degree $\leqq 4$. But now by a theorem of Posner [4, p. 184], since R is a prime ring satisfying a polynomial identity, R is an order in a simple ring Q which is finite dimensional over its center C. In addition, Q satisfies an identity of degree $d \leqq 4$, and so by a well-known theorem of Kaplansky [4, p. 157], $\dim_C Q \leqq [d/2]^2 \leqq 4$.

We show next that if I is an nonzero *-ideal of R, then V_I is actually nontrivial.

LEMMA 22. *Let I be a nonzero *-ideal of R. Then*
(1) *V_I, $[V_I, V]$, and $[V_I, V_I]$ are all nonzero, and*
(2) *V_I' contains a nonzero *-ideal of R*
unless R is an order in a simple ring Q, with center C, such that $\dim_C Q \leqq 4$.

Proof. To show (1), it will be enough to show $[V_I, V_I] \neq (0)$. So, assume that $[V_I, V_I] = (0)$. Since I is an ideal in the prime ring R, I itself is a prime ring in which V_I satisfies a polynomial identity of degree 2. By the same argument as in Theorem 21, this implies that I is an order in a simple ring Q of dimension $\leqq 4$ over its center. But then R would also be an order in the same ring Q.

To show that V_I' contains a nonzero *-ideal of R, it will suffice to show that V_I' contains a nonzero ideal of R. Now if the prime ring I were an order in a simple Q, $\dim_C Q \leqq 4$, then R would be also. So by Theorem 21 applied to I, we may assume that V_I' contains a nonzero ideal L of I. Since I is prime, $ILI \neq 0$; But ILI is a nonzero ideal of R in V_I'.

The next lemma gives a criterion for when a Lie ideal contains V_I.

LEMMA 23. *Let A be an additive subgroup of V such that A' contains a nonzero ideal I of R, and let U be an additive subgroup of R with $[U, A] \subset U$. Suppose there exists $c \neq 0$ in S such that $cx + x^*c \in U$, all $x \in I$. Then $U \supseteq V_J$, for some nonzero *-ideal J of R.*

Proof. Let $x \in I$ and $a \in A$. Now

$$[cx + x^*c, a] = acx + (acx)^* + cxa + (xa)^*c .$$

Since $[cx + x^*c, a] \in U$ and $c(xa) + (xa)^*c \in U$, we must have $acx + (acx)^* \in U$. By induction, exactly as in Theorem 2 of [10], it is possible to show that $bcx + (bcx)^* \in U$, all $b \in A^n$, and thus $bca + (bcx)^* \in U$, all $b \in A'$. Then $ycx + (ycx)^* \in U$, for all $x, y \in I$. Let $J = IcI$; $J \neq (0)$ since R is prime, and $V_J \subset U$. J is a *-ideal of R since $c^* = c$.

COROLLARY 24. *If U and A are as in Lemma 23, then U' contains a nonzero *-ideal of R, unless R is an order in a simple ring Q, with center C, such that* $\dim_c Q \leqq 4$.

Proof. By Lemma 23, $U \supset V_J$, where J is a nonzero *-ideal of R. Thus $U' \supset V_J'$, so apply Lemma 22 to V_J'.

The next theorem is the only point at which $\dim_c Q \leqq 36$ (rather than $\dim_c Q \leqq 16$) seems necessary. However, the theorem is crucial in what follows.

THEOREM 25. *$[V, V]'$ contains a nonzero *-ideal of R, unless R is an order in a simple ring Q, with center C, such that* $\dim_c Q \leqq 36$.

Proof. Let $W = [V, V]$. Now W is a Lie ideal of V, so if $a, b \in W$ and $x \in R$, we have

$$(a^2b + ba^2)x + x^*(a^2b + ba^2) \in W'$$

by Lemma 2 of [10]. If for some $a, b \in W$, $a^2b + ba^2 \neq 0$, we may apply Corollary 24 with $U = W$, $A = V$, and $(c = a^2b + ba^2)$ to see that W' contains a nonzero *-ideal of R.

We may assume that $a^2b + ba^2 = 0$, all $a, b \in W$. But then V satisfies a polynomial identity of degree 6, so by the same argument as in the proof of Theorem 21, R is an order in a simple ring Q, with $\dim_c Q \leqq 36$.

COROLLARY 26. *If $a \in R$ centralizes $[V, V]$, then $a \in Z$, unless R is an order in a simple ring Q,* $\dim_c Q \leqq 36$.

Proof. If a centralizes $[V, V]$, then by Theorem 25, a centralizes

a nonzero ideal of R. Since R is prime, this implies $a \in Z$.

We have now finished the preliminaries and can begin the actual description of Lie ideals of V.

LEMMA 27. *If U is a Lie ideal of V such that $u^2 = 0$ for all $u \in U$, then $U = (0)$.*

Proof. Say $u \in U$ and $v \in V$. Then $uv + vu \in U$, and so $(uv + vu)^2 = 0 = uvuv + uv^2u + vuvu$ since $u^2 = 0$. Multiplying on the right by u, we see $uvuvu = 0$. Linearizing on v and multiplying by vu again, we get $uvuwuvu = 0$, for all $v, w \in V$. Thus $uvuVuvu = 0$, all $v \in V$. But in a prime ring, whenever $aVa = 0$ with $a^2 = 0$ and $a \in V$, it must happen that $a = 0$ (by Lemma 4 of [10]. Thus $uvu = 0$, all $v \in V$, and so $u = 0$ by repeating the argument. Thus $U = (0)$.

LEMMA 28. *If U is a Lie ideal of V such that $u^2 \in Z$, all $u \in U$, then $U \subset Z$ unless R is an order in a simple ring Q, $\dim_c Q \leqq 16$.*

Proof. First observe that by linearizing the relation $u^2 \in Z$, we obtain $[U, U] \subset Z$. Now if R is simple, then by Theorem 5 of [10], either $U \subset Z$ or $U \supseteq [V, V]$, unless $\dim_z R \leqq 16$. If $U \supseteq [V, V]$, then $[[V, V], [V, V]] \subseteq [U, U] \subset Z$. But by Theorem 7 of [10], $[V, V] = [[V, V], [V, V]]$, and thus $[V, V] \subset Z$. Then certainly $[[V, V], V] = 0$; this means that V satisfies a polynomial identity of degree 3. By applying the theorems of Amitsur and Kaplansky as in Theorem 21, we see $\dim_z R \leqq 9$.

We may therefore assume that R is *not* simple. Let I be a nonzero ideal of R. As before, we may assume that I is actually a *-ideal of R.

First we claim that $I \cap V \neq 0$. For, if $I \cap V = (0)$, choose $x \in I$. Then $x^* \in I$, and $x + x^* \in I \cap V = (0)$. But then $x = x^*$; that is, $I \subseteq S$. Let $r \in R$. Since I is an ideal of R, $Ir \subseteq S$, so $(ir)^* = r^*i = ir$, all $i \in I, r \in R$. In particular, $is = si$, all $s \in S$. By Theorem 21, this implies that I commutes with a nonzero ideal of R, and so $I \subseteq Z$ since R is prime. But now any element of R commutes with I, a nonzero ideal, and so must be in Z. Thus $R \subseteq Z$; that is, R is commutative, a contradiction. Thus $I \cap V \neq (0)$.

For the remainder of the proof, we assume that the center of R is a field (as has been done previously, we consider RZ^{-1}). We claim that $[U, I \cap V] = 0$. For $[U, I \cap V] \subseteq U \cap I$, which is a Lie ideal of V. Now if $a \in U \cap I$, and $a^2 \neq 0$, a would be invertible since $a^2 \in Z$. This contradicts I being a proper ideal of R. Thus $a^2 = 0$, all $a \in U \cap I$. By Lemma 27, $U \cap I = (0)$, and so $[U, I \cap V] = (0)$.

Let $c \neq 0$ be any element of $I \cap V$. Then $cx + x^*c \in I \cap V$, for

any $x \in R$. Using Corollary 23 with $I \cap V$ and $A = V$, we see that $(I \cap V)'$ contains a nonzero ideal of R. But then since $[U, I \cap V] = 0$, U must commute with a nonzero ideal of R. Thus $U \subset Z$ since R is prime.

LEMMA 29. *If U is a Lie ideal of V, then either u^2 centralizes U, all $u \in U$, or $U \supset [V_J, V]$, for some nonzero *-ideal J of R.*

Proof. Define $T(U) = \{x \in V \mid [x, V] \subset U\}$; $T(U)$ is a Lie ideal of V. By Lemma 8 of [10], if $a, b \in U$ and $x \in R$, then

$$(a^2b + ba^2)x + x^*(a^2b + ba^2) \in T(U) .$$

Assume that $a^2b + ba^2 = c \neq 0$, for some $a, b \in U$. Then $cx + x^*c \in T(U)$, for all $x \in R$, so by Lemma 23, $T(U) \supset V_J$, for some nonzero *-ideal J of R. Thus $[V_J, V] \subseteqq U$.

We may thus assume that $a^2b + ba^2 = 0$, for all $a, b \in U$. This is simply the statement that a^2 centralizes U, for all $a \in U$.

LEMMA 30. *If U is an additive subset of S such that $[U, A] \subset U$, where $[A, A]'$ contains a nonzero ideal of R, then $[U, U] \subset Z$ implies $u^2 \in Z$, all $u \in U$.*

Proof. Let $u \in U$ and $a \in A$. Now

$$u^2a + au^2 = [u, [u, a]] \in [U, U] \subset Z .$$

Thus $[u^2a + au^2, a] = 0 = u^2a^2 + a^2u^2$. Linearizing on a, we have $[u^2, [a, b]] = 0$ for all $a, b \in A$, and thus u^2 centralizes $[A, A]$. By hypothesis, this implies that u^2 centralizes a nonzero ideal of R, and so $u^2 \in Z$.

We are now able to prove the complete structure theorem for Lie ideals of V.

THEOREM 31. *Any Lie ideal of V is either contained in Z, or contains $[V_J, V]$ for some nonzero *-ideal J of R, unless R is an order in a simple ring Q of dimension $\leqq 36$ over its center.*

Proof. Let U be any Lie ideal of V, and say $U \not\supseteq [V_J, V]$ for all ideals J of R. Then by Lemma 29, $[u^2, U] = 0$ for all $u \in U$. Linearizing, $[[U, U], U] = (0)$ and so $[U, U]$ is a commutative Lie ideal of V. Let $w \in [U, U]$. Then $wv + vw \in [U, U]$, all $v \in V$, and $[w, wv + vw] = 0 = w^2v + vw^2$. In other words, w^2 centralizes V. By Theorem 21 this means that w^2 centralizes a nonzero ideal of R, and so $w^2 \in Z$. By Lemma 28, $[U, U] \subset Z$. But now since $[V, V]'$ contains a nonzero

ideal of R by Theorem 25, we may apply Lemma 30 to see that $u^2 \in Z$ for all $u \in U$. By a second application of Lemma 28, we see that $U \subset Z$.

COROLLARY 32. *$[[V, V], [V, V]]'$ contains a nonzero *-ideal of R, unless R is an order in a simple ring Q, $\dim_c Q \leqq 36$.*

Proof. Let $W = [[V, V], [V, V]]$; W is a Lie ideal of V, so by Theorem 31 either $W \subset Z$ or $W \supseteqq [V_J, V]$ for some nonzero *-ideal J of R. If $W \supseteqq [V_J, V]$, consider $[V_J, V_J]$, which is nonzero by Lemma 22. By Theorem 25 applied to the prime ring J, it follows that $[V_J, V_J]'$ contains a nonzero *-ideal L of J. But then exactly as in Lemma 22, JLJ is a nonzero *-ideal of R contained in W', and we are done.

Therefore assume that $W = [[V, V], [V, V]] \subset Z$. By, Lemma 30, since $[V, V]$ is a Lie ideal of V and $[V, V]'$ contains a nonzero ideal of R by Theorem 25, we obtain $w^2 \in Z$, all $w \in [V, V]$. By Lemma 28, this implies $[V, V] \subset Z$. Repeating the argument, we find $V \subset Z$, so by Theorem 21 Z contains a nonzero ideal of R, and so R is commutative, a contradiction, unless R is an order in a simple ring Q with $\dim_c Q \leqq 4$.

As a corollary to Theorem 31, we are also able to give a complete description of Lie ideals of S.

THEOREM 33. *Any Lie ideal of S is either contained in Z or contains $[V_J, V]$ for some nonzero *-ideal J of R, unless R is an order in a simple ring Q of dimension $\leqq 36$ over its center.*

Proof. Let U be a Lie ideal of S, and let $W = [U, S]$. Then W is a Lie ideal of V. By Theorem 31, either $W \supseteqq [V_J, V]$ for some *-ideal J or $W \subset Z$. If $W \supset [V_J, V]$, then certainly $U \supseteqq [U, S] \supseteqq [V_J, V]$. So, assume $W = [U, S] \subset Z$. Since $V \subset S$, $[U, [V, V]] \subseteqq [[U, V], V] = (0)$, and thus U centralizes $[V, V]$. By Theorem 25, $U \subset Z$.

Having described the Lie structure of V and S, we now turn to Lie ideals of $[V, V]$. We will assume for the remainder of the proofs that R is *not* an order in a simple ring Q, such that $\dim_c Q \leqq 36$. As a first step in the proof, we prove a crucial lemma—the analog of Lemma 28.

LEMMA 34. *If U is a Lie ideal of $[V, V]$ such that $u^2 \in Z$, all $u \in U$, then $U \subset Z$.*

Proof. As in Lemma 28, we have $[U, U] \subset Z$. If R is simple,

we argue exactly as in Lemma 28 (using Theorem 11 of [10]) to show that $[V, V] \subset Z$, and so $\dim_z R \leqq 9$, unless $U \subset Z$. We may therefore assume that R contains a nonzero*-ideal I.

We claim that $I \cap [V, V] \neq (0)$. For, say that $I \cap [V, V] = (0)$. By exactly the same argument as in Lemma 28, we obtain $I \cap V \neq (0)$. But $[I \cap V, V] \subseteqq [V, V] \cap I = (0)$, and so $I \cap V$ centralizes V. By Theorem 21, $I \cap V$ centralizes a nonzero ideal of R, and so $I \cap V \subset Z$ since R is prime. Since we may assume without loss of generality that the center of R is a field, $I \cap V$ would contain an invertible element of R, which contradicts I being a proper ideal of R. Thus $I \cap [V, V] \neq (0)$.

Again, by exactly the same proof as in Lemma 28, we see that $[U, I \cap [V, V]] = (0)$, and so to show that $U \subset Z$, it will be enough to show that $(I \cap [V, V])'$ contains a nonzero ideal of R.

Now $[I \cap [V, V], V] \subseteqq I \cap [V, V]$, since I is an ideal of R and $[[V, V], V] \subseteqq [V, V]$. Thus $I \cap [V, V]$ is a Lie ideal of V. By Theorem 31, $I \cap [V, V] \supseteqq [V_J, V]$ for some nonzero *-ideal J of R, or $I \cap [V, V] \subset Z$. If $I \cap [V, V] \subset Z$, then since we may assume Z is a field and $I \cap [V, V] \neq 0$, we have contradicted I being a proper ideal. Thus we may assume that $I \cap [V, V] \supseteqq [V_J, V]$ for some J. But then by the same argument as in Corollary 32, $[V_J, V_J]'$ contains a nonzero ideal of R, and so also does $(I \cap [V, V])'$, and the lemma is proved.

COROLLARY 35. *If U is a Lie ideal of $[V, V]$, then $[U, U] \subset Z$ implies that $U \subset Z$.*

Proof. Follow exactly the proof of Lemma 30, using $[[V, V], [V, V]]$ instead of $[V, V]$ (by Corollary 32, we know that $[[V, V], [V, V]]'$ contains a nonzero ideal of R) to see that $u^2 \in Z$, all $u \in U$. Now apply Lemma 34.

To complete our description of the Lie ideals of $[V, V]$, we define a new set $T(U)$ as in [10, p. 400]: If U is a Lie ideal of $[V, V]$, define $T(U)$ by

$$T(U) = \{v \in V \mid [v, V] \subset U\} .$$

The following properties of $T = T(U)$ are easy to verify:

(1) $T \supseteqq [U, U]$

(2) $[T, [V, V]] \subseteqq T$

(3) $[[T, T], V] \subseteqq T$

(4) If $a \in T$, then $[a^2, V] = [a, [a, V]] \subset T$.

We establish another property of T:

LEMMA 36. *If $a \in T$ and $a^2 \notin Z$, then $T \supseteqq [a, V_J]$ for some nonzero *-ideal J of R.*

Proof. $W = \{v \in V \mid [a, v] \subset T\}$. We will show that $W \supset V_J$, for some J, by using Lemma 23. First observe that $W \supseteq [V, V]$ by property (2) above. Thus W is a Lie ideal of V, and by Theorem 21, V' contains a nonzero ideal of R. Since $a^2 \notin Z$, there exists $s \in V$ so $a^2s + sa^2 = c \neq 0$, since otherwise a^2 would centralize a nonzero ideal of R, and so would be in Z, a contradiction. Now

$$\begin{aligned} cx + x^*c &= (a^2s + sa^2)x + x^*(a^2s + sa^2) \\ &= [a^2, sx + x^*s] + [s, xa^2 + a^2x^*] + sa^2(x + x^*) + (x + x^*)a^2s\,. \end{aligned}$$

The first two terms are in $[V, V]$, and by Lemma 10 of [10] we have $[a, sa^2(x + x^*) + (x + x^*)a^2s] \in T$. Thus $[a, cx + x^*c] \in T$ for all $x \in R$, and so $cx + x^*c \in W$. Thus by Lemma 23, $W \supset V_J$, some J.

THEOREM 37. *If U is a Lie ideal of $[V, V]$, then either $U \subset Z$ or $U \supseteq [V_J, V]$ for some nonzero *-ideal J of R*

Proof. First assume that for some $a, b, \in T$, that $a^2b^2 + b^2a^2 \neq 0$. Now $[a, V_I] \subseteq T$ for some I by Lemma 36, and $[b^2, V] \subseteq [b, [b, V]] \subseteq T$ by properties (2) and (4) of T listed above. Thus by Lemma 10 of [10], $a[b^2V]a \subseteq T$, and so $a^2b^2v + vb^2a^2 = [a, ab^2v + vb^2a] + a[b^2, v]a \in T$ for all $v \in V_I$. Let $c = a^2b^2 + b^2a^2$, and say $x \in I$. Now

$$\begin{aligned} cx + x^*c &= (a^2b^2 + b^2a^2)x + x^*(a^2b^2 + b^2a^2) \\ &= a^2b^2(x + x^*) + (x + x^*)b^2a^2 + [a^2, b^2x^* + xb^2] \\ &\quad + [b^2, a^2x + x^*a^2] \in T \end{aligned}$$

since $x + x^* \in V_I$. Thus $cx + x^*c \in T$, all $x \in I$, and so $T \supset V_J$ for some ideal J, by Lemma 23. Since $[V, T] \subseteq U$, this means $[V_J, V] \subseteq U$.

We may thus assume that if $U \not\supseteq [V_J, V]$ for all ideals J of R, then $a^2b^2 + b^2a^2 = 0$, for all $a, b \in T$. Linearizing on a and b, we see that $[[T, T], [T, T]] = (0)$. But then $[T, T]$ is a commutative Lie ideal of $[V, V]$, and so $[T, T] \subset Z$ by Corollary 35. Since $T \supseteq [U, U]$, we have $[[U, U], [U, U]] \subset Z$. Applying Corollary 35 to $[U, U]$ and then to U, we obtain $U \subset Z$, the desired result.

We conclude with a theorem which describes the Lie ideals of S when the involution is of the second kind. This extends a theorem of Herstein on simple rings [6, p. 27].

THEOREM 38. *Let R be a prime ring of characteristic 2 with an involution of the second kind. If U is a Lie ideal of S, then either $U \subset Z$ or $U \supseteq [J \cap S, S]$, where J is an ideal of R, unless R is an order in a simple ring Q, with center C, such that $\dim_C Q \leqq 4$.*

Proof. Since * is of the second kind, choose $\alpha \in Z$ with $\alpha^* \neq \alpha$.

Then $\alpha^* + \alpha \neq 0$, since R has characteristic 2. Let $r \in R$. Then $(\alpha + \alpha^*)r = (\alpha r^* + \alpha^* r) + \alpha(r + r^*) \in S + \alpha S$; that is, $(\alpha + \alpha^*)R \subseteq S + \alpha S$. Similarly $(\alpha + \alpha^*)Z \subseteq Z_s + \alpha Z_s$, where $Z_s = Z \cap S$.

Let $W = U(\alpha + \alpha^*)Z$. Since $(\alpha + \alpha^*)R \subseteq S + \alpha S$, W is a Lie ideal of R. Thus by Theorem 13, either $W \subseteq Z$ or $W \supseteq [I, R]$ for some ideal I of R. If $W \subseteq Z$, then $U(\alpha + \alpha^*)Z \subseteq Z$, and so $U \subseteq Z$. Thus we may assume $W \supseteq [I, R]$.

We claim that $U \supseteq [[I, I], [I, I]] \cap S$.[1] We show first that $[U, W] \cap S \subseteq [U, UZ \cap S]$. Let $u \in U$ and $w = v(\alpha + \alpha^*)z \in W$, where $v \in U$, $z \in Z$. Now $(\alpha + \alpha^*)z = z_1 + \alpha z_2$, where $z_1, z_2 \in Z_s$ and so

$$\begin{aligned}[u, w] &= [u, v(\alpha + \alpha^*)(z_1 + \alpha z_2)] \\ &= [u, v](\alpha + \alpha^*)z_1 + \alpha[u, v](\alpha + \alpha^*)z_2 \in S + \alpha S .\end{aligned}$$

Thus if $[u, w] \in [U, W] \cap S$, we must have $z_2 = 0$, and so

$$[u, w] = [u, v](\alpha + \alpha^*)z_1 = [u, v(\alpha + \alpha^*)z_1] \in [U, UZ \cap S] .$$

Now

$$\begin{aligned}U \supseteq [U, S] \supseteq [U, UZ \cap S] \supseteq [U, W] \cap S \\ \supseteq [W, W] \cap S \supseteq [[I, I], [I, I]] \cap S .\end{aligned}$$

Now $[[I, I]], [I, I]]$ is a Lie ideal of R, and so either contains $[J, R]$ for some ideal J of R, or is contained in Z by Theorem 13. If the first possibility occurs, then $U \supseteq [J, R] \cap S \supseteq [J \cap S, S]$ and we are done. We may therefore assume that $[[I, I], [I, I]] \subset Z$. Then $[[[I, I], [I, I]], I] = (0)$; that is, I satisfies a polynomial identity of degree 5. Since I is an ideal in a prime ring, I itself is a prime ring, so we may apply the theorem of Posner used in Theorem 21 to see that I is an order in a simple ring Q, finite-dimensional over its center C. In addition, Q also satisfies an identity of degree 5, and thus by Kaplansky's theorem, $\dim_C Q \leq [5/2]^2 = 4$. Since R is also an order in the same Q, the theorem is proved.

REFERENCES

1. S. A. Amitsur, *Rings with involution*, Israel Math. **6** (1968), 99-106.
2. N. Bourbaki, *Algèbre Commutative, chapter* 2: *Localisation*, Actualités Sci. Indust., no. 1290, Hermann, Paris, 1961.
3. T. S. Erickson, *The Lie Structure in Prime Rings with Involution*, to appear.
4. I. N. Herstein, *Non-Commutative Rings*, Carus Monograph no. 15, The Math. Asso. of America, 1968.
5. ———, *On the Lie structure of an associative ring*, J. of Algebra **14** (1970), 561-571.
6. ———, *Topics in Ring Theory*, University of Chicago Press, Chicago, 1969.
7. C. Lanski, *The group of units of a simple ring I*, J. of Algebra **15** (1970), 554-569.

[1] The idea for this part of the proof comes from Theorem 1 of Erickson [3].

8. ———, *Subgroups and conjugates in Semi-Prime Rings*, Math. Annalen to appear.
9. W. S. Martindale III, *Rings with involution and polynomial identities*, J. of Algebra, **11** (1968), 186-194.
10. S. Montgomery, *Lie structure of simple rings of characteristic* 2, J. of Algebra, **15** (1970), 387-407.

Received June 1, 1971.

UNIVERSITY OF SOUTHERN CALIFORNIA

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics
Vol. 42, No. 1 January, 1972