LIE ALGEBRAS OF CHARACTERISTIC p

BY

IRVING KAPLANSKY[1]

1. **Introduction.** Recent publications have exhibited an amazingly large number of simple Lie algebras of characteristic p. At this writing one cannot envisage a structure theory encompassing them all; perhaps it is not even sensible to seek one.

Seligman [3] picked out a subclass corresponding almost exactly to the simple Lie algebras of characteristic 0. He postulated restrictedness and the possession of a nonsingular invariant form arising from a restricted representation. In this paper our main purpose is to weaken his hypotheses by omitting the assumption that the form arises from a representation. We find no new algebras for ranks one and two. On the other hand, it is known that new algebras of this kind do exist for rank three, and at that level the investigation will probably become more formidable.

For rank one we are able to prove more. Just on the assumption of a nonsingular invariant form we find only the usual three-dimensional algebra to be possible. Assuming simplicity and restrictedness permits in addition the survival of the Witt algebra. Still further information on algebras of rank one is provided by Theorems 1, 2 and 4.

Characteristics two and three are exceptions to nearly all the results. In those two cases we are sometimes able to prove more, sometimes less; for the reader's convenience, these theorems are assembled in an appendix. In addition, characteristic five is a (probably temporary) exception in Theorem 7.

TWO REMARKS ON STYLE. (a) Several proofs are broken up into a series of lemmas. To avoid endless repetition, these lemmas are stated in skeleton form, not intelligible beyond the immediate context. If, however, a lemma has an application occurring substantially later in the paper, its hypotheses are given in full.

(b) Binomial coefficients with subscript two abound in the paper. For the sake of typographical simplicity we adopt the unorthodox notation $n_2 = n(n-1)/2$. At one point we similarly write n_3 for $n(n-1)(n-2)/6$.

PART I. RANK ONE

2. **Basic definitions.** We shall always be dealing with a finite-dimensional Lie algebra L over an algebraically closed field of characteristic $p>0$. We use ordinary juxtaposition xy for the operation in L; brackets are reserved for

Received by the editors February 7, 1957.

(1) Work on this paper was supported in part by the Office of Scientific Research of the Air Force.

actual commutation in an associative algebra. We write R_x, rather than $\mathrm{Ad}(x)$, for the mapping $a \to ax$.

If H is a nilpotent subalgebra of L, there is a unique decomposition $L = \sum L_\alpha$ as a vector space sum; here each α is a scalar function on H called a *root*, and L_α consists of all x in L which are annihilated by some power of $R_h - \alpha(h)I$ for every h in H. We have $L_\alpha L_\beta \subset L_{\alpha+\beta}$ (in the sense that $L_\alpha L_\beta = 0$ if $\alpha+\beta$ is not a root). Thus L_0 is a subalgebra containing H, and we say that H is a *Cartan subalgebra* if $H = L_0$. An element u is said to be *regular* if the multiplicity of the characteristic root 0 in R_u is minimal; this minimal number is called the *rank* of L. If the above decomposition is performed with H the one-dimensional subalgebra spanned by a regular element, it turns out that L_0 is a Cartan subalgebra. Thus there always exists a Cartan subalgebra whose dimension is the rank of L. One must beware of the fact that for characteristic $p > 0$ the dimension of a Cartan subalgebra is not necessarily invariant; but of course the rank is a well defined invariant.

We shall consider restricted Lie algebras only when they are centerless. Thus we define a centerless Lie algebra L to be *restricted* if the pth power of every inner derivation is inner. Then for every x there exists a unique element y satisfying $R_y = (R_x)^p$; we write $y = x^p$.

Let L be a Lie algebra of rank one, and select any nonzero element u in a one-dimensional Cartan subalgebra. Then the root spaces L_α are simply indexed by the characteristic roots of R_u and are elements of the base field. By multiplying u by a suitable scalar we can convert any desired root α into 1.

Suppose L, in addition, is restricted (note that any Lie algebra of rank one is centerless). Then one easily sees that it is possible to choose u so that $u^p = u$. It then follows that the roots are all in the prime field (integers mod p) and that R_u acts as a scalar on each root space. Each of these facts makes for big simplifications.

The product of any element of L_α by an element of $L_{-\alpha}$ is a scalar multiple of u; this gives rise to an inner product between the spaces L_α and $L_{-\alpha}$. Of course this inner product is not necessarily nonsingular. Accordingly, we write M_α for the subspace of L_α annihilating $L_{-\alpha}$, and we have that the spaces L_α/M_α and $L_{-\alpha}/M_{-\alpha}$ are paired in nonsingular fashion. We shall write $n(\alpha)$ for their common dimension. We shall prove ultimately (for characterstic >3) that $n(\alpha) = 0$ or 1. In the next section we take a preliminary step.

3. **Proof that $n(\alpha)$ is at most 2.** As we noted above, we may harmlessly assume that $\alpha = 1$.

A *simple product* in a Lie algebra is one formed by successive multiplications by single elements. Write N_i for the subspace spanned by all simple products of i elements of L_1. Write W_i for the subspace spanned by all simple products of i elements of L_1, where at least one factor is in M_1 (the annihilator of L_{-1} within L_1). Thus we have $W_i \subset N_i \subset L_i$, $N_{i+1} = N_i L_1$, $W_{i+1} = N_i M_1 + W_i L_1$. Note that $W_1 = M_1$, $W_2 = M_1 L_1$. We also set $W_0 = 0$, $N_0 = L_0$ (= the set of scalar muliples of u).

LEMMA 1. *N_i is invariant under R_u.*

Proof. The lemma is clear for $i=1$, and we proceed by induction. By the Jacobi identity

$$N_{i+1}u = (N_iL_1)u \subset (N_iu)L_1 + N_i(L_1u) \subset N_iL_1 + N_iL_1 = N_{i+1}.$$

LEMMA 2. *W_i is invariant under R_u.*

Proof. We first check this for $i=1$. We have to prove that M_1u annihilates L_{-1}. By the Jacobi identity, $(M_1u)L_{-1}\subset(M_1L_{-1})u+M_1(L_{-1}u)=0$. Then by Lemma 1 and induction:

$$\begin{aligned} W_{i+1}\, u &= (N_iM_1 + W_iL_1)u \\ &\subset (N_iu)M_1 + N_i(M_1u) + (W_iu)L_1 + W_i(L_1u) \\ &\subset N_iM_1 + W_iL_1 = W_{i+1}. \end{aligned}$$

LEMMA 3. *$L_{-1}N_{i+1}\subset N_i$.*

Proof. This is true for $i=0$ since $N_1=L_1$, $N_0=L_0$. Then by induction and Lemma 1,

$$\begin{aligned} L_{-1}N_{i+1} &= L_{-1}(N_iL_1) \subset (L_{-1}N_i)L_1 + (L_{-1}L_1)N_i \\ &\subset N_{i-1}L_1 + uN_i = N_i. \end{aligned}$$

LEMMA 4. *$L_{-1}W_{i+1}\subset W_i$.*

Proof. This is true for $i=0$ since $W_1=M_1$, $W_0=0$. Then by induction and Lemmas 2 and 3:

$$\begin{aligned} L_{-1}W_{i+1} &= L_{-1}(N_iM_1 + W_iL_1) \\ &\subset (L_{-1}N_i)M_1 + (L_{-1}M_1)N_i + (L_{-1}W_i)L_1 + (L_{-1}L_1)W_i \\ &\subset N_{i-1}M_1 + 0 + W_{i-1}L_1 + uW_i \subset W_i. \end{aligned}$$

We insert at this point a lemma with several later applications.

LEMMA 5. *If a, b are linearly independent elements of L_1 with a not in M_1 then $ab\neq 0$.*

Proof. We can find $x\in L_{-1}$ with $ax=u$. We have $b\cdot ax+a\cdot xb+x\cdot ba=0$. Now xb is a scalar multiple of u. If $ab=0$ we find that bu is a scalar multiple of au. Since R_u is nonsingular on L_1, this is a contradiction.

Now let us assume that L_1/M_1 is at least two-dimensional. Since M_1 is invariant under R_u (Lemma 2) we may think of R_u as acting on L_1/M_1 and pick a two-dimensional invariant subspace. Lifting a suitable basis of this back to L_1 we arrive at elements a and b which satisfy

$$au \equiv a, \qquad bu \equiv b + \lambda a \qquad (\mathrm{mod}\ M_1) \tag{1}$$

where λ is a scalar (which we could take to be 0 or 1). Write $ab=c$.

LEMMA 6. $cu \equiv 2c \pmod{W_2}$.

Proof. By the Jacobi identity

$$ab\cdot u + bu\cdot a + ua\cdot b = 0. \tag{2}$$

If we make the replacements (1) in (2), and recall $W_2 = M_1L_1$, we arrive at the statement in the lemma.

Since a and b are linearly independent modulo M_1, we can find an element x in L_{-1} such that $ax = u$, $bx = 0$. Let y be any element in L_{-1} with $ay = 0$. Write $ay = \nu u$ (ν a scalar), and set $au = d$.

LEMMA 7. $cx = -bu$, $cy = \nu d$.

Proof. These statements follow directly from the Jacobi identity applied to the triples a, b, x and a, b, y respectively.

LEMMA 8. $dy = 0$.

Proof. This follows from $ay = 0$ and the fact that a and d differ by an element of M_1.

Define $c_0 = c$, $c_i = cR_d^i$, and note that c_i lies in N_{i+2} for $i \geqq 1$.

LEMMA 9. $c_iy = 0$ *for* $i \geqq 1$.

Proof. Apply the Jacobi identity to c, d, y, bearing Lemmas 7 and 8 in mind. The result is $cd\cdot y = 0$, which is the case $i = 1$ of the lemma. The general case then follows since R_d and R_y commute (Lemma 8).

LEMMA 10. $c_iu \equiv (i+2)c_i \pmod{W_{i+2}}$.

Proof. The case $i = 0$ is covered by Lemma 6. We proceed by induction.

$$c_id\cdot u + du\cdot c_i + uc_i\cdot d = 0. \tag{3}$$

Now $du \equiv d \pmod{M_1}$; this follows from the corresponding fact for a, the fact that d and a differ by an element of M_1, and the invariance of M_1 under R_u (Lemma 2). Hence $du\cdot c_i \equiv dc_i \equiv -c_{i+1} \pmod{W_{i+3}}$. Applying our inductive assumption to c_iu in (3) we arrive at $c_{i+1}u \equiv (i+3)c_{i+1} \pmod{W_{i+3}}$.

LEMMA 11. $c_1x \equiv 3c \pmod{W_2}$.

Proof. We write

$$cd\cdot x + dx\cdot c + xc\cdot d = 0. \tag{4}$$

Now $dx = u$ (since $ax = u$ and $a - d \in M_1$), while $cu \equiv 2c \pmod{W_2}$ by Lemma 6. Also $cx = -bu$ by Lemma 7, and $bu \equiv b + \lambda a \pmod{W_1}$. Inserting these changes in (4), we obtain $cd\cdot x = c_1x \equiv 3c \pmod{W_2}$.

LEMMA 12. $c_ix \equiv (i+2)_2c_{i-1} \pmod{W_{i+1}}$.

Proof. The case $i = 1$ is Lemma 11. Proceeding by induction and using

Lemma 10, we find

$$\begin{aligned} c_{i+1}x &= c_i d\cdot x = -dx\cdot c_i - xc_i d \\ &\equiv -uc_i + (i+2)_2 c_{i-1}d \pmod{W_{i+2}} \\ &\equiv (i+2)c_i + (i+2)_2 c_i \pmod{W_{i+2}} \\ &= (i+3)_2 c_i. \end{aligned}$$

LEMMA 13. *For $i \leqq p-3$, c_i is not in W_{i+2}.*

Proof. First, $c_0 = c$ is not in W_2. For $cx = -bu$ (Lemma 7), and thus by Lemma 4 we would have $bu \in W_1 = M_1$, a contradiction. We then apply Lemmas 4 and 12, noting that the binomial coefficient $(i+2)_2$ is not 0 till $i = p-2$.

As a particular case of Lemma 13 we have that c_{p-3} is not 0. (Here we must insist on characteristic at least 5. This assumption will be made henceforth tacitly in the lemmas, but it will be restated in the major theorems.) Now y was taken to be any element of L_{-1} annihilating a. Hence (Lemma 9) we have discovered a nonzero element c_{p-3} in L_{-1} which annihilates anything in L_{-1} which annihilates a. Suppose now that L_{-1}/M_{-1} has dimension $\geqq 3$. Then there are at least two elements of L_{-1} linearly independent modulo M_{-1} in the annihilator of a. Lemma 5 shows that c_{p-3} must be a scalar multiple of each of these. This being impossible, we have proved:

LEMMA 14. $n(\alpha) \leqq 2$.

4. **Preliminary results on the case $n(\alpha) = 2$.** We shall ultimately see that $n(\alpha) = 2$ is impossible. In this section we collect a number of cases where $n(\alpha) = 2$ turns out to be impossible. In §6 (with the aid of the results in §5) we shall complete the proof.

First we note that $n(2\alpha)$ cannot vanish if $n(\alpha) = 2$.

LEMMA 15. *If $n(\alpha) = 2$, then $n(2\alpha) \geqq 1$.*

Proof. We assume $\alpha = 1$. The spaces L_1/M_1 and L_{-1}/M_{-1} are two-dimensional and are paired by a nonsingular inner product. We pick a basis for L_1/M_1 in Jordan canonical form under R_u, and then choose a dual basis for L_{-1}/M_{-1}. After lifting these bases to L_1 and L_{-1} we obtain elements a, $b \in L_1$, x, $y \in L_{-1}$ satisfying $ax = by = u$, $ay = bx = 0$, $au \equiv a$, $bu \equiv b + \lambda a$ (mod M_1), $\lambda = 0$ or 1. The equations $cx = -bu$, $cy = au$ hold as in Lemma 7, where c is again ab. Then $c\cdot xy = -x\cdot yc - y\cdot cx = x\cdot au + y\cdot bu = xa + yb = -2u$. Thus $L_2L_{-2} \neq 0$ and $n(2) \geqq 1$.

We continue to assume $\alpha = 1$, $n(1) = 2$. Changing notation, we write $b_1, \cdots, b_r$ for a basis of M_1 and augment this basis by elements a_1, a_2 to a basis of L_1.

LEMMA 16. *The elements a_1a_2, a_1b_i, a_2b_j are linearly independent* $(1 \leqq i, j \leqq r)$. *The dimension of L_2 is at least $2r+1$. If* $\dim(L_2) \leqq \dim(L_1)$, *then $r = 0$ or 1.*

Proof. Assume

$$\lambda a_1a_2 + \sum \mu_i a_1 b_i + \sum \nu_j a_2 b_j = 0. \tag{5}$$

We can find x in L_{-1} with $a_1x=u$, $a_2x=0$. Of course $b_1x=\cdots b_rx=0$. By the Jacobi identity,

$$x\cdot a_1a_2 = a_2u, \qquad x\cdot a_1b_i = b_iu, \qquad x\cdot a_2b_j = 0. \tag{6}$$

Left-multiply (5) by x and apply (6). Since R_u is nonsingular on L_1, we obtain $\lambda=\mu_i=0$. Similarly $\nu_j=0$. The final statements of the lemma are evident.

LEMMA 17. $(L_{-1}M_{-1})L_1^2=0$.

Proof. Let $a\in L_{-1}$, $b\in M_{-1}$, c, $d\in L_1$. Then $b\cdot cd=0$ by the Jacobi identity on b, c, d. Also $b(a\cdot cd)=0$ since $a\cdot cd\in L_1$. An application of the Jacobi identity to a, b, and cd then shows that $ab\cdot cd=0$.

LEMMA 18. *The following is impossible*: $n(1)=n(2)=2$, *and* $L_{\pm 1}$, $L_{\pm 2}$ *three-dimensional.*

Proof. From Lemma 16 we see that L_2 is spanned by L_1^2. Again by Lemma 5, $L_{-1}M_{-1}$ is two-dimensional. This shows (by Lemma 17) that a two-dimensional subspace of L_{-2} annihilates all of L_2. This is incompatible with the hypotheses that $n(2)=2$ and the spaces L_2, L_{-2} are three-dimensional.

The next lemma will be used again in §5 and §11; we accordingly state it in full with adequate generality.

LEMMA 19. *Let L be a Lie algebra over an algebraically closed field of characteristic $p>3$. Let $\{L_\alpha\}$ denote the root spaces of L under the decomposition relative to R_u, where $u\in L$. Assume $b\in L_\alpha$, $y\in L_{-\alpha}$, $t\in L_{-2\alpha}$, $by=u$, $yu=-\alpha y$, $tu=-2\alpha t$, $t(bu-\alpha b)=0$, $ty=0$. Assume further that $tb\cdot b$ is a scalar multiple of u. Then $t=0$.*

Proof. We may assume $\alpha=1$. Write $tb=t_1$. We apply the Jacobi identity three times: the triple (t, b, y) yields $t_1y=-2t$; the triple (t, b, u) yields $t_1u=-t_1$; the triple (t_1, b, y) yields $t_1b\cdot y=-3t_1$. Now t_1b is a scalar multiple of u by hypothesis. Hence $t_1b\cdot y$ is a scalar multiple of y. It follows that $t_1y=0$ and $t=0$.

LEMMA 20. *The following is impossible*: $n(1)=2$, $L_{\pm 1}$ *two-dimensional, and* R_u *acting as the identity on* L_1.

Proof. L_1 and L_{-1} are two-dimensional spaces paired by a nonsingular inner product. From the Jacobi identity, applied to u, L_1 and L_{-1}, we see that R_u on L_{-1} is the negative of the adjoint of R_u on L_1. Thus $R_u=-I$ on L_{-1}. Choose dual bases: a, b for L_1 and x, y for L_{-1}. We now follow the notation and use the results in §3, defining $c=ab$, $c_i=cR_a^i$. It should be noted that in the present case $M_1=0$, so that the W's are all 0 and the congruences in §3 are replaced by equalities. Write $t=c_{p-4}$. By Lemma 9, $ty=0$. By Lemma 10, $tu=-2t$ (note that t lies in L_{-2}). All the hypotheses of Lemma 19 are fulfilled (with $\alpha=1$) and we conclude that $t=0$. But this contradicts Lemma 13.

LEMMA 21. *The following is impossible*: $n(1)=2$, dim $(L_{\pm 1})=2$, dim $(L_{\pm 2})=1$.

Proof. Since Lemma 20 rules out the possibility that R_u is the identity on L_1, we have a basis a, b for L_1 with $au=a$, $bu=b+a$. On the dual basis x, y for L_{-1}, we have $yu=-y$, $xu=-x-y$. Again we set $c=ab$, $c_i=cR_a^i$. Concerning the element c_{p-4} we again have that it is a nonzero element in L_{-2} and that it annihilates y. Now consider the element xy in L_{-2}. The fact that $ac=c_1$ is not zero (Lemma 13) is mirrored by the fact that xy does not annihilate y. Hence xy and c_{p-4} are linearly independent elements of L_{-2}, and L_{-2} is at least two-dimensional.

LEMMA 22. *The following is impossible*: $n(1)=n(2)=2$, $L_{\pm 1}$, $L_{\pm 2}$ *all two-dimensional.*

Proof. We continue the analysis occurring in Lemma 21, studying further the linearly independent elements c_{p-4} and xy in L_{-2}. We have $xy\cdot u=-2xy$; this is the analogue of the statement $cu=2c$ (Lemma 6). Further, $c_{p-4}u=-2c_{p-4}$ by Lemma 10. Since L_{-2} is assumed to be two-dimensional, it is spanned by xy and c_{p-4}; thus R_u acts as $-2I$ on L_{-2}. We can now invoke Lemma 20, with L_{-2} playing the role of L_1.

LEMMA 23. *The following is impossible*: $n(1)=n(2)=2$, L_1 *two-dimensional*, L_{-1} *and* L_{-2} *three-dimensional.*

Proof. Since $n(1)=2$ and L_{-1} is three-dimensional, M_{-1} is one-dimensional. Pick a nonzero element z in M_{-1}. Choose a basis a, b for L_1 as usual: $au=a$, $bu=b+\lambda a$. The annihilator of a in L_{-1} will be a two-dimensional subspace containing z which is invariant under R_u; thus it will have a basis y, z satisfying $zu=-z$, $yu=-y+\mu z$. Now we repeat the idea of the last two lemmas, constructing the nonzero element c_{p-4} in L_{-2}. This time $c_{p-4}y=c_{p-4}z=0$, for c_{p-4} annihilates the annihilator of a in L_{-1} (Lemma 9). It follows that $c_{p-4}s=0$, where $s=yz$. Now it is impossible for c_{p-4} and s to be linearly independent, for then by Lemma 5 they would both lie in M_{-2}, whereas M_{-2} is one-dimensional. Hence c_{p-4} is a scalar multiple of s, and it follows that $ys=0$. Let b be any element in L_1 with $by=u$. Since $bz=0$, the Jacobi identity on (b, y, z) yields $bs=z$. Applying the Jacobi identity to (b, y, s) we obtain $su=s$, which is impossible since $s\in L_{-2}$.

5. **Study of the case** $n(\alpha)=1$. In this section we begin to examine the case $n(\alpha)=1$. The results will be used in §6 to complete the proof that $n(\alpha)$ is at most one, and will again be used in §7 to get our structure theorems.

The preliminary lemmas have an application in §11, and so we formulate them so as to apply to general Lie algebras (not necessarily of rank one).

LEMMA 24. *Let a, x, u be elements in a Lie algebra L with $ax=u$. Let W be a subspace of L which contains $au-a$, is invariant under R_u, and is annihilated by R_x. Let T be a product (in any order) of R_a's, R_x's, R_u's and right multiplications by elements of W. Suppose r of the factors are R_a's and s are R_x's.*

(a) *If $s>r$, $WT=0$.*

(b) *If $s\leqq r$, assume in addition that $(WR_a^k)W=0$ for $0\leqq k\leqq r-s$, and that at least one right-multiplication by an element of W is actually present in T. Then again $WT=0$.*

Proof. We shall prove this by a steady process of pushing terms R_u, R_x to the left. Take the first factor in T which is R_u or R_x.

CASE I. It is R_u. If T leads off with R_u, we can simply suppress R_u, for $WR_u\subset W$ by hypothesis. Otherwise there is a factor preceding R_u, and it is either R_a or of the form R_d with d in W. Now

$$R_aR_u = R_uR_a + R_a + R_c \qquad (c\in W). \tag{7}$$

With each of the three terms on the right of (7), we have accomplished the desired progress of either eliminating R_u or pushing it to the left. Again, $R_dR_u=R_uR_d+R_e$, $e\in W$, and the procedure is successful here too.

CASE II. It is R_x. If T leads off with R_x, we have $WT=0$. Otherwise we have R_a or R_d preceding R_x $(d\in W)$. Now R_d simply commutes with R_x, and for R_aR_x we have the equation

$$R_aR_x = R_xR_a + R_u. \tag{8}$$

In the case of the first term on the right of (8) we have pushed R_x to the left. In the case of the second term we have eliminated one R_x and one R_a, thereby maintaining the difference between the number of R_a's and the number of R_x's.

In case (a), we shall in this way eliminate all R_a's. At least one R_x will always survive, and when it arrives at the extreme left, we get 0.

In case (b), all R_x's and all R_u's get eliminated. What we have left is something of the form $R_a^kR_e\cdots$, where $e\in W$ and $0\leqq k\leqq r-s$. (Note that the presence of at least one right-multiplication by an element of W is preserved throughout the reduction process.) By hypothesis $WR_a^kR_e=0$. This concludes the proof of Lemma 24.

LEMMA 25. *Let a, x, u be elements in a Lie algebra L with $ax=u$. Let W be a subspace of L which contains $au-a$, is invariant under R_u, and is annihilated by R_x. Let an element b in W, and integers i, m, n $(0\leqq i,\ m\leqq n)$ be given.* (a) *If $m=n$, there is no further assumption.* (b) *If $m<n$, assume $(WR_a^k)W=0$ for $0\leqq k\leqq n-m-1$. Then*

$$bR_a^iR_uR_a^{n-i}R_x^m = b(R_u + iI)R_a^nR_x^m. \tag{9}$$

where I is the identity linear transformation.

Proof. We make an induction on i. For $i=0$, the equation is an identity. Assume (9) known for $i-1$ and apply (7). The term involving R_c vanishes by Lemma 24; corresponding to the two cases of the present lemma we cite part (a) or (b) of Lemma 24. Hence

$$\begin{aligned} bR_a^iR_uR_a^{n-i}R_x^m &= bR_a^{i-1}(R_uR_a + R_a)R_a^{n-i}R_x^m \\ &= b[R_u + (i-1)I]R_a^nR_x^m + bR_a^nR_x^m \end{aligned}$$

be the inductive assumption. This proves the lemma.

LEMMA 26. *Let a, x, u be elements in a Lie algebra L with $ax=u$. Let W be a subspace of L which contains $au-a$, is invariant under R_u, and is annihilated by R_x. Let integers m, n $(0<m\leqq n)$ be given.* (a) *If $m=n$, there is no further assumption.* (b) *If $m<n$, assume $(WR_a^k)W=0$ for $0\leqq k\leqq n-m-1$. Then for any b in W,*

$$bR_a^nR_x^m = bT_{n-m+1}\cdots T_{n-1}T_nR_a^{n-m}, \tag{10}$$

where $T_i = iR_u + i_2I$.

Proof. First we prove, for any i $(0\leqq i\leqq n)$,

$$bR_a^iR_xR_a^{n-i}R_x^{m-1} = bT_iR_a^{n-1}R_x^{m-1}. \tag{11}$$

For $i=0$, both sides of (11) vanish. Apply (8) on the left side of (11) to the first occurrence of R_aR_x, and then use induction and Lemma 25. The result is

$$bR_a^iR_xR_a^{n-i}R_x^{m-1} = b[T_{i-1} + R_u + (i-1)I]R_a^{n-1}R_x^{m-1},$$

which proves (11).

The special case $i=n$ of (11) reads

$$bR_a^nR_x^m = bT_nR_a^{n-1}R_x^{m-1} \tag{12}$$

By repeated use of (12) we obtain (10).

We now return specifically to the study of a Lie algebra L of rank one. We shall assume in the remainder of this section that $n(1)=1$. Select an element a in L_1 but not in M_1, and an element x in L_{-1} but not in M_{-1}; normalize so that $ax=u$. Since M_1 has co-dimension one in L_1 we have that $au-a\in M_1$. Also, we recall (Lemma 2) that M_1 is invariant under R_u. Thus, with $W=M_1$, all the hypotheses of Lemmas 24–26, part (a), are fulfilled.

LEMMA 27. $M_1R_a^{p-2}\subset M_{-1}$.

Proof. Let z be any element in M_{-1}. We have $az=0$, $M_1z=0$. Hence $M_1R_a^{p-2}$ is annihilated by z. But $M_1R_a^{p-2}\subset L_{-1}$, and it follows from Lemma 5 that the annihilator of M_{-1} within L_{-1} is contained in M_{-1}. Hence $M_1R_a^{p-2}\subset M_{-1}$.

For $j=1, \cdots, p-1$ set $S_j=M_1R_a^{j-1}$; thus $S_1=M_1$ and $S_j\subset L_j$. Write $S=S_1+\cdots+S_{p-1}$. Note that by Lemma 27, $S_{p-1}a=0$, whence S is invariant under R_a.

LEMMA 28. $S_1S_j=0$.

Proof. We prove this by induction on j; the argument will simultaneously establish the initial stage $j=1$ of the induction.

Set $n=p-2$, $m=n-j+1$. If $j=1$, we have $m=n$, and Lemma 26 (a) is applicable. If $j>1$, we note that $n-m-1=j-2$. Our inductive assumption tells us then that $(WR_a^k)W=0$ for $W=S_1$ and $0\leqq k\leqq n-m-1$. Thus Lemma 26 (b) is applicable. The linear transformations $T_{n-m+1}, \cdots, T_n$ occurring on the right of (10) are easily seen to be nonsingular on L_1 and they map S_1 onto itself (since S_1 is invariant under R_u). We conclude that $R_a^nR_x^m$ induces a one-to-one linear transformation from S_1 onto $S_1R_a^{n-m}=S_j$. Now S_1 annihilates $S_1R_a^n$ (Lemma 27). Since $S_1x=0$, the annihilator of S_1 is stable under R_x. Hence $S_1S_j=S_1(S_1R_a^nR_x^m)=0$.

We record for later use the following facts (consequences of our observation that $R_a^nR_x^m$ induces a one-to-one linear transformation from S_1 onto S_j):

LEMMA 29. *The spaces $S_1, \cdots, S_{p-1}$ all have the same dimension. For $1\leqq i\leqq p-2$, R_a induces a one-to-one linear transformation from S_i onto S_{i+1}. For $2\leqq i\leqq p-1$, R_x induces a one-to-one linear transformation from S_i onto S_{i-1}.*

LEMMA 30. $S^2=0$.

Proof. We prove $S_iS=0$ by induction, noting that Lemma 28 is the case $i=1$. We have $S_iS=(S_{i-1}a)S\subset(S_{i-1}S)a+S_{i-1}(aS)=0$, since $aS\subset S$.

LEMMA 31. *R_u acts as a scalar on each S_i.*

Proof. We prove this first for $i=1$. Let b be an element in S_1. By Lemma 27 we have $bR_a^{p-1}=0$. Apply Lemma 26 (a) with $m=n=p-1$. The linear transformations $T_1, \cdots, T_{p-1}$ which occur on the right of (10) are all nonsingular except the last, which is R_u-I. Hence $b(R_u-I)=0$.

Assume the lemma known for $i-1$. Then for $t\in S_{i-1}$ we have $ta\cdot u=tu\cdot a+t\cdot au$. Now $tu=(i-1)t$ by induction; $au=a+c$ $(c\in S_1)$ and $tc=0$ by Lemma 28. Hence $ta\cdot u=i\cdot ta$.

LEMMA 32. *Suppose that the dimension of L_i is at most equal to the dimension of L_1. Then $S_{-i}L_i=0$.*

Proof. Assume on the contrary that there exist elements $y\in S_{-i}$, $b\in L_i$

with $by=u$. Now S_i is a subspace of L_i with the same dimension as S_1 (Lemma 29). Since S_1 is just one dimension short of L_1, it follows from our hypothesis that the codimension of S_i in L_i is 0 or 1. In either event we have $bu-ib\in S_i$, since S_i is invariant under R_u. Take any nonzero element t in S_{-2i}. Then ty and $t(bu-ib)$ are both zero by Lemma 30. Also, $tu=-2it$, $yu=-y$ by Lemma 31. We have a contradiction of Lemma 19 (the notation is exactly that of Lemma 19, except that α is to be replaced by i).

6. **Proof that $n(\alpha)$ is at most one.** In this section we shall complete the proof that $n(\alpha)$ can never exceed one. We suppose that $n(\alpha)=2$ for some α and eventually reach a contradiction. Among all root spaces L_α with $n(\alpha)=2$ we may assume that L_1 has maximal dimension, and we write $r+2$ for that dimension. By Lemma 15, $n(2)=1$ or 2. We distinguish the two cases.

I. $n(2)=1$. By Lemma 16, the dimension of L_2 is at least $2r+1$. Thus M_2 (the annihilator of L_{-2} within L_2) has a dimension (say s) which is at least $2r$. The dimension of L_2 is $s+1$. We are now going to apply the theory of §5, with L_2 playing the role of the L_1 of that section. The sequence of S_i's there constructed arises anew here, but it starts from $S_2=M_2$, and we are principally concerned with the subspace of L_1 which emerges; the appropriate notation for it is S_1, but it is not to be confused with M_1 (the annihilator of L_{-1} within L_1). Suppose that the dimension of L_1 is at most equal to that of L_2 (i.e., $r+2\leqq s+1$). Then Lemma 32 applies to tell us that $S_1L_{-1}=0$, $S_1\subset M_1$. But S_1 is s-dimensional (Lemma 29) and M_1 is r-dimensional. Hence $s\leqq r$, a contradiction. Therefore the dimension of L_1 is strictly larger than that of L_2, that is, $r+1>s$. In conjunction with the inequality $s\geqq 2r$, this implies $r=s=0$. Thus L_1 is two-dimensional, L_2 is one-dimensional. By our maximality assumption, L_{-1} is also two-dimensional. By symmetry (we are now able to replace L_1 by L_{-1}), L_{-2} is one-dimensional. But Lemma 21 asserts that this combination is impossible.

II. The demolition of Case I shows us that whenever $n(\alpha)$ is 2, then $n(2\alpha)$ is also 2. Moreover the dimension of $L_{2\alpha}$ is at least that of L_α; this is now clear if L_α is two-dimensional, and otherwise it follows from Lemma 16. But in fact the two dimensions are equal. For the chain of spaces L_α, $L_{2\alpha}$, $L_{4\alpha}$, $\cdots$ closes back to L_α, and so we must have equality at every step. Referring to Lemma 16 again, we see that the dimension of $L_{2\alpha}$ must be 2 or 3. Take L_1 to have $n(1)=2$ with (as above) maximal dimension among all L_α with $n(\alpha)=2$. Then there are three possibilities: (a) dim $(L_1)=$dim $(L_{-1})=2$, (b) dim $(L_1)=3$, dim $(L_{-1})\doteq 2$, (c) dim $(L_1)=$dim $(L_{-1})=3$. In every case, L_2 has the same dimension as L_1, L_{-2} the same as L_{-1}. We have prepared three lemmas exploding these three cases: Lemmas 22, 23, and 18, respectively.

We have completed the proof of our first major theorem.

THEOREM 1. *Let L be a Lie algebra of rank one over an algebraically closed field of characteristic >3. Let L_α, L_β, $\cdots$ be the root spaces relative to a one-*

dimensional Cartan subalgebra. Let M_α be the annihilator of $L_{-\alpha}$ within L_α. Then: L_α/M_α is either zero or one-dimensional.

7. **Simple algebras with integral roots.** In this section we shall determine the structure of a substantial class of simple Lie algebras of rank one.

THEOREM 2. *Let L be a simple Lie algebra of rank one over an algebraically closed field of characteristic $p>3$. Suppose that L contains a regular element u such that the characteristic roots of R_u are in the prime field $GF(p)$. Then L is either three-dimensional or isomorphic to the Witt algebra.*

The proof will be given after several preliminary lemmas.

Among the root spaces L_i ($i=1, \cdots, p-1$) for which $L_iL_{-i}\neq 0$ choose notation so that L_1 has maximal dimension. We adopt the notation and use the results of §5.

LEMMA 33. *$S_{-i}L_i=0$ for all i.*

Proof. If $L_iL_{-i}=0$ there is nothing to prove. Otherwise, by our normalization to make L_1 have maximal dimension, the dimension of L_i is at most that of L_1. Lemma 33 then follows from Lemma 32.

LEMMA 34. *S is an ideal in L.*

Proof. By induction we prove simultaneously the following two statements

$$S_iL_j \subset S \text{ for } \quad i+j \equiv t \pmod{p}, \tag{13}$$

$$L_tS \subset S. \tag{14}$$

By symmetry it suffices to cover the range $t=0, 1, \cdots, (p-1)/2$. For $t=0$, (13) follows from Lemma 33, and (14) follows from Lemma 31. Suppose the two assertions are known for $t-1$. We proceed to prove (13) for the value t. The range $0\leqq j\leqq t-1$ is already covered by our inductive assumption on (14). The case $j=t$ is vacuous, since $S_0=0$. The remaining range on j is from $t+1$ to $p-1$; on i the range is also from $t+1$ to $p-1$. We make an induction on i, noting that the induction can begin at $i=t$. Since $S_i=S_{i-1}a$ we have

$$S_iL_j \subset a\cdot S_{i-1}L_j + S_{i-1}\cdot aL_j. \tag{15}$$

The first term on the right of (15) lies in S by our inductive assumption on t in (13); the second lies in S by our inductive assumption on i.

It remains to prove (14). That is, we must prove $L_tS_k\subset S$ for any k. The range $p-t\leqq k\leqq p-1$ is covered by our induction on (13). This leaves the range $1\leqq k\leqq p-t-1$ to be covered. We make a descending induction on k, the induction beginning at $k=p-t$. Since $S_k=S_{k+1}x$ (Lemma 29), we have

$$L_tS_k \subset L_tS_{k+1}\cdot x + L_tx\cdot S_{k+1}. \tag{16}$$

The first term on the right of (16) lies in S by our inductive assumption on k; the second lies in S by our inductive assumption on t in (14). This completes the proof of Lemma 34.

If L is simple, S must be 0 (since, of course, $S \neq L$). We continue our analysis, assuming $S=0$. Thus L_1 and L_{-1} are one-dimensional; we maintain our standard notation: $a \in L_1$, $x \in L_{-1}$, $ax=u$.

The next steps in the discussion are based on a computation like that occurring in §5. In the present context the work is much easier, simply because there is no term R_c in (7). Since Lemmas 35–37 will be used again later we state them with adequate generality.

LEMMA 35. *Let a, x, u, b be elements in a Lie algebra satisfying $ax=u$, $au=a$, $bx \cdot a=0$. Then for any n*

$$bR_a^n R_x = bT_n R_a^{n-1}, \tag{17}$$

where $T_n = nR_u + n_2 I$.

Proof. From $[R_a R_u] = R_a$ we first establish inductively:

$$R_a^n R_u = (R_u + nI)R_a^n. \tag{18}$$

Then we prove (17) by use of induction, (18), and (8).

LEMMA 36. *Let L be a Lie algebra over an algebraically closed field of characteristic $p>3$. Let a, x, u be elements of L satisfying $ax=u$, $au=a$, $xu=-x$. Let $\{L_\alpha\}$ denote the root spaces of L under the decomposition induced by R_u (note that u is not assumed to be a regular element). Assume that $L_0 R_a^2 R_x$ and $L_0 R_x^2 R_a$ are 0. Then:* (a) *$R_a R_x$ induces a one-to-one map of L_j onto itself for $2 \leqq j \leqq (p-1)/2$;* (b) *$R_x R_a$ induces a one-to-one map of L_j onto itself for $(p+1)/2 \leqq j \leqq p-2$.*

Proof. By symmetry it is sufficient to prove (b). Suppose $bR_x R_a = 0$' $b \in L_j, (p+1)/2 \leqq j \leqq p-2$. Write $m=p-j+2$. Then $bR_a^{m-2} \in L_0$, so that $bR_a^m R_x = 0$. We note that $T_n = nR_u + n_2 I$ is nonsingular on L_j for $1 \leqq n \leqq m$. By repeated application of Lemma 35 we arrive at $b=0$.

The next lemma is an immediate consequence of Lemma 36.

LEMMA 37. *The hypotheses are the same as in Lemma 36. Then: for $2 \leqq j \leqq (p-1)/2$, R_a maps L_j one-to-one into L_{j+1}, and R_x maps L_{j+1} onto L_j. For $(p+1)/2 \leqq j \leqq p-2$, R_a maps L_{j-1} onto L_j and R_x maps L_j one-to-one into L_{j-1}.*

We return to the context of simple Lie algebras of rank one. It is to be noted that the hypothesis $L_0 R_a^2 R_x = 0$ of Lemmas 36 and 37 is fulfilled; indeed $uR_a^2 = 0$.

LEMMA 38. *For $2 \leqq j \leqq (p-1)/2$, L_j is the direct sum of $L_{j-1}R_a$ and the null space of $R_x R_a$ in L_j.*

Proof. For $j=2$ this is clear since R_xR_a annihilates L_2 ($L_2R_x \subset L_1$, and L_1 is the one-dimensional space spanned by a). Assume $j>2$. For $c \in L_j$, write $d=cx$. Since R_aR_x is one-to-one on L_{j-1} (Lemma 36), we may write $d=d_1R_aR_x$, $d_1 \in L_{j-1}$. Then $c=(c-d_1a)+d_1a$ splits c into a term annihilated by R_x and one in $L_{j-1}R_a$. To see that the sum is direct, assume $cx=0$, $c=ea$, $e\in L_{j-1}$. Then $ea\cdot x=0$, whence $e=0$, since R_aR_x is one-to-one on L_j.

LEMMA 39. *For $2 \leqq j \leqq (p-1)/2$, R_a^{p-2j} induces a one-to-one map of L_j onto L_{p-j}, and R_x^{p-2j} induces a one-to-one map of L_{p-j} onto L_j.*

Proof. It will suffice to prove that $R_a^{p-2j}R_x^{p-2j}$ is one-to-one on L_j. Write N_i for the null space of R_xR_a in L_i. (Note that $N_2=L_2$, and that for $3\leqq i \leqq (p-1)/2$, N_i is by Lemma 37 simply the null space of R_x in L_i). By iterated use of Lemma 38, we have that L_j is the direct sum of $N_j, N_{j-1}R_a, \cdots, N_2R_a^{j-2}$. It will suffice to prove that $R_a^{p-2j}R_x^{p-2j}$ maps each $N_iR_a^{j-i}$ one-to-one onto itself ($2\leqq i\leqq j$). Now by iterated use of Lemma 35 we find, for b in N_i,

$$bR_a^{j-i}R_a^{p-2j}R_x^{p-2j} = bT_{j-i+1}T_{j-i+2}\cdots T_{p-j-i}R_a^{j-i}.$$

For n in the range from $j-i+1$ to $p-j-i$ we verify that $T_n=nR_u+n_2I$ is nonsingular on L_i. Also: N_i is invariant under R_u (and hence invariant under each T_n); for $i=2$ this is vacuous, while for $i>2$ it follows from $[R_xR_u]=-R_x$ and the fact that N_i is merely the null space of R_x. Hence $R_a^{p-2j}R_x^{p-2j}$ induces a one-to-one mapping of $N_iR_a^{j-i}$ onto itself.

LEMMA 40. *Suppose $L_rL_s=0$, where $r=(p-1)/2$, $s=(p+1)/2$. Then:* (a) *$L_iL_j=0$ for $2\leqq i, j\leqq p-2$, $i+j\equiv 1$, 0 or -1* (mod p). (b) *Either xL_2 or aL_{-2} is* 0. (c) *If xL_2 and aL_{-2} are both* 0, *then $L_2+L_3+\cdots+L_{p-2}$ is an ideal in L.*

Proof. (a). By symmetry we can confine ourselves to the cases $i+j\equiv 1$ or 0 (mod p). We can, moreover, confine j to the range $s, \cdots, p-2$, and then i will be either $p-j$ or $p+1-j$. We make an ascending induction on j. To start the induction at $j=s$, we have to check $L_rL_s=L_sL_s=0$. The first of these is zero by hypothesis. To prove $L_sL_s=0$, it is sufficient to show that it annihilates x. Since $L_sx\subset L_r$, this follows from the Jacobi identity.

Suppose now that $L_iL_j=0$ is known for a certain j, where i is either $p-j$ or $p+1-j$. We proceed to $j+1$. We are supposing of course that $j+1$ is at most $p-2$. Hence Lemma 37 is applicable and tells us that L_{j+1} is equal to L_ja. Then

$$(19) \qquad L_iL_{j+1} \subset a\cdot L_iL_j + aL_i\cdot L_j \subset a\cdot L_iL_j + L_{i+1}L_j.$$

Take $i=(p+1)-(j+1)=p-j$. Then the right side of (19) vanishes by our induction on j. The other value of i we have to treat is $i=p-(j+1)$. Since $j+1\leqq p-2$, we have $i\geqq 2$. Hence $L_i=L_{i+1}x$ by Lemma 37. Then

$$L_iL_{j+1} \subset x\cdot L_{i+1}L_{j+1} + L_{i+1}L_j. \tag{20}$$

The first term on the right of (20) vanishes by the case we have just treated. The second vanishes by our induction on j.

(b) Suppose for instance that $L_{-2}a$ is not zero (and hence equal to L_{-1}). We prove that L_2x vanishes by pushing the first half of the argument of part (a) one step further. In detail:

$$L_2L_{-1} = L_2\cdot L_{-2}a \subset a\cdot L_2L_{-2} + L_3L_{-2},$$

which vanishes by part (a).

(c) If $L_2x = L_{-2}a = 0$, then $L_2 + \cdots + L_{p-2}$ admits multiplication by L_1 and L_{-1} (as well as by L_0 of course). By part (a), $L_2 + \cdots + L_{p-2}$ is a subalgebra. Hence it is an ideal.

We are ready to proceed to the proof of Theorem 2 itself. By Lemma 37, the spaces $L_2, \cdots, L_r$ $(r=(p-1)/2)$ have dimensions which increase, in the weak sense. The same is true for the sequence of spaces $L_{p-2}, \cdots, L_s$ $(s=(p+1)/2)$. The spaces L_r and L_s have the same dimension. If that common dimension is 0 or 1, then all L_i have dimension 0 or 1. In this case Zassenhaus [4, pp. 37–47] has proved that L is either 3-dimensional or the Witt algebra. We therefore assume henceforth that L_r and L_s have dimension greater than one and shall eventually reach a contradiction. We have that $L_rL_s = 0$, for otherwise Lemma 34 shows that L has a nontrivial ideal. (Alternatively, we could cite again our initial normalization of L_1 to have maximal dimension among all spaces L_i with $L_iL_{-i} \neq 0$). We apply parts (b) and (c) of Lemma 40. For definiteness let us assume $L_2x \neq 0$, $L_{-2}a = 0$. Select $d \in L_2$ with $dx = a$.

Write $Z_i = T_1 + \cdots + T_i$, where, as always, $T_n = nR_u + n_2I$. One computes that $Z_i = (i+1)_2R_u + (i+1)_3I$. We next prove that for any element b with $bx = 0$, and any j,

$$bR_a^jR_dR_x^{j+2} = bZ_{j+1}T_1 \cdots T_j. \tag{21}$$

For $j=0$, (21) is verified by applying $[R_dR_x] = R_a$ and (17) with $n=1$. We assume (21) known for $j-1$. Then

$$\begin{aligned} bR_a^jR_dR_x^{j+2} &= bR_a^j(R_xR_d + R_a)R_x^{j+1} \\ &= bT_jR_a^{j-1}R_dR_x^{j+1} + bR_a^{j+1}R_x^{j+1} \\ &= bT_jZ_jT_1 \cdots T_{j-1} + bT_1T_2 \cdots T_{j+1} \\ &= bZ_{j+1}T_1 \cdots T_j. \end{aligned}$$

(In this computation we used $bT_jR_x = 0$, which follows from $bx = 0$ and $[R_xR_u] = -R_x$.)

In the sequence of spaces $L_1, L_2, \cdots, L_r$ the first is one-dimensional and the last has dimension greater than one. R_x maps each into its predecessor.

Hence for some k with $2 \leqq k \leqq r = (p-1)/2$ there exists a nonzero element b in L_k with $bx = 0$. Apply (21) with $j = p-2k-1$. It is readily computed that $T_1, \cdots, T_j, Z_{j+1}$ are all nonsingular on L_k, and thus the right side of (21) is nonzero. We now distinguish two cases.

I. $k=2$. Then $bR_a^jR_d$ lies in L_{p-1} and is annihilated by R_x, a contradiction.

II. $k>2$. Write $c = bR_a^jR_d$. We note that the right side of (21) is annihilated by R_x, for the null space of R_x is invariant under R_u and hence under all the T's and Z's. Hence $cR_x^{j+3} = 0$. Now c lies in L_{p-k+1} and we have $s \leqq p-k+1 \leqq p-2$. Also, $j+3 = p-2k+2$. But by Lemma 39, R_x^{p-2k+2} is one-to-one on L_{p-k+1}. Hence $c=0$, a contradiction of the fact that the right side of (21) is nonzero. This completes the proof of Theorem 2.

8. **Restricted algebras.** If L is a restricted simple Lie algebra of rank one, the hypotheses of Theorem 2 are fulfilled, as we noted in §2. Hence:

THEOREM 3. *Let L be a restricted simple Lie algebra of rank one over an algebraically closed field of characteristic $p>3$. Then L is either three-dimensional or isomorphic to the Witt algebra.*

For the reader who wishes to reach this theorem rapidly, we remark that large portions of the preceding material can be by-passed. The crucial parts are: Lemma 19, Lemma 20, the latter half of §5, and §7.

9. **Algebras with an invariant form.** An invariant form on a Lie algebra L is a symmetric bilinear form f satisfying $f(ab, c) = f(a, bc)$ for all a, b, c in L. It is nonsingular if no nonzero element of L is orthogonal to all of L. It then follows that any Cartan subalgebra H is also nonsingular relative to f, and that $L_\alpha, L_{-\alpha}$ are nonsingular dual spaces under f (see [3, p. 8]). From this we can further deduce that no nonzero element x of L_α can annihilate all of $L_{-\alpha}$; $xL_{-\alpha} = 0$ implies $f(xL_{-\alpha}, H) = 0$, $f(x, L_{-\alpha}H) = 0$, $x = 0$, since $L_{-\alpha}H = L_{-\alpha}$.

Let us analyze the algebras of rank one possessing this last property.

THEOREM 4. *Let L be a Lie algebra of rank one over an algebraically closed field of characteristic $p>3$. Assume that no nonzero element of a root space L_α annihilates all of $L_{-\alpha}$. Then: all root spaces are one-dimensional. If L is not three-dimensional, the roots form a group under addition.*

Proof. That the root spaces are all one-dimensional follows at once from Theorem 1.

Suppose that L is not three-dimensional. Let α and β be roots; we must show that $\beta-\alpha$ is a root. We do this first on the assumption that β is not an integral multiple of α. Normalize so that $\alpha=1$. Pick nonzero elements a in L_1, x in L_{-1}, b in L_α, normalized so that $ax = u$. If $\alpha - 1$ is not a root, $bx = 0$. Lemma 35 is applicable and shows in particular that bR^{p-1} is not 0. But then $\alpha-1$ is a root after all.

What remains to be shown is this: if L is not three dimensional and 1 is a root, then i is a root for every i in $GF(p)$. Let M denote the subalgebra $\sum L_i$,

$i \in GF(p)$. M is easily seen to be simple, and if it is not three-dimensional, it is the Witt algebra by Theorem 2. In particular, every i in $GF(p)$ is a root. We shall prove that M is not three dimensional. If it is, there is some root α not in $GF(p)$. By the result proved in the preceding paragraph, $\alpha-1$ and $\alpha+1$ are roots. Moreover, since $\alpha+1$ is not an integral multiple of $\alpha-1$, $(\alpha+1)-(\alpha-1)=2$ is a root. This contradiction completes the proof of Theorem 4.

THEOREM 5. *Let L be a Lie algebra of rank one over an algebraically closed field of characteristic $p>3$. Assume that L possesses a nonsingular invariant form f. Then L is three-dimensional.*

Proof. We continue where Theorem 4 leaves off. Assume that L is not three-dimensional and normalize so that 1 is a root. Pick a, b nonzero elements in L_1, $L_{(p-1)/2}$ respectively. We have $f(ab, b)=f(a, bb)=0$. Since f is nonsingular between $L_{(p-1)/2}$ and $L_{(p+1)/2}$ this implies $ab=0$, contradicting Lemma 37 (what we have just shown is merely that, for $p>3$, the Witt algebra does not admit a nonsingular invariant form).

PART II. RANK TWO

10. **The diagonable case.** In Part II we shall be dealing mainly with a Lie algebra L over an algebraically closed field of characteristic $p>3$, which is centerless, restricted, and possesses a nonsingular invariant form. If H is a Cartan subalgebra of L, it is easily seen that $h \in H$ implies $h^p \in H$. If H is two-dimensional it follows from the results in [1] that there is a basis u, v for H with $u^p=u$, $v^p=v$ or 0. We study the two cases separately.

If $u^p=u$, $v^p=v$ then H acts diagonally on L. More generally, assume that L is any Lie algebra with a nonsingular invariant form f and a Cartan subalgebra H that acts diagonally. For any root α there is a unique element $h_\alpha \in H$ such that $\alpha(h)=f(h, h_\alpha)$ for every $h \in H$. We call α *nonisotropic* if $f(h_\alpha, h_\alpha) \neq 0$.

THEOREM 6. *Let L be a centerless Lie algebra over an algebraically closed field of characteristic $p>3$. Assume that L possesses a nonsingular invariant form f and a Cartan subalgebra that acts diagonally. Then: all roots in L are nonisotropic.*

Proof. We assume that α is an isotropic root and eventually reach a contradiction. Call a root β orthogonal to α if $f(h_\alpha, h_\beta)=0$.

(a) If β is not orthogonal to α, then $\beta-\alpha$ is a root.

Pick $a \in L_\alpha$, $x \in L_{-\alpha}$ with $f(a, x)=-1$. Then $ax=h_\alpha$ [3, Corollary 3.2]. Since α is isotropic, $ah_\alpha=xh_\alpha=0$. Take $b \neq 0$ in L_β. Assume that $\beta-\alpha$ is not a root; then $bx=0$. We now prove

$$bR_a^i R_x = i\beta(h_\alpha) bR_a^{i-1}. \tag{22}$$

For $i=0$, both sides vanish. Assume (22) known for $i-1$. Then

$$\begin{aligned} bR_a^i R_x &= bR_a^{i-1}(R_x R_a + R_{h_\alpha}) \\ &= (i-1)\beta(h_\alpha)bR_a^i + bR_{h_\alpha}R_a^{i-1} \end{aligned}$$

since R_a and R_{h_α} commute. Since $b\in L_\beta$ and A acts diagonally, $bh_\alpha=\beta(h_\alpha)b$. Thus (22) is proved. The element bR_a^{p-1} vanishes, for $\beta-\alpha$ is not a root. By iterated use of (22) we reach the contradiction $b=0$ (note that $\beta(h_\alpha)$ is nonzero by hypothesis).

(b) If γ is a nonisotropic root, 2γ is not a root.

Form the algebra M spanned by h_γ and $\sum L_{i\gamma}$, i running over all nonzero integers mod p. M is an algebra of rank one with a nonsingular invariant form. By Theorem 5, 2γ is not a root.

(c) If β is another isotropic root, then β is orthogonal to α.

Suppose on the contrary that β is not orthogonal to α. By part (a), $\alpha+\beta$ is a root. Since $f(h_\alpha, h_{\alpha+\beta})=f(h_\alpha, h_\alpha+h_\beta)=f(h_\alpha, h_\beta)\neq 0$, $\alpha+\beta$ is not orthogonal to α. Hence, again by (a), $2\alpha+\beta$ is a root. Similarly we argue that $2\alpha+\beta$ is not orthogonal to β, and hence $2\alpha+2\beta$ is a root. But $f(h_{\alpha+\beta}, h_{\alpha+\beta})=2f(h_\alpha, h_\beta)\neq 0$. Thus $\alpha+\beta$ is a nonisotropic root. We have contradicted part (b).

(d) If γ is not orthogonal to α (hence, by (c), is nonisotropic), then $f(h_\alpha, h_\gamma)/f(h_\gamma, h_\gamma)$ cannot be an integer.

Suppose this ratio is an integer i, necessarily different from 0. Let $j=-(2i)^{-1}$. By iterated use of (a), $\delta=\gamma+j\alpha$ is a root. However $f(h_\delta, h_\delta)=f(h_\gamma+jh_\alpha, h_\gamma+jh_\alpha)=0$, $f(h_\delta, h_\alpha)\neq 0$. This contradicts (c).

(e) The proof of (d) shows further: if γ is not orthogonal to α, each $\gamma+i\alpha$ (i an integer) is a nonisotropic root.

(f) We now complete the proof of Theorem 6. There must exist some root γ which is not orthogonal to α; otherwise h_α would be central, contrary to hypothesis. By (e), $\alpha-\gamma$ and $\alpha+\gamma$ are nonisotropic roots. We claim that $\alpha-2\gamma$ is not a root. If it were, $\alpha-2\gamma+\alpha=2(\alpha-\gamma)$ would also be a root by (a), contrary to (b). Similarly $\alpha+2\gamma$ is not a root. Write $u=h_\gamma/f(h_\gamma, h_\gamma)$. Select $a\in L_\gamma$, $x\in L_{-\gamma}$ with $ax=u$; note that $au=a$, $xu=-x$. Take $b\neq 0$ in $L_{\alpha-\gamma}$. We have $bx=0$, $bR_a^3=0$. Let n be the smallest integer such that $bR_a^n=0$ $(1\leqq n\leqq 3)$. Lemma 35 is applicable and tells us that $bT_n=b(nR_u+n_2I)=0$. Since $bh_\gamma=f(h_{\alpha-\gamma}, h_\gamma)b$, we deduce that $f(h_{\alpha-\gamma}, h_\gamma)+(n-1)f(h_\gamma, h_\gamma)=0$. It follows that $f(h_\alpha, h_\gamma)/f(h_\gamma, h_\gamma)$ is an integer, in contradiction to (d).

Theorem 6 is a generalization of Theorem 4.2 in [3]. Since Seligman makes no further use of the assumption that his invariant form arises from a representation, this accomplishes the classification of simple restricted Lie algebras with a nonsingular invariant form and a Cartan subalgebra that acts diagonally.

11. **The nondiagonable case.** It remains to discuss simple restricted Lie algebras of rank two with a nonsingular invariant form and a Cartan sub-

algebra with basis u, v satisfying $u^p = u$, $v^p = 0$. In this section we shall show that such algebras do not exist.

THEOREM 7. *Let L be a restricted simple Lie algebra of rank two over an algebraically closed field of characteristic >5. Assume that L possesses a nonsingular invariant form. Then any two-dimensional Cartan subalgebra of L acts diagonally.*

The proof will be broken up into a number of lemmas.

On any root space we have $R_v^p = 0$. Hence the roots are indexed merely by the characteristic roots of R_u: the integers mod p. On L_i, R_u acts as i times the identity.

LEMMA 41. *If $a \in L_1$ and $av \neq 0$, then $a^p = 0$.*

Proof. It is easily seen that a^p lies in H. Moreover $a \cdot a^p = 0$. If $av \neq 0$, no nonzero element of H annihilates a.

We shall make a large number of computations of a product of an element a in L_1 by an element x in L_{-1} in the following way: to determine ax it suffices to know $f(ax, u)$ and $f(ax, v)$, since f is nonsingular on H. Now $f(ax, u) = f(a, xu) = -f(a, x)$; $f(ax, v) = -f(av, x)$. So the ingredients of the computation are provided by the inner products of x with a and av. A large number of cases are covered by the next lemma; when slightly different computations have to be made later we shall leave them to the reader.

LEMMA 42. *Suppose that $a_i \in L_1$, $x_i \in L_{-1}$ $(i = 1, \cdots, n)$; that $a_i v = a_{i+1}$ $(i = 1, \cdots, n-1)$; and that $f(a_i, x_j) = \delta_{ij}$ (Kronecker delta). Then*: (a) $a_1x_1 = \cdots = a_nx_n$. *This element is orthogonal to v and has inner product -1 with u.* (b) $a_1x_2 = a_2x_3 = \cdots = a_{n-1}x_n$. *This element is orthogonal to u and has inner product -1 with v.* (c) $a_ix_j = 0$ *if $j \neq i$ or $i+1$.*

Proof. (a) $f(a_ix_i, u) = -1$ and $f(a_ix_i, v) = -f(a_{i+1}, x_i) = 0$.
(b) $f(a_ix_{i+1}, u) = 0$ and $f(a_ix_{i+1}, v) = -f(a_{i+1}, x_{i+1}) = -1$.
(c) If $j \neq i$ or $i+1$, a_ix_j is orthogonal to both u and v.

LEMMA 43. *If $a \in L_1$, $av \neq 0$, then aL_{-1} is all of H.*

Proof. The elements $a_1 = a$, $a_2 = av$ are linearly independent. Therefore we can find elements x_1, x_2 in L_{-1} such that $f(a_i, x_j) = \delta_{ij}$. By Lemma 42, a_1x_1 is nonzero and orthogonal to v; a_1x_2 is nonzero and orthogonal to u. Hence a_1x_1 and a_1x_2 span H.

LEMMA 44. *For any $a \in L_1$ we have $(av)R_a^{p-2} = 0$.*

Proof. If $av = 0$ there is nothing to prove. Otherwise by Lemma 43 there exists $z \in L_{-1}$ with $az = v$. By Lemma 41, $zR_a^p = 0$. Since $zR_a^2 = va$, this proves the lemma.

LEMMA 45. $f(v, v) = 0$.

Proof. We must have $R_v \neq 0$; otherwise v is in the center of L. Thus we may assume the existence of an element a in L_1 with $b = av \neq 0$. Let us write x for an element in L_{-1} with $f(a, x) = 1, f(b, x) = 0$. By Lemma 42 we have that $bx = 0$ and also that $w = ax$ is a nonzero element of H orthogonal to v. The lemma is proved if we show that w is a scalar multiple of v. We shall derive a contradiction from the contrary assumption. By a harmless normalization we may assume that w is of the form $u + \lambda v$. Then $aw - a$ is a scalar multiple of b. Now if we write W for the one-dimensional subspace spanned by b, the hypotheses of Lemma 26 (a) are fulfilled (except that the element u of that lemma is to be replaced by w). Hence

$$bR_a^{p-2}R_x^{p-2} = bT_1T_2 \cdots T_{p-2}, \tag{23}$$

where $T_i = iR_w + i_2 I$. But the left side of (23) vanishes by Lemma 44, while the right side is nonzero, since $iR_w + i_2 I$ is nonsingular on L_1 for $1 \leqq i \leqq p-2$.

LEMMA 46. *If $R_v^2 \neq 0$, then $f(u, u) = 0$.*

Proof. We may assume that R_v^2 is not zero on L_1. Pick a in L_1 with $aR_v^2 \neq 0$. Write $b = av$, $c = bv$. The elements a, b, c are linearly independent and thus we may pick elements x, y, z in L_{-1} dual to a, b, c (relative to f). From Lemma 42 we have that $az = 0$, and that bz is a nonzero element of H orthogonal to u. We note that R_a and R_z commute. From this we first derive $bR_aR_z = bR_zR_a \neq 0$, since a is not annihilated by any nonzero element of H. Hence $ba \neq 0$. By Lemma 44, $bR_a^{p-2} = 0$.

The lemma will be proved if we show that bz is a scalar multiple of u. Assume not; we may normalize so that $bz = v + \lambda u$. Let i be the smallest integer such that $bR_a^i = 0$ (necessarily $i \geqq 2$). Then

$$0 = bR_a^iR_z = bR_zR_a^i = (v + \lambda u)R_a^i.$$

Now $uR_a^i = 0$ and $vR_a = -b$. Hence $bR_a^{i-1} = 0$, a contradiction.

LEMMA 47. $R_v^3 = 0$.

Proof. Assume that R_v^3 is not zero on L_1. Then we can find a, $b = av$, $c = bv$, $d = cv$ linearly independent in L_1. Let w, x, y, z be elements of L_{-1} which are dual to a, b, c, d relative to f. By Lemmas 42 and 46 we have $ax = cz =$ a nonzero multiple of u. We may normalize so that $ax = cz = u$. Further, we have $cx = az = 0$. By Lemma 35, $cR_a^{p-2}R_x^{p-2} = cT_1 \cdots T_{p-2}$, and from this it follows as usual that $t = cR_a^{p-2}$ is not zero. Write $s = tc$. Then $f(s, c) = f(tc, c) = f(t, cc) = 0$. Hence $f(sc, u) = f(s, cu) = f(s, c) = 0$. It follows that $sc = tc \cdot c$ is a scalar multiple of u (Lemma 46). Next we prove $tz = 0$. This is done just as in §3. In brief: $ca \cdot z = -a$, $cR_a^2R_z = 0$, $cR_a^{p-2}R_z = cR_zR_a^{p-2} = 0$. All the hypotheses of Lemma 19 are now fulfilled (with b and y replaced by c and z). The conclusion $t = 0$ is a contradiction.

LEMMA 48. $R_v^2=0$.

Proof. Assume that R_v^2 does not vanish on L_1. Choose a, $b=av$, $c=bv$ linearly independent in L_1, and x, y, z dual to them (relative to f) in L_{-1}. Assembling the information in Lemmas 42 and 46, we have $ax=by=cz=$ a nonzero multiple of v which we can normalize to be v; $ay=bz=$ a multiple of u; all other products between a, b, c and x, y, z vanish. We can prove $ay=u$. For let $ay=\lambda u$. Then from the Jacobi identity on a, b, y we get $ab\cdot y=(1-\lambda)b$. But $f(ab\cdot y, y)=f(ab, yy)=0$, while $f(b, y)=1$. Hence $\lambda=1$.

Write $'$ for R_v (an inner derivation). We note: $a'=b$, $a''=c$. For any r in L we have $r'''=0$ by Lemma 47. Then by Leibniz's formula

$$0 = (ra)''' = r''' + a''' + 3r''a' + 3r'a''.$$

Hence

$$r''b + r'c = 0. \tag{24}$$

Write $d=ba$, and note $d'=ca$, $d''=cb$. Making use of the equations $az=0$, $bz=u$, $cz=v$, we can systematically compute products with z, beginning with $dz=-a$, $d'z=-b$, $d''z=0$. To (24), with $r=d$, apply R_z on the right. The result is $d''\cdot bz+d'z\cdot c+d'\cdot cz=0$, $d''u-bc+d'v=0$, $4d''=0$ (note that d and its derivatives are in L_2). Hence $d''=0$.

Next, let $e=da$. We find $e'=d'a+db$, $e'z=d'z\cdot a+dz\cdot b+d\cdot bz=-ba-ab+du=2d$. Also $e''=2d'b+dc$, $e''z=2(d'z\cdot b+d'\cdot bz)+dz\cdot c+d\cdot cz=2d'u-ac+dv=6d'$. To (24), with $r=e$, apply R_z on the right. We obtain $0=e''z\cdot b+e''u+e'z\cdot c+e'v=6d'b+3e''+2dc+e''$. Apply R_z again: $0=6(d'z\cdot b+d'u)+4e''z+2(dz\cdot c+dv)=12d'+24d'-2ac+2d'=40d'$. Hence $d'=0$, $b=-d'z=0$, a contradiction. (This is the one place in the proof of Theorem 7 that characteristic 5 causes trouble.)

LEMMA 49. *R_v acting on L_i has at most one elementary divisor of degree two.*

Proof. Assume the contrary for $i=1$. Then in L_1 we can find four linearly independent elements a, $b=av$, c, $d=cv$; note that $bv=dv=0$. Let w, x, y, z be elements of L_{-1} dual to a, b, c, d relative to f. By computations like that in Lemma 42, together with Lemma 45, we have $cx=cw=ay=az=bw=dy=0$; aw, bx, cy, dz are nonzero multiples of v; ax and cz are nonzero elements orthogonal to u (hence linearly independent of v). We can find a linear combination r of w and x with $ar=u$, and similarly a linear combination s of y and z with $cs=u$. We observe that $cr=as=0$.

Next we note that $cd\cdot y=0$, directly from the Jacobi identity. Also $cd\cdot z=0$, for by the Jacobi identity it is a scalar multiple of d, which must vanish since it is orthogonal to z (relative to f). Hence $cd\cdot s=0$.

By Lemma 35,

$$cR_a^{p-3}R_r^{p-3} = cT_1T_2\cdots T_{p-3},$$

where $T_i = iR_u + i_2 I$. Hence $t = cR_a^{p-3}$ is not 0. Again $cR_aR_s = cR_sR_a = -a$. Hence $ts = cR_a^{p-3}R_s = cR_sR_a^{p-3} = 0$. This allows us to apply Lemma 35 again, as follows:

$$tR_c^4R_s^4 = tT_1T_2T_3T_4. \tag{25}$$

Since $t \in L_{-2}$, we see that the right side of (25) is not 0. But $tR_c^2 \in H$, $tR_c^3 =$ a linear combination of c and d, $tR_c^4 =$ a scalar multiple of cd, $tR_c^4R_s = 0$. This contradiction completes the proof of Lemma 49.

Lemma 50. *If $a \in L_i$, $x \in L_{-i}$, and av and xv are not zero, then ax is not a scalar multiple of v.*

Proof. If ax is a scalar multiple of v, then by Lemma 45, $f(ax, v) = 0$, whence $f(a, xv) = 0$. But by Lemma 49, xv spans $L_{-i}v$. Hence $f(a, L_{-i}v) = 0$, $f(av, L_{-i}) = 0$, a contradiction since av is not zero.

We pause at this point to fix notation and collect information for the remainder of the proof of Theorem 7. Assume that L_1v is not 0. By Lemmas 48 and 49, L_1 has a basis $a, b, c_1, \cdots, c_r$ with $av = b$, $bv = c_iv = 0$. Take a basis $x, y, z_1, \cdots, z_r$ for L_{-1} which is dual relative to f. Since R_v on L_{-1} is the negative of the adjoint of R_v on L_1, we have $yv = -x$, $xv = z_iv = 0$. Computation like that in Lemma 42 reveals first that all products between L_1 and L_{-1} vanish except: ax, by, ay, $c_1z_1, \cdots, c_rz_r$. Next, $ax = by = c_iz_i =$ a nonzero scalar multiple of v which we can normalize to be v. There remains only the product ay. Suppose $ay = \lambda u + \alpha v$. From the Jacobi identity on a, b, y we get $ab \cdot y = (1-\lambda)b$. But $f(ab \cdot y, y) = f(ab, yy) = 0$, while $f(b, y) = 1$. Hence $\lambda = 1$, $ay = u + \alpha v$. (We have here repeated a fragment of the proof of Lemma 48.)

Set $w = y - \alpha x$; then $aw = u$. The element w is convenient for our purposes since the triple a, w, u fits the hypotheses of Lemmas 35–37 (with w replacing x).

Lemma 51. $(L_iv \cdot L_i)L_{-i} = 0$.

Proof. We take $i = 1$, and use the notation fixed above. Since L_1v is spanned by b, what we have to show is that ab and bc_i annihilate L_{-1}. Everything comes right out of the Jacobi identity except the fact that $ab \cdot y = 0$, which was noted just above.

Lemma 52. *For $2 \leqq j \leqq (p-1)/2$, R_a maps L_j one-to-one into L_{j+1}, and R_w maps L_{j+1} onto L_j. For $(p+1)/2 \leqq j \leqq p-2$, R_w maps L_j one-to-one into L_{j-1}, and R_a maps L_{j-1} onto L_j.*

Proof. This is immediate from Lemma 37 as soon as we check $L_0R_a^2R_w = 0$, $L_0R_w^2R_a = 0$. But both statements follow from Lemma 51.

Lemma 53. *R_v annihilates either L_i^2 or L_{-i}^2.*

Proof. Assume the contrary for $i = 1$, and use the notation above. L_1^2 is spanned by ab, ac_j, bc_j $(j=1, \cdots, r)$. The elements ab, bc_j are visibly annihilated by v. Hence some $ac_j \cdot v \neq 0$. Similarly some $yz_k \cdot v \neq 0$. It then follows from Lemma 50 (with $i=2$) that $ac_j \cdot yz_k$ is not a multiple of v. But we are able to compute this product and find that it is a multiple of v. We have $c_j y=0$, $az_k=0$, $ay=u+\alpha v$, $by=v$, $c_j z_k=0$ or v. By repeated use of the Jacobi identity $ac_j \cdot y=-c_j$, $ac_j \cdot z_k$ is a multiple of b, $ac_j \cdot yz_k$ is a linear combination of $c_j z_k$ and by and is a multiple of v.

LEMMA 54. *R_v annihilates L_i^2.*

Proof. Assume the contrary for $i=1$. Continuing the argument of Lemma 53, we have that some ac_j is not annihilated by R_v, that is, $bc_j \neq 0$. Let us write simply c for c_j.

By Lemma 35, $cR_a^i R_w = cT_i R_a^{i-1}$. Since $c \in L_1$ and $T_i = iR_u + i_2 I$, cT_i is simply $(i+1)_2 c$. Thus

$$cR_a^i R_w = (i+1)_2 c R_a^{i-1}. \tag{26}$$

We apply (26) with $i=p-2$. By Lemma 53, $L_{-1}^2 v=0$ (since we are assuming $L_1^2 v \neq 0$). Now $cR_a^{p-2}R_w \in L_{-1}^2$. Hence $cR_a^{p-3}R_v=0$. We are going to contradict this by a computation which is a slight variant of numerous earlier ones.

We have $R_a R_x = R_x R_a + R_v$. Since $cv=cx=0$, we deduce $cR_a R_x=0$ and further

$$cR_a^2 R_x = cR_a R_v = cb. \tag{27}$$

We next note

$$cR_a^2 R_v R_w = 4cb. \tag{28}$$

To prove (28) we write $R_v R_w = R_w R_v + R_x$ (recall that $w=y-\alpha x$ so that $wv=yv=-x$), use (27), and (26) with $i=2$.

We are going to establish inductively

$$cR_a^i R_v R_w^{i-1} = (i+2)(i+1)_2 i_2 \cdots 5_2 4_2 cb \tag{29}$$

for $i \geqq 2$. For $i=2$ we interpret (29) to coincide with (28); at any rate the reader can check that the induction can start correctly this way. In (29) replace $R_v R_w$ by $R_w R_v + R_x$. The first of the resulting terms is

$$(i+1)_2(i+1)i_2(i-1)_2 \cdots 4_2 cb \tag{30}$$

by (26) and induction. We study the remaining term $cR_a^i R_x R_w^{i-2}$. By Lemma 51, xw annihilates L_1; in particular xw annihilates a, c and all their products. It follows that R_x and R_w may be interchanged in the expression. The R_w thus made adjacent to cR_a^i can be absorbed as in (26). Then we are ready to commute R_w and R_x again. By a succession of these steps we eventually push R_x all the way to the right, arriving at

$$(i+1)_2 i_2 \cdots 4_2 c R_a^2 R_x = (i+1)_2 \cdots 4_2 cb \tag{31}$$

by (27). Since (30) and (31) add up to the right side of (29), the induction is complete.

Set $i=p-3$ in (29). We saw that the left side vanishes. The coefficient on the right is nonzero, and further cb is nonzero by assumption. This contradiction concludes the proof of Lemma 54.

LEMMA 55. $L_{2i}v \cdot L_{-i}=0$.

Proof. It suffices to prove $f(L_{2i}v \cdot L_{-i},\ L_{-i})=0$, or $f(L_{2i}v,\ L_{-i}^2)=0$, or $f(L_{2i},\ vL_{-i}^2)=0$, and this is true by Lemma 54.

We record for later use three more computational lemmas. For conciseness we introduce a new symbol: $F_i=i(i+3)/2$.

LEMMA 56. *For* $i \geqq 1$, $bR_a^i R_w = F_{i-1} b R_a^{i-1}$.

Proof. By Lemma 51, $ba \cdot w=0$. We can then apply Lemma 35 to deduce $(ba)R_a^{i-1}R_w = baT_{i-1}R_a^{i-1}$. Here $T_{i-1}=(i-1)R_u+(i-1)_2 I$. Since $(ab)R_u=2ab$, we compute that $(ab)T_{i-1}=F_{i-1}ab$.

LEMMA 57. *For* $i \geqq 2$

$$bR_a^i R_x R_w^{i-2} = 0. \tag{32}$$

Proof. For $i=2$ we have to prove $bR_a^2R_x=0$, and this admits direct verification. We assume (32) known with i replaced by $i-1$. In (32) replace R_xR_w by $R_wR_x+R_{xw}$. By Lemma 51 (since $wv=-x$), xw annihilates a and b and hence all their products. This term therefore drops out. To the remaining term apply Lemma 56 and our inductive assumption.

LEMMA 58. *For* $i \geqq 1$, $bR_a^i R_v R_w^{i-1}=0$.

Proof. The case $i=1$ ($bR_aR_v=0$) is immediate. Replace R_vR_w by $R_wR_v+R_x$. The first resulting term vanishes by Lemma 56 and induction. The second vanishes by Lemma 57.

LEMMA 59. *Suppose that* R_v *vanishes on every* L_i *except for* $i=\pm 1$. *Let* S *denote the subspace of* L *spanned by* v, b, $bR_a, \cdots, bR_a^{p-3}$, x, $xR_w, \cdots, xR_w^{p-3}$. *Then* S *is an ideal in* L.

Proof. We begin by noting that S is invariant under R_a and R_w; by symmetry it suffices to handle R_w. We have $wv=-x$, $bw=v$. By Lemma 44, xR_w^{p-3} is annihilated by R_w. Lemma 56 covers the application of R_w to bR_a^i.

Let T denote the set of elements t satisfying $tL \subset S$. T is invariant under R_a and R_w: for instance $tw \cdot L \subset tL \cdot w + t \cdot wL \subset Sw+S \subset S$. Since L_1v and $L_{-1}v$ are spanned by b and x, and all other L_iv are 0, we have $v \in T$. It follows that vR_a^i and vR_w^i lie in T for all i. This proves $S \subset T$, and S is an ideal in L.

Up to this point we have in effect been analyzing the structure of any restricted Lie algebra of rank two with a nonsingular invariant form; simplicity has not yet been invoked. Possibly the full structure of this class of algebras can be elucidated (it is a fact that examples do exist); but we shall make use of the simplicity from now on.

In the next four lemmas we maintain our assumption that L_1v is nonzero and continue to use the notation we have established.

LEMMA 60. *ab and xy are not* 0.

Proof. We shall assume $ab=0$ and derive a contradiction by showing that $L_jv=0$ for $j\neq\pm 1$ (this, by Lemma 59, provides a proper ideal in L).

First we prove $L_jb=0$ for $2\leqq j\leqq(p-1)/2$. This is true for $j=(p-1)/2$ by Lemma 55 (take $i=1/2$). We make a descending induction on j. We suppose $L_{j+1}b=0$ known $(2\leqq j<(p-1)/2)$. Then $L_jR_aR_b=0$. But R_a and R_b commute; hence $L_jR_bR_a=0$. On L_{j+1}, R_a is one-to-one (Lemma 52); hence $L_jb=0$.

We already know $bc_1=\cdots=bc_r=0$ by Lemma 54. The hypothesis $ba=0$ tells us therefore that L_1b is 0, whence $L_2R_wR_b=0$. So for any j with $2\leqq j\leqq(p-1)/2$, $L_jv=L_j\cdot bw\subset L_j(R_bR_w+R_wR_b)=0$, as desired.

LEMMA 61. *L_2 contains an element d satisfying $dy=a$.*

Proof. Since $xy\neq 0$ (Lemma 58) there exists an element $d\in L_2$ with $f(d, xy)\neq 0$. Now dy lies in L_1 and is orthogonal to y, relative to f. Hence dy is a linear combination of $a, c_1, \cdots, c_r$. The a-component must actually be present, for otherwise we have the contradiction $f(dy, x)=0$. Since $ac_i\cdot y=-c_i$ by the Jacobi identity, we can adjust d by a suitable linear combination of the elements ac_i so as to have $dy=a$ (after a further normalization by a scalar).

LEMMA 62. Dim $(L_2)\geqq$ dim (L_1).

Proof. We prove this by showing that the elements $ab, ac_1, \cdots, ac_r$ and the element d of Lemma 61 are linearly independent. Under R_y, ac_i is sent into $-c_i$, d into a, and ab into 0 (Lemma 51). Together with the fact that ab is nonzero, this proves the linear independence.

LEMMA 63. Dim $(L_{(p-1)/2})\geqq$ dim L_1. *If the two dimensions are equal, then all root spaces L_j $(j\neq 0)$ have the same dimension.*

Proof. In the sequence of spaces $L_1, L_2, \cdots, L_{(p-1)/2}$ the dimensions are increasing (in the weak sense); the step from L_1 to L_2 is covered by Lemma 62, snd the remaining steps by Lemma 52. This implies both statements in the present lemma.

LEMMA 64. *If for some i the root spaces L_i and L_{2i} are both not annihilated by R_v, then all root spaces L_j $(j\neq 0)$ have the same dimension.*

Proof. We have dim $(L_{2i})\geqq$ dim (L_i) by Lemma 62. Now let L_{2i} play the role of L_1 in Lemma 63; L_i becomes $L_{(p+1)/2}$ and its dimension is the same as that of $L_{(p-1)/2}$. The hypothesis of Lemma 63 is therefore fulfilled.

It is our intention to prove that in all cases the root spaces have equal dimension. The discussion need only continue under the assumption $L_1v\neq 0$, $L_2v=0$. The crucial fact then is that the element d of Lemma 61 satisfies $dv=0$. Applying R_v to the equation $dy=a$ we then compute

$$dx = -b. \tag{33}$$

Recalling that $w=y-\alpha x$, we find from (33):

$$dw = a + \alpha b. \tag{34}$$

Apply the Jacobi identity to the triple d, x, w. The result is:

$$d\cdot xw = -2v. \tag{35}$$

We proceed to more elaborate computations of products involving d.

LEMMA 65. *For* $i\geqq 1$,

$$dR_a^iR_w = F_idR_a^{i-1} + \alpha bR_a^i \tag{36}$$

where, as in Lemma 56, $F_i=i(i+3)/2$.

Proof. We check this first for $i=1$, using $R_aR_w=R_wR_a+R_u$, $du=2d$, and (34). Assume (36) for $i-1$. Then

$$\begin{aligned} dR_a^iR_w &= dR_a^{i-1}(R_wR_a + R_u) \\ &= (F_{i-1}dR_a^{i-2} + \alpha bR_a^{i-1})R_a + (i+1)dR_a^{i-1}, \end{aligned}$$

and this boils down to the right side of (36).

LEMMA 66. *For* $i\geqq 1$,

$$dR_a^iR_xR_w^{i-1} = G_iba, \tag{37}$$

where $G_1=-1$, $G_2=-3$,

$$G_i = F_iG_{i-1} + 2F_{i-2}\cdots F_2F_1. \tag{38}$$

Proof. We have $R_aR_x=R_xR_a+R_v$. Then $dR_aR_x=dx\cdot a+dv=-ba$ by (33). This checks (37) for $i=1$. We begin the induction at this point, making a special remark on $i=2$ at the appropriate moment. In (37) replace R_xR_w by $R_wR_x+R_{xw}$. On the first resulting term we use Lemma 65, obtaining

$$(F_idR_a^{i-1} + \alpha bR_a^i)R_xR_w^{i-2}. \tag{39}$$

The second of the terms in (39) vanishes by Lemma 57. The first, by induction, is $F_iG_{i-1}ba$. It remains to discuss the term $dR_a^iR_{xw}R_w^{i-2}$. Since xw annihilates a (Lemma 51) we can commute R_{xw} past R_a^i. Quoting (35), we reach

$-2vR_a^iR_w^{i-2}=2bR_a^{i-1}R_w^{i-2}$. By using Lemma 56 repeatedly we identify this as $2F_{i-2}\cdots F_2F_1ba$ (for $i=2$ it is simply $2ba$, and this leads to the value $G_2=-3$, since $F_2G_1+2=5(-1)+2=-3$). Summarizing: the left side of (38) equals $F_iG_{i-1}ba+2F_{i-2}\cdots F_2F_1ba$ as was to be shown.

LEMMA 67. *For* $i\geqq 0$

$$dR_a^iR_vR_w^i = H_iba, \tag{40}$$

where $H_0=0$,

$$H_i = F_iH_{i-1} + G_i. \tag{41}$$

Proof. For $i=0$, the left side of (40) is $dv=0$, and the right side is 0 too. Then use $R_vR_w=R_wR_v+R_x$, which follows from $wv=-x$.

$$\begin{aligned} dR_a^iR_vR_w^i &= dR_a^i(R_wR_v + R_x)R_w^{i-1} \\ &= (F_idR_a^{i-1} + abR_a^i)R_vR_w^{i-1} + dR_a^iR_xR_w^{i-1} \\ &= F_iH_{i-1}ba + G_iba \end{aligned}$$

by Lemma 65, induction, Lemma 58, and Lemma 66.

Let us compute the values of F_i, G_i, H_i up to $i=4$. $F_1=2$, $F_2=5$, $F_3=9$, $F_4=14$. Now use (38). $G_3=9(-3)+4=-23$, $G_4=14(-23)+2\cdot 5\cdot 2=-302$. Next use (41). $H_1=-1$, $H_2=5(-1)-3=-8$, $H_3=9(-8)-23=-95$, $H_4=14(-95)-302=-1632$.

Since H_1 is not 0, we have, by (40), that $dR_aR_v\neq 0$. Now $da\in L_3$; hence $L_3v\neq 0$. If H_4 is not 0, we similarly have $dR_a^4R_v\neq 0$ and $L_6v\neq 0$. Then Lemma 64 tells us that all root spaces have the same dimension. Now $H_4=-1632$ is divisible by 2, 3 and 17. So there is trouble for characteristic 17. But the trouble is easily resolved by a slight additional argument. We have in any event $L_3v\neq 0$. If $L_6v\neq 0$, all is well. If $L_6v=0$, we can replace L_1 by L_3 in the argument we have just carried out. Conclusion: $L_9v\neq 0$. But $1=2.9$ for characteristic 17, so Lemma 64 is applicable again. We have proved:

LEMMA 68. *All root spaces* L_j $(j\neq 0)$ *have the same dimension.*

This enables us to sharpen Lemma 52.

LEMMA 69. *For* $2\leqq j\leqq p-3$, R_a *induces a one-to-one linear transformation of* L_j *onto* L_{j+1} *and* R_w *induces a one-to-one linear transformation of* L_{j+1} *onto* L_j.

LEMMA 70. *Assume* $L_2v\neq 0$. *Then* L_2v *is spanned by* ab; $L_{-2}v$ *is spanned by* xy.

Proof. By symmetry it suffices to establish the second statement. Since $L_{-2}v$ is one-dimensional (Lemma 49) and xy is nonzero (Lemma 60), it suffices to prove $xy\in L_{-2}v$. It is equivalent to prove $f(xy, N)=0$ where N is the null space of R_v within L_2.

As we saw in Lemma 62, the elements d, ab, and ac_i $(1 \leqq i \leqq r)$ span a subspace of L_2 with the same dimension as that of L_1. Now that we know that L_1 and L_2 have the same dimension, we have a basis of L_2 consisting of these elements. Since R_v annihilates ab and ac_i (Lemma 54), and since N has codimension one in L_2, ab and ac_i constitute a basis of N. We know that x annihilates ab and ac_i. Hence $f(xy, N) = 0$.

From Lemma 70 we are able to deduce that (33), previously established only on the assumption that L_2v is 0, also holds when L_2v is nonzero. For dv is a scalar multiple of ab and $y \cdot ab = 0$. Applying R_v to the equation $dy = a$ then yields (33); $dx = -b$. Equation (34) and (35) follow as before.

LEMMA 71. *The null space of R_w within L_2 is spanned by ab.*

Proof. We examine R_w on the basis d, ab, ac_i of L_2. We have $dw = a + \alpha b$, $ac_i \cdot w = -c_i$ (recall $c_i w = 0$, $aw = u$). Since $ab \cdot w = 0$, and since the elements $a + \alpha b$, $c_1, \cdots, c_r$ are linearly independent, the lemma follows.

LEMMA 72. *For $3 \leqq j \leqq p-2$, $L_j R_{xw}$ is spanned by bR_a^{j-3}.*

Proof. First we examine R_{xw} on L_2. Since xw annihilates ab and ac_i, and since $d \cdot xw = -2v$ by (35), $L_2 R_{xw}$ is spanned by v. For $3 \leqq j \leqq p-2$ we have $L_j = L_2 R_a^{j-2}$ by Lemma 69. R_a and R_{xw} commute; consequently $L_j R_{xw} = L_2 R_{xw} R_a^{j-2}$, which is spanned by $vR_a^{j-2} = -bR_a^{j-3}$.

LEMMA 73. *For $2 \leqq j \leqq p-1$, $L_j x$ is spanned by bR_a^{j-2}.*

Proof. (a) $j = 2$. We must examine the products dx, $ab \cdot x$, $ac_i \cdot x$, and we find $dx = -b$, $ab \cdot x = ac_i x = 0$.

(b) $2 < j < p-1$. Since R_w is one-to-one on L_j (Lemma 69), and $bR_a^{j-2} R_w$ is a scalar multiple of bR_a^{j-3} (Lemma 56), it suffices to prove that $L_j R_x R_w$ is spanned by bR_a^{j-3}. Now

$$L_j R_x R_w \subset L_j R_w R_x + L_j R_{xw}. \tag{42}$$

The first term on the right of (42) is contained in $L_{j-1} R_x$ which is spanned by bR_a^{j-3} by induction. The second term is covered by Lemma 72.

(c) A special argument is needed for xL_{p-1}. We know that xL_{-1} is spanned by xw, and so our problem is to prove that xw is a scalar multiple of bR_a^{p-3}. By Lemma 44, xw is annihilated by R_w^{p-3}. Thus xR_w^{p-3} is an element of L_2 annihilated by R_w. By Lemma 71, xR_w^{p-3} is a scalar multiple of ab. But by iterated use of Lemma 56, $bR_a^{p-3} R_w^{p-4}$ is a nonzero scalar multiple of ab. So: we have two elements, namely xw and bR_a^{p-3} in L_{-2}; on applying R_w^{p-4} they both become scalar multiples of ab. By Lemma 69, R_w^{p-4} is a one-to-one map of L_{-2} into L_2. Since bR_a^{p-3} is nonzero, we conclude that xw is a scalar multiple of bR_a^{p-3}.

The moment has arrived for concluding the proof of Theorem 7: we shall produce a proper ideal in L. It is the subspace S spanned by $x, v, b, bR_a, bR_a^2, \cdots,$

bR_a^{p-3}. Note that this sequence is obtained from x by repeated operation of R_a, and that a final application of R_a yields 0 by Lemma 44. Hence $Sa\subset S$. As in the proof of Lemma 59, all will be done as soon as we verify $xL\subset S$. The action of R_x on the spaces $L_2, \cdots, L_{p-1}$ is covered by Lemma 73. On the two remaining spaces L_0 and L_1 we have known all along that L_0x is spanned by x and L_1x is spanned by v. The proof is complete.

PART III. APPENDIX ON CHARACTERISTICS TWO AND THREE

12. **Rank one, characteristic two.** The counterpart of Theorem 2 for the case of characteristic two is very easy—see Lemma 74. However we can go further and analyze any collection of roots.

THEOREM 8. *Let L be a simple Lie algebra of rank one over an algebraically closed field of characteristic two. Let $\{L_\alpha\}$ denote the root spaces relative to a one-dimensional Cartan subalgebra. Then each L_α $(\alpha\neq 0)$ is two-dimensional, and the roots form a group under addition.*

As usual we write u for a nonzero element of the Cartan subalgebra. The product of any two elements of L_α is a scalar multiple of u. Suppose $L_\alpha^2\neq 0$. Then we can find x, $y\in L_\alpha$ with $xy=u$ (note that x and y are necessarily linearly independent). Let z be a possible third linear independent element in L_α. Apply the Jacobi identity to the triple x, y, z. The result: zu is a linear combination of xu and yu. Since R_u is nonsingular on L_α, this is impossible. Hence:

LEMMA 74. *For any root space L_α, either $L_\alpha^2=0$ or L_α is two-dimensional.*

From this, it takes just a moment to dispose of the restricted case: there are no simple restricted Lie algebras of rank one and characteristic two.

LEMMA 75. *If $L_\alpha^2\neq 0$ and x is an element of L annihilating L_α, then $x=0$.*

Proof. There exist elements a, b in L_α with $ab=u$. Applying the Jacobi identity to a, b, x we find $ux=0$. Hence x is a scalar multiple of u. But R_u is nonsingular on L_α. Hence $x=0$.

LEMMA 76. *Suppose α, β, γ are roots with $\beta+\gamma=\alpha$, $L_\alpha^2\neq 0$, $L_\beta^2=L_\gamma^2=0$. Then $L_\beta L_\gamma=0$.*

Proof. Let $y\in L_\beta$, $z\in L_\gamma$, $yz=x$. We have $xL_\alpha=yz\cdot L_\alpha\subset yL_\alpha\cdot z+zL_\alpha\cdot y\subset L_\gamma^2+L_\beta^2=0$. By Lemma 75, $x=0$.

LEMMA 77. *Let α be a root such that $L_\alpha^2\neq 0$. Let β be any other root, and $\gamma=\alpha+\beta$. Then γ is also a root. If L_β is two-dimensional, so is L_γ.*

Proof. If γ is not a root then $L_\alpha L_\beta=0$, which is impossible by Lemma 75.

Suppose L_β is two-dimensional. Let x, y be elements of L_α with $xy=u$. We have $R_xR_y+R_yR_x=R_u$. The subspace $L_\beta+L_\gamma$ is invariant under R_x and

R_y; hence the trace of R_u on $L_\beta+L_\gamma$ is 0. On L_β, the trace of R_u is 0. On L_γ, the trace of R_u is γ multiplied by the dimension of L_γ. Hence that dimension must be even.

Because of the equation $R_xR_y+R_yR_x=R_u$, the null spaces of R_x and R_y on L_γ have zero intersection. If the dimension of L_γ is k, these null spaces have dimension at least $k-2$ (since the range is in L_β, which is two-dimensional). Hence k must be 2 or 4. It remains for us to exclude the possibility $k=4$.

We again pick elements x, y in L_α with $xy=u$, this time in Jordan form: $xu=\alpha x$, $yu=\alpha y+\lambda x$, $\lambda=0$ or 1. Let N denote the (necessarily two-dimensional) null space of R_x in L_γ. From the equation $[R_xR_u]=\alpha R_x$ we see that N is invariant under R_u. Since $R_yR_x=R_u$ on N we have that R_x is a one-to-one mapping of L_β onto N. Pick a nonzero element a in N with $au=\gamma a$. Write $ay=c$, $cy=e$. We apply the Jacobi identity five times in succession, listing the triple and the resulting equation. (a) a, x, y: $cx=\gamma a$. (b) a, y, u: $cu=\beta c$. (c) c, x, y: $ex=\alpha c$. (d) c, y, u: $eu=\gamma c+\lambda\gamma a$. (e) e, x, y: $ey\cdot x=\beta e+\lambda\gamma a$. Since $ey\in L_\beta$ and R_x maps L_β into N, we deduce $e\in N$. But this means $ex=0$, whereas $ex=\alpha c\neq 0$.

With these preliminary lemmas at our disposal, we are ready to give the proof of Theorem 8. Write Γ for the set of all roots γ such that $L_\gamma^2\neq 0$. Let Δ be the group generated by Γ (i.e. the set of all sums of elements in Γ). We have three things to prove: (1) Every member of Δ is a root, (2) For $\delta\in\Delta$, L_δ is two-dimensional, (3) Every root lies in Δ.

(1) Let $\delta\in\Delta$, $\delta=\gamma_1+\gamma_2+\cdots+\gamma_n$, $\gamma_i\in\Gamma$. We may assume by induction on n that $\zeta=\gamma_2+\cdots+\gamma_n$ is a root. By Lemma 77, $\delta=\gamma_1+\zeta$ is a root.

(2) We may further assume by induction that L_ζ is two-dimensional. By the second half of Lemma 77, L_δ is also two-dimensional.

(3) (This is the sole portion of the proof that uses simplicity.) Let S denote the subspace of L spanned by $\{L_\alpha\}$, where α is not in Δ. We shall prove that S is an ideal. Given a root α not in Δ, and any root β, we must prove $L_\alpha L_\beta\subset S$. If $\alpha+\beta$ is not in Δ, all is well. Assume $\alpha+\beta=\gamma_1+\gamma_2+\cdots+\gamma_n$, $\gamma_i\in\Gamma$. We shall in this case prove $L_\alpha L_\beta=0$. This is immediate from Lemma 76 if $n=1$ (note that $L_\alpha^2=L_\beta^2=0$ since α and β are not in Γ; they are not even in Δ). We make an induction on n. The roots $\alpha+\gamma_1$ and β are not in Δ and they add up to a root in Δ. By our inductive assumption $L_{\alpha+\gamma_1}L_\beta=0$. Similarly $L_\alpha L_{\beta+\gamma_1}=0$. By the Jacobi identity, $(L_\alpha L_\beta)L_{\gamma_1}=0$, whence, by Lemma 75, $L_\alpha L_\beta=0$. This completes the proof of Theorem 8.

To conclude this section we give an example showing that there is a genuine distinction between the sets Γ and Δ introduced above, i.e. that in a simple Lie algebra there may exist a root space L_α with $L_\alpha^2=0$. The smallest possible dimension for an example is 7. In the following example the Cartan subalgebra is spanned by u; there are three root spaces L_α, L_β, L_γ ($\gamma=\alpha+\beta$) spanned by a, $b\in L_\alpha$, p, $q\in L_\beta$, r, $s\in L_\gamma$. R_u acts diagonally on its root spaces. We have $pq=u$, $rs=u$, but $ab=0$ so that $L_\alpha^2=0$. The remaining products are as follows: $ap=0$, $aq=s$, $ar=p$, $as=0$, $bp=\beta s$, $bq=r$, $br=\beta q$, $bs=p$, $pr=\gamma b$, $ps=\alpha a$, $qr=0$, $qs=b$. Brutal computation verifies the Jacobi identity and the simplicity.

13. **Rank one, characteristic three.** We are able to establish the analogue of Theorem 2 by finding the simple algebras whose only roots are ± 1.

THEOREM 9. *Let L be a simple Lie algebra over an algebraically closed field of characteristic three. Assume that a one-dimensional Cartan subalgebra of L is spanned by an element u such that the characteristic roots of R_u are* 1, -1, 0. *Then L is either* 3*-dimensional or isomorphic to a certain* 7*-dimensional algebra.*

Proof. Write V and W for the root spaces L_1 and L_{-1} respectively. We begin by recalling Lemma 5: if $a\in V$ and $Wa\neq 0$ then the only elements of V annihilated by a are the scalar multiples of a.

If $V^3=W^3=0$, it is readily seen that V^2+W^2 is an ideal in L, hence 0. This makes V and W one-dimensional, L 3-dimensional. We therefore assume $V^3\neq 0$ and select elements $a, b, c\in V$ with $a\cdot bc=u$. Write $bc=x$, $ca=y$, $ab=z$.

If r and s are any elements of V, we claim $r\cdot rs=0$. To see this, note that $r\cdot rs$ and $s\cdot rs$ are scalar multiples of u, say αu and βu. From the Jacobi identity on r, s, rs we get $\beta ur-\alpha us=0$. If r and s are linearly dependent, there is nothing to prove. Otherwise there is a contradiction unless $\alpha=\beta=0$.

From this we get the following vanishing products: $ay=az=bx=bz=cx=cy=0$.

Apply the Jacobi identity to the triples y, a, b and c, a, z. The result is

$$yz = -a\cdot by = -a\cdot cz. \tag{43}$$

It follows from (43) that by and cz are equal, say to λu. The Jacobi identity on a, b, c gives us $ax+by+cz=0$. Since $ax=u$, we find $1+2\lambda=0$, $\lambda=1$, $by=cz=u$. Since yz annihilates a, it is a scalar multiple of a. From (43) we deduce simultaneously $yz=-a$, $au=a$. By symmetry (a, b and c are now on an equal footing), $zx=-b$, $xy=-c$, $bu=b$, $cu=c$. The Jacobi identity on u, b, c yields $xu=-x$ and similarly $yu=-y$, $zu=-z$. We have identified all products in the 7-dimensional algebra spanned by u, a, b, c, x, y, z and recognize it, for instance, as the Cayley numbers of trace 0 under commutation. Finally we must show that L contains nothing else. Think of the equation $R_bR_c-R_cR_b=R_x$ applied to W. If the dimension of W is n, the range of R_x on W is $(n-1)$-dimensional (since R_x annihilates only x). But the range of $R_bR_c-R_cR_b$ is spanned by b and c. Hence n is 3. This proves that V and W are 3-dimensional and completes the proof of Theorem 9.

14. **Rank two, nondiagonable case.** In the case of a simple restricted Lie algebra of rank two and characteristic 2 or 3, we can rule out the nondiagonable case without the aid of an invariant form. Moreover, the proof is much simpler than that of Theorem 7.

THEOREM 10. *Let L be a simple restricted Lie algebra of rank two over an algebraically closed field of characteristic* 2 *or* 3. *Then any two-dimensional Cartan subalgebra H acts diagonally.*

The first step in the proof can be taken for any p. We have a basis u, v for H with $u^p=u$, $v^p=0$. Write $'$ for R_v, and U for the one-dimensional subspace spanned by u.

LEMMA 78. *If $a\in L_1$, $a'R_a^{p-2}\neq 0$, and $x\in L_{-1}$, then $ax\in U$.*

Proof. The proof of Lemma 41 is valid and shows that $a^p=0$. Hence $xR_a^p=0$. Suppose xa has a nonzero v-component. Then xR_a^3 is a nonzero scalar multiple of $a'a$. It follows that $a'R_a^{p-2}=0$, a contradiction.

We are ready to handle the case of characteristic 2. There is only one root space L_1. If $L_1v=0$, v is central. Hence there exists a in L_1 with $a'\neq 0$. We shall prove $L_1^2\subset U$; this is a contradiction, for then $L^2=L$ fails to contain v. We have $aL_1\subset U$ by Lemma 78. Take any $b\in L_1$. If $b'\neq 0$, then $bL_1\subset U$. If $b'=0$, then $(a+b)'\neq 0$, $(a+b)L_1\subset U$, $bL_1\subset U$.

The proof of Theorem 10 now continues only for the case of characteristic 3.

LEMMA 79. *For any $a\in L_1$, $a'a=0$.*

Proof. The argument is similar to the one just given. Assume the existence of $a\in L_1$ with $a'a\neq 0$. Then $aL_{-1}\subset U$ by Lemma 78. Take any $b\in L_1$. If $b'b\neq 0$, $bL_{-1}\subset U$. If $b'b=0$, we study $c=a+b$, $d=a-b$. Since $c'c+d'd=-a'a$, either $c'c$ or $d'd$ is nonzero, say $c'c$. Then $(a+b)L_{-1}\subset U$, whence $bL_{-1}\subset U$. We have proved $L_1L_{-1}\subset U$, a contradiction for L^2 fails to contain v.

LEMMA 80. *L_1v and $L_{-1}v$ are not* 0.

Proof. Assume $L_{-1}v=0$. Then L_1v cannot be 0; otherwise v would be central. From the Jacobi identity on v, L_1, L_{-1} we get $L_1v\cdot L_{-1}=0$. Take a in L_1 with $a'\neq 0$. We have $a'L_{-1}=0$ and by Lemma 79, $a'a=0$. From the Jacobi identity on a, a', L_{-1} it then follows that $aL_{-1}\cdot a'=0$, whence $aL_{-1}\subset V$, the one-dimensional subspace spanned by v. Take any $b\in L_1$. If $b'\neq 0$, $bL_{-1}\subset V$ by what we have just shown. If $b'=0$, then $(a+b)'\neq 0$, $(a+b)L_{-1}\subset V$, $bL_{-1}\subset V$. Hence $L_1L_{-1}\subset V$, a contradiction since u is not in the square of L.

LEMMA 81. *R_v^2 vanishes on L_1.*

Proof. Assume the contrary. Then we have elements a, b, $c\neq 0$ in L_1 with $b=a'$, $c=b'$. Take any x in L_{-1} and apply the Jacobi identity to a, b, x. Since $ab=0$, we get $bx\cdot a+xa\cdot b=0$, and this equation requires that ax lie in U. Take any d in L_1. If $dR_v^2\neq 0$, then $dx\in U$ by what we just proved. If $dR_v^2=0$, then $(a+d)R_v^2\neq 0$, $(a+d)x\in U$, $dx\in U$. This shows that $L_1L_{-1}\subset U$, a contradiction.

We conclude the proof of Theorem 10 by producing an ideal in L, namely the subspace S spanned by v, M, and N where M, N are the null spaces of R_v in L_1 and L_{-1}. Of course, S is invariant under R_u and R_v. We have $Lv \subset S$ by Lemma 81. What is left to prove is the following: for $c \in M$, show $cL_1 \subset N$ and $cL_{-1} \subset V$. For the first we take any $a \in L_1$ and have to prove $(ac)'=0$. Now $a'a=(a+c)'(a+c)=0$ by Lemma 79. Since $c'=0$, we get $a'c=0$, whence $(ac)'=0$. Next take $x \in L_{-1}$. By Lemma 80, there exists an element b in L_1 with $b' \neq 0$. We note that $bc \in N$, $bc \cdot x \in M$ by two applications of what we have just proved. Apply the Jacobi identity to b, c, x. The term $bx \cdot c$ lies in M. Hence so does $cx \cdot b$. This means $cx \in V$, as required.

We conclude this section with an example showing the failure of Theorem 6 for characteristic 3. (That Theorem 6 fails for characteristic 2 is quite evident; indeed in the case of characteristic 2, one expects all roots to be isotropic. It should also be noted that Theorem 6 survives if the form is assumed to come from a restricted representation; the proof of Theorem 4.2 in [3] is valid.)

The example is 10-dimensional and has a 2-dimensional Cartan subalgebra with basis u, v. If we write α for the root which is 1 on u, 0 on v and β for the root which is 0 on u, 1 on v, the list of roots and corresponding root vectors reads: α, a; $-\alpha, b$; β, c; $-\beta, d$; $\alpha+\beta, e$; $-\alpha-\beta, f$; $\alpha-\beta, g$; $\beta-\alpha, h$. The products are as follows: $ac=bd=be=cf=de=0$, $ab=v$, $ad=g$, $ag=-f$, $ah=-c$, $bc=h$, $bf=-g$, $bg=-d$, $bh=e$, $cd=u$, $ce=g$, $cg=a$, $ch=-f$, $df=-h$, $dg=e$, $dh=b$, $ef=u+v$, $eg=b$, $eh=d$, $fg=-c$, $fh=-a$, $gh=v-u$. The roots $\pm\alpha$, $\pm\beta$ are isotropic and the remaining ones nonisotropic. The form is given by $-f(u,v)=f(a,b)=f(c,d)=f(e,f)=f(g,h)=1$, with all other inner products vanishing. The algebra is simple and restricted.

15. **Rank two, characteristic two.** Without any assumption of an invariant form, we can give a complete classification of the simple restricted Lie algebras of rank two and characteristic two. It is not surprising that quadratic forms admitting composition play a role in the proof, for Lie algebras of characteristic two resemble Jordan algebras in many ways.

THEOREM 11. *Let L be a simple restricted Lie algebra of rank two over an algebraically closed field of characteristic two. Then the dimension of L is* 8, 14, *or* 26, *and in each case L is uniquely determined.*

By Theorem 10, a Cartan subalgebra H of L has basis u, v satisfying $u^2=u$, $v^2=v$. There are (possibly) three root spaces which we label A, B, C; on A, R_u is 1, R_v is 0; on B, R_u is 0, R_v is 1; on C, R_u and R_v are both 1.

LEMMA 82. *If $x \in A$ (resp. B, C) then x^2 is a scalar multiple of v (resp. u, $u+v$).*

Proof. Assume $x \in A$. We have $x^2 \in H$ and $xx^2 = xR_x^2 = 0$. The only elements of H annihilating a nonzero element of A are the scalar multiples of v. The proof is similar if x lies in B or C.

For any x in A we define $g(x)$ by the equation $x^2=g(x)v$. Manifestly g is a quadratic form on A. We define g similarly on B and C. If f is the corresponding bilinear form, then $xy=f(x, y)v$ for x and y in A; similarly for B and C. There is no need for us to attempt to extend g or f beyond $A\cup B\cup C$.

LEMMA 83. *If x and y lie in $A\cup B\cup C$, but are not both in the same set,* $g(xy)=g(x)g(y)$.

Proof. Assume for definiteness that x lies in A and y in B. Then xy lies in C and $(xy)^2=g(xy)(u+v)$. To evaluate $g(xy)$ it suffices to test $(xy)^2$ on x. Now $x\cdot xy=yR_x^2=g(x)y$; $y\cdot xy=xR_y^2=g(y)x$. Hence $x\cdot(xy)^2=g(x)g(y)x$. This shows that $g(xy)=g(x)g(y)$.

LEMMA 84. *If $a\in A$, $b\in B$, $c\in C$, then $f(ab, c)=f(bc, a)=f(ca, b)$.*

Proof. By the Jacobi identity $ab\cdot c+bc\cdot a+ca\cdot b=0$. We thus have scalar multiples of $u+v$, v, and u adding up to 0. This is possible only if all three coefficients are equal.

LEMMA 85. *The form f is nonsingular on A (or B or C).*

Proof. Define A_0 to be the subset of A annihilating A. Define B_0, C_0 similarly. We claim that $A_0+B_0+C_0$ is an ideal in L. Invariance under R_u and R_v is trivial. The typical thing that remains to be proved is $A_0B\subset C_0$, that is, $A_0B\cdot C=0$. Since $A_0\cdot BC=0$, this is immediate from Lemma 84. By the simplicity of L, $A_0=0$, as required.

We now introduce a new multiplication in A. Fix elements $b\in B$, $c\in C$ with $g(b)=g(c)=1$. For r, $s\in A$ define $r*s=rb\cdot sc$.

LEMMA 86. *Under this multiplication A has a two-sided unit element. Also,* $g(r*s)=g(r)g(s)$.

Proof. The unit element is given by $a=bc$. For $ac=bR_c^2=b$, $r*a=rb\cdot ac=rR_b^2=r$. Similarly, $ab=c$, $a*s=s$. That $g(r*s)=g(r)g(s)$ follows from repeated application of Lemma 83.

On A we thus have a quadratic form admitting composition, in exactly the way this is formulated in [2]. Hence the dimension of A is 2, 4, or 8. Moreover the multiplication and quadratic form are uniquely determined in each case. The rest of the structure of L can be reconstructed from this information. Three instances of this will suffice: (1) products BB, (2) products AB, (3) products BC.

(1) Since R_c maps A onto B, a typical product in BB has the form $rc\cdot sc$ (r, $s\in A$). By Lemma 84, $rc\cdot sc$ can be determined from $r(sc\cdot c)=rs$.

(2) A typical product in AB has the form $r\cdot sc$ (r, $s\in A$). To identify $r\cdot sc$ it suffices to know its product with b (since R_b maps C one-to-one onto A). Now $(r\cdot sc)b=rb\cdot sc+r(sc\cdot b)=r*s+r(sc\cdot b)$. The scalar $sc\cdot b$ is known from (1).

(3) A product in BC is $rb \cdot sc$ which is simply $r*s$.

We remark finally that these three algebras have concrete realizations as follows: the 8-dimensional one is all 3 by 3 matrices of trace 0; the 14-dimensional one is all 4 by 4 matrices of trace 0, modulo scalars; the 26-dimensional one is the cube $[[AA]A]$ of the algebra A of 8 by 8 skew-symplectic matrices, modulo scalars.

Added in proof (September 5, 1958). By a supplement to Lemma 48, I have checked that Theorem 7 is also valid for characteristic 5.

I take this opportunity to announce some further results. Assume characteristic at least 5 throughout.

1. If in a simple Lie algebra L of rank one all root spaces are one-dimensional, then either L is three-dimensional or the roots form a group.

2. In a simple restricted Lie algebra any three-dimensional Cartan subalgebra is abelian.

3. Assume that L admits a nonsingular form and that the root space L_α is not one-dimensional. Then α is isotropic.

4. If in addition L is simple then either all roots are nonisotropic (and L is of the type classified by Seligman) or all are isotropic.

BIBLIOGRAPHY

1. N. Jacobson, *Commutative restricted Lie algebras*, Proc. Amer. Math. Soc. vol. 6 (1955) pp. 476–481.

2. I. Kaplansky, *Infinite-dimensional quadratic forms admitting composition*, Proc. Amer. Math. Soc. vol. 4 (1953) pp. 956–960.

3. G. Seligman, *On Lie algebras of prime characteristic*, Memoirs Amer. Math. Soc., no. 19, New York, 1956.

4. H. Zassenhaus, *Über Lie'sche Ringe mit Primzahlcharacteristik*, Abh. Math. Sem. Univ. Hamburg vol. 13 (1939) pp. 1–100.

UNIVERSITY OF CHICAGO,
CHICAGO, ILL.
PRINCETON UNIVERSITY,
PRINCETON, N. J.