ON LIE ALGEBRAS OF RANK ONE(1)

BY
RICHARD E. BLOCK

1. **Introduction.** Let F be an algebraically closed field of characteristic $p > 3$. Aside from the 3-dimensional simple algebra, every known simple Lie algebra over F of rank one is an Albert-Zassenhaus algebra. By an Albert-Zassenhaus algebra (over F) we mean an algebra over F with a basis $\{u_\alpha \mid \alpha \in G\}$, where G is a finite additive subgroup of F, and with multiplication

$$u_\alpha u_\beta = \{\alpha h(\beta) - \beta h(\alpha) + \alpha - \beta\} u_{\alpha+\beta}, \qquad \alpha, \beta \in G \tag{1.1}$$

where h is any additive mapping of G into F (see [1, p. 138]). Each of these algebras is a simple Lie algebra, for which u_0 spans a one-dimensional Cartan subalgebra, with one-dimensional root spaces spanned by the u_α. We shall prove that under certain hypotheses, these are the only Lie algebras over F of rank one.

Kaplansky in [5] has proved that any restricted simple Lie algebra over F of rank one is either 3-dimensional or the Witt algebra. He has also obtained a number of results on (not necessarily restricted) Lie algebras of rank one, and in particular has proved [5, Theorem 4] that if L is a Lie algebra of dimension > 3 over F, and if L has a one-dimensional Cartan subalgebra such that multiplication between L_α and $L_{-\alpha}$ is nondegenerate for every nonzero root α (i.e., no nonzero element of a root space L_α annihilates all of $L_{-\alpha}$), then all root spaces are one-dimensional and the roots form a group under addition. The result we shall obtain is the following:

THEOREM. *Let L be a Lie algebra of dimension greater than three over an algebraically closed field F of characteristic $p > 3$. Suppose L has a one-dimensional Cartan subalgebra such that, for every nonzero root α, multiplication between L_α and $L_{-\alpha}$ is nondegenerate. Then L is an Albert-Zassenhaus algebra.*

It is easy to see, conversely, that any Albert-Zassenhaus algebra over F satisfies the hypotheses of the theorem. Although certain parameters are used in (1.1) in the definition of Albert-Zassenhaus algebras, it is conceivable that there are only finitely many nonisomorphic Albert-Zassenhaus algebras over F for each dimension p^n. Indeed, this has been proved by Ree [6] for the Zassenhaus algebras (those algebras defined by (1.1) for which $\alpha h(\beta) - \beta h(\alpha)$ vanishes identically).

Presented to the Society, October 25, 1958; received by the editors May 23, 1959.
(1) This research was supported by the Office of Naval Research.

Even if the 7-dimensional algebra is taken into account, our theorem does not hold for characteristic $p = 3$, as may be seen by considering some of the simple algebras of dimension $p^n - 2$ discussed in [2].

2. **Preliminary remarks and notation.** The proof of the theorem will be given in a series of lemmas. Let L satisfy the hypotheses of the theorem, and let u_0 be a nonzero element of the one-dimensional Cartan subalgebra. By identifying any root for this Cartan subalgebra with its value on u_0, we may consider the roots to be elements of F. The scalar α representing a given nonzero root may be changed to 1 by changing u_0; it will be convenient to make this change in the proofs of certain lemmas. However, *in the statements of all lemmas, we shall regard* u_0 *as being fixed*, and hence *the scalars representing roots also remain fixed.*

By the results of Kaplansky mentioned above, the root spaces are one-dimensional and the roots form a group G. For each nonzero root α let u_α be a nonzero element in the root space L_α. Then $\{u_\alpha \mid \alpha \in G\}$ is a basis of L, and for any roots α and β,

$$u_\alpha u_\beta = n_{\alpha\beta} u_{\alpha+\beta},$$

where $n_{\alpha\beta} \in F$. Obviously, for any roots α, β and γ, we have

$$n_{\alpha,0} = \alpha, \qquad n_{\alpha\beta} = -n_{\beta\alpha}$$

and, by the Jacobi identity,

$$n_{\alpha\beta} n_{\alpha+\beta,\gamma} + n_{\beta\gamma} n_{\beta+\gamma,\alpha} + n_{\gamma\alpha} n_{\gamma+\alpha,\beta} = 0. \tag{2.1}$$

Also, if $\alpha \neq 0$ then $n_{\alpha,-\alpha} \neq 0$.

Of course the scalars $n_{\alpha\beta}$ depend on the particular basis $\{u_\beta\}$ chosen; in what follows, it will always be clear what basis is being used to determine the $n_{\alpha\beta}$. Our aim is to show that this basis may be chosen so that (1.1) holds. It may easily be shown [1, p. 133] by using the Jacobi identity that, in order for (1.1) to hold, it is sufficient for there to exist a skew-symmetric biadditive mapping f from $G \times G$ to F such that

$$n_{\alpha\beta} = f(\alpha,\beta) + \alpha - \beta \qquad (\alpha,\beta \in G). \tag{2.2}$$

In fact, for such a mapping f, we may take $h(\alpha) = -\gamma^{-1} f(\alpha,\gamma)$ for any fixed nonzero γ in G.

We shall call roots *independent* if they are linearly independent over the prime field F_p. Also, F_p^* will denote the set of nonzero elements of F_p.

3. **Representations of the Witt algebra.**

LEMMA 3.1. *For any root* β, *the elements* $u_{i\beta}$, $i \in F_p^*$, *may be chosen, in one and only one way, so that*

$$n_{i\beta,j\beta} = (i-j)\beta, \qquad i,j \in F_p. \tag{3.1}$$

Proof. We assume without loss of generality that $\beta = 1$. It follows from Lemma 37 of [5] or [7, pp. 42–43] that L_i does not annihilate L_j if $j \neq i, -2i$. Since $-2(-2i) \neq i$ if $i \neq 0$, it follows that $L_iL_j \neq 0$ if $i \neq j$. The existence of elements u_i such that (3.1) holds then follows from [7, pp. 45–47]. The uniqueness is trivial.

Now take a fixed nonzero root β and suppose the elements $u_{i\beta}$ have multiplication given by (3.1). Thus

$$W = \sum_{i \in F_p} L_{i\beta}$$

is a p-dimensional subalgebra of L isomorphic to the Witt algebra. As is well known, the Witt algebra W also has a basis $e_{-1}, e_0, \cdots, e_{p-2}$ with multiplication

$$e_ie_j = (i-j)e_{i+j} \quad \text{if} \quad i+j \leqq p-2,$$

$$e_ie_j = 0 \quad \text{if} \quad i+j > p-2,$$

where in fact we may take

$$e_{-1} = \beta^{-1}u_{-\beta}, \quad e_0 = \beta^{-1}(u_0 - u_{-\beta}).$$

Let α be any root such that α and β are independent. Then

$$M = \sum_{i \in F_p} L_{\alpha+i\beta}$$

is a p-dimensional representation space for a representation $\sigma = \sigma(\alpha,\beta,L)$ of W, the transformation x^σ of M ($x \in W$) being the right multiplication of x on M. Let I denote the identity transformation of M.

LEMMA 3.2. *There is a scalar $\varepsilon_{-1} = \varepsilon_{-1}(\sigma)$ such that $(e_{-1}^\sigma)^p = \varepsilon_{-1}I$. Let ζ be a given scalar, with $\zeta \neq$ (resp. $=$) $(\alpha/\beta)^p - (\alpha/\beta)$. Then there are at most p (resp. $p-1$) inequivalent representations τ of the Witt algebra for which there is an algebra L_τ, satisfying the hypotheses of the theorem, such that $\tau = \sigma(\alpha,\beta,L_\tau)$ and $\varepsilon_{-1}(\tau) = \zeta$.*

Proof. We may again assume that $\beta = 1$. Let M_0 be an irreducible subspace of M. We write E, E_{-1}, E_0, U_0 for the restrictions to M_0 of $I, e_{-1}^\sigma (= u_{-1}^\sigma), e_0^\sigma, u_0^\sigma$, respectively. By Theorem 1 of [3] there exist scalars ε_{-1} and ε_0 such that

$$E_{-1}^p = \varepsilon_{-1}E, \quad E_0^p - E_0 = \varepsilon_0 E. \tag{3.2}$$

Since $E_0 = U_0 - E_{-1}$, we have [4, p.16]

$$E_0^p = U_0^p - E_{-1}^p + \sum_{i=1}^{p-1} s_i,$$

where $(p-i)s_i$ is the coefficient of λ^{p-i-1} in the $(p-1)$-fold commutator

$$[\cdots[U_0, \lambda U_0 - E_{-1}], \cdots, \lambda U_0 - E_{-1}].$$

But $[U_0, E_{-1}] = E_{-1}$, so $s_i = 0$ if $i \neq 1$, and $s_1 = -E_{-1}$. Hence

$$E_0^p - E_0 = U_0^p - E_{-1}^p - U_0.$$

But for any v in $L_{\alpha+i}$ we have $v\{(u_0^\sigma)^p - u_0^\sigma\} = (\alpha^p - \alpha)v$. Thus $E_0^p - E_0 = (\alpha^p - \alpha - \varepsilon_{-1})E$, so

$$\varepsilon_0 = \alpha^p - \alpha - \varepsilon_{-1}. \tag{3.3}$$

In particular not both ε_{-1} and ε_0 are zero. Chang considered all irreducible representations of degree $\leqq p\,(p>3)$ of the Witt algebra, in Hauptsatz 2′ of [3]. He showed that for any given values of his invariants $\varepsilon_{-1}, \varepsilon_0$, defined as in (3.2), if $\varepsilon_0 \neq 0$ (resp. $\varepsilon_0 = 0, \varepsilon_{-1} \neq 0$), then there are exactly p (resp. $p-1$) inequivalent irreducible representations of rank p of the Witt algebra, and no representations of lower rank. Hence in our case it follows from (3.3) that $M_0 = M$ and that the lemma holds.

We shall now use the Albert-Zassenhaus algebras to exhibit explicitly all the representations σ of W which may occur. If the multiplication in L were given by (1.1), then we would have

$$\begin{aligned} \varepsilon_{-1} &= \beta^{-p} \prod_{j \in F} (-\eta + \alpha + j\beta) \\ &= \beta^{-p}(-\eta + \alpha)^p - \beta^{-1}(-\eta + \alpha), \end{aligned} \tag{3.4}$$

where η denotes $\alpha h(\beta) - \beta h(\alpha)$. Now let a value of ε_{-1} in F be given and suppose that η in F satisfies (3.4). Then for any i, $\eta + i\beta$ also satisfies (3.4). But for any i, there obviously is an Albert-Zassenhaus algebra having α and β as roots such that $\alpha h(\beta) - \beta h(\alpha) = \eta + i\beta$. This of course gives rise to an irreducible representation of W, denoted by $\sigma(\eta + i\beta)$, whose invariant ε_{-1} has the given value (here we are identifying W with the subalgebra spanned by the $u_{i\beta}$ in the Albert-Zassenhaus algebra).

LEMMA 3.3. *The representations $\sigma(\eta)$ and $\sigma(\eta + i\beta)$, $i \neq 0$, are equivalent if and only if the sets $\{\eta, \eta + i\beta\}$ and $\{\beta, 2\beta\}$ coincide. The invariant ε_{-1} of $\sigma(\eta)$ equals $(\alpha/\beta)^p - (\alpha/\beta)$ if and only if $\eta = j\beta$ for some integer j.*

Proof. We may assume that $\beta = 1$. Suppose that $\sigma(\eta)$ and $\sigma(\eta + i)$, $i \neq 0$, are equivalent. For $j = 0, i$, let v_j be a nonzero characteristic vector of $u_0^{\sigma(\eta+j)}$ with characteristic root α. Thus $v_j = c_j u_\alpha$ for some c_j in F, so that

$$(v_j u_1)u_{-1} = (\eta + j + \alpha - 1)(-\eta - j + \alpha + 2)v_j.$$

Since the coefficients on the right must be equal for $j = 0, i$, we have $0 = -i(2\eta + i - 3)$, and $\eta = (3-i)/2$. The coefficient of v_j in $((v_j u_1)u_1)u_{-2}$ is

$$(\eta + j + \alpha - 1)(\eta + j + \alpha)(-2\eta - 2j + \alpha + 4).$$

Again we may equate the expressions for $j = 0, i$. A straightforward computation then shows that $0 = -i(i-1)(i+1)$, so that $i = 1$ or -1. But if $i = 1$ then $\eta = 1$ and $\eta + i = 2$, while if $i = -1$ then $\eta = 2$ and $\eta + i = 1$. This proves one direction of the lemma's first statement. The final statement of the lemma follows from (3.4). The other direction of the first statement then follows from Lemma 3.2 (or may easily be proved directly).

Now by Lemmas 3.2 and 3.3, there is a scalar η such that the representation σ of W on M is equivalent to $\sigma(\eta)$. By Lemma 3.3, η is uniquely determined by σ except in one case. Let A be the Albert-Zassenhaus algebra used in defining $\sigma(\eta)$. Any $u_{\alpha+i\beta}$ in A, being a characteristic vector of $u_0^{\sigma(\eta)}$, corresponds, under an equivalence of σ and $\sigma(\eta)$, to an element of $L_{\alpha+i\beta}$. Thus we have proved the following lemma.

LEMMA 3.4. *Let α and β be independent roots. Then there is a scalar η and a choice of the basis elements $u_{i\beta}$, $u_{\alpha+i\beta}$ $(i \in F_p)$ such that* (3.1) *holds and*

$$n_{\alpha+i\beta,j\beta} = j\eta + \alpha + (i-j)\beta, \qquad i,j \in F_p. \tag{3.5}$$

Moreover η is uniquely determined unless η has one of the values $\beta, 2\beta$, in which case it may also be chosen to have the other of the two values (with respect to a suitable basis).

We now define a mapping f of pairs of roots into F. If α and β are dependent, we set $f(\alpha,\beta) = 0$. For any independent α, β, if the value of η in Lemma 3.4 is neither β nor 2β, we set $f(\alpha,\beta) = \eta$. We shall complete the definition of f in §6. Until then, with one exception explicitly mentioned in the proof of Lemma 5.4, we shall set $f(\alpha,\beta) = 2\beta$ in the case in which, in Lemma 3.4, η may be taken to be either β or 2β. Thus (3.5) becomes

$$n_{\alpha+i\beta,j\beta} = jf(\alpha,\beta) + \alpha + (i-j)\beta, \qquad i,j \in F_p. \tag{3.6}$$

Obviously, for any α,β,

$$f(\alpha + i\beta, j\beta) = jf(\alpha,\beta), \qquad i,j \in F_p. \tag{3.7}$$

Our aim is to complete the definition of f, and to show that then f is skew-symmetric, biadditive, and (with respect to a suitable basis) satisfies (2.2).

4. Properties of f.

LEMMA 4.1. *For any roots γ, δ and β, if $L_\gamma L_\delta \neq 0$ then*

$$f(\gamma + \delta, \beta) - f(\gamma,\beta) - f(\delta,\beta) = i\beta$$

for some i in F_p. For any roots α,β, and any j in F_p, there is an i in F_p such that

$$f(j\alpha,\beta) - jf(\alpha,\beta) = i\beta.$$

Proof. Suppose that $L_\gamma L_\delta \neq 0$. Choose a basis for L such that (3.1) and (3.6) hold for $\alpha = \gamma,\ \delta,\ \gamma+\delta$. Thus $u_\gamma u_\delta$ is a nonzero element of $L_{\gamma+\delta}$. Let D denote the pth power of the right multiplication by u_β. By (3.6),

$$\begin{aligned}(u_\gamma u_\delta)D &= \prod_{i\in F_p} \{f(\gamma+\delta,\beta) + \gamma + \delta + i\beta\}\, u_\gamma u_\delta \\ &= \{f(\gamma+\delta,\beta)^p + \gamma^p + \delta^p - [f(\gamma+\delta,\beta) + \gamma + \delta]\beta^{p-1}\}u_\gamma u_\delta.\end{aligned}$$

But since D is a derivation,

$$\begin{aligned}(u_\gamma u_\delta)D &= (u_\gamma D)u_\delta + u_\gamma(u_\delta D) \\ &= \{f(\gamma,\beta)^p+\gamma^p-[f(\gamma,\beta)+\gamma]\beta^{p-1}+f(\delta,\beta)^p+\delta^p-[f(\delta,\beta)+\delta]\beta^{p-1}\}u_\gamma u_\delta.\end{aligned}$$

Hence $f(\gamma+\delta,\beta)$ is a root of the polynomial $x^p - x\beta^{p-1} - f(\gamma,\beta)^p + f(\delta,\beta)^p - [f(\gamma,\beta)+f(\delta,\beta)]\beta^{p-1}$. This polynomial has the p roots $f(\gamma,\beta)+f(\delta,\beta)+i\beta$, $i\in F_p$, so the first statement of the lemma is proved. Now $0 = f(0,\beta) = f(\alpha,\beta) + f(-\alpha,\beta) + i\beta$ for some i in F_p, and $f(\alpha,\beta) = f(2\alpha,\beta) + f(-\alpha,\beta) + k\beta$ for some k in F_p. It follows that the second statement of the lemma holds when $j = 2$. The general case then follows from the first statement of the lemma by induction.

LEMMA 4.2. *For any roots α and β, there is a j in F_p^* such that $(2\alpha,\beta) = jf(\alpha,\beta)$.*

Proof. We may assume that (3.6) holds. Formula (2.1), with $\alpha + i\beta$, α and $i\beta$ in place of α, β and γ, respectively, gives

$$n_{\alpha+i\beta,\alpha}\, n_{2\alpha+i\beta,i\beta} = n_{\alpha+i\beta,i\beta}\, n_{\alpha+2i\beta,\alpha}. \tag{4.1}$$

Suppose that for every i in F_p^* we have $f(i\beta,\alpha) \neq -i\beta$, so that $n_{\alpha+i\beta,\alpha} \neq 0$. Then we may take the product over i in F_p^* of both sides of (4.1) and cancel $\prod_i n_{\alpha+i\beta,\alpha}$, getting

$$\prod_{i\in F_p^*} n_{2\alpha+i\beta,i\beta} = \prod_{i\in F_p^*} n_{\alpha+i\beta,i\beta}.$$

By (3.6), the left side of this equals $(2\alpha)^{p-1} - f(2\alpha,\beta)^{p-1}$, while the right side equals $\alpha^{p-1} - f(\alpha,\beta)^{p-1}$. Thus $f(2\alpha,\beta)^{p-1} = f(\alpha,\beta)^{p-1}$, so the conclusion of the lemma holds for this case.

Now suppose that $f(k\beta,\alpha) = -k\beta$ for some k in F_p^*. In particular, α and β must then be independent. By Lemma 4.1, for any i in F_p^* there is an l such that $f(ik\beta,\alpha) = -ik\beta + l\alpha$. Then, by (3.7), for any $m \neq 1$ in F_p, we have $f(ik\beta, m\alpha) = -mik\beta + ml\alpha \neq -ik\beta$. Therefore the case of the lemma already proved may be applied to $m\alpha$ and β. Thus $f(2^n\alpha,\beta) = j_n f(2^{n-1}\alpha,\beta)$ for $2^{n-1} \equiv 2, 4, \cdots, (p+1)/2 \pmod p$, where $j_n \in F_p^*$. The conclusion of the lemma follows.

LEMMA 4.3. *Let α and β be independent roots. Then there may be chosen basis elements $u_{i\alpha+j\beta}$ $(i,j \in F_p)$, along with nonzero scalars c_{ij}, where $c_{i,0} = c_{0,i} = 1$, such that*

$$
\begin{aligned}
n_{i\alpha+j\beta,k\beta} &= kf(i\alpha,\beta) + i\alpha + (j-k)\beta, \\
n_{i\beta+j\alpha,k\alpha} &= \{kf(i\beta,\alpha) + (j-k)\alpha + i\beta\}c_{ij}\, c_{i,j+k}^{-1}, \qquad i,j,k \in F_p.
\end{aligned} \tag{4.2}
$$

If (4.2) *holds then*

$$
c_{ij}\{if(j\alpha,\beta) + j\alpha - i\beta\} = -jf(i\beta,\alpha) + j\alpha - i\beta, \qquad i,j \in F_p. \tag{4.3}
$$

Proof. Using Lemma 1, we choose basis elements $u_{i\alpha}$, $u_{i\beta}$ such that $n_{i\gamma,j\gamma} = (i-j)\gamma$ for all i, j in F_p and for $\gamma = \alpha, \beta$. Using Lemma 2, we choose a nonzero element $w_{i\alpha+j\beta}$ in $L_{i\alpha+j\beta}$ for each j and nonzero i in F_p, such that

$$
w_{i\alpha+j\beta}u_{k\beta} = \{kf(i\alpha,\beta) + i\alpha + (j-k)\beta\}w_{i\alpha+(j+k)\beta}, \qquad i,j,k \in F_p. \tag{4.4}
$$

If for some i and some scalar c, each $w_{i\alpha+j\beta}$ is replaced by $cw_{i\alpha+j\beta}$, then (4.4) remains unchanged. Hence we may assume that $w_{i\alpha} = u_{i\alpha}$ for each nonzero i and we then set $u_{i\alpha+j\beta} = w_{i\alpha+j\beta}$ for all i,j in F_p^*. Thus the first formula of (4.2) holds.

Now by symmetry we may choose a nonzero element $v_{i\alpha+j\beta}$ in each $L_{i\alpha+j\beta}$, where $v_{i\alpha} = u_{i\alpha}$ and $v_{i\beta} = u_{i\beta}$, such that (4.4) holds with v in place of w and with α and β interchanged. Now for any i and j, $u_{i\beta+j\alpha} = c_{ij}v_{i\beta+j\alpha}$ for some nonzero scalar c_{ij}. In particular $c_{i,0} = c_{0,i} = 1$ for any i. For these values of c_{ij}, the second formula of (4.2) follows immediately from new version of (4.4).

Now for any i and j,

$$
if(j\alpha,\beta) + j\alpha - i\beta = n_{j\alpha,i\beta} = -n_{i\beta,j\alpha} = -\{jf(i\beta,\alpha) - j\alpha + i\beta\}c_{ij}^{-1},
$$

which proves the last statement of the lemma.

LEMMA 4.4. *If α and β are nonzero roots such that $f(\alpha,\beta)/\beta \notin F_p^*$, then $f(2\alpha,\beta) = 2f(\alpha,\beta)$.*

Proof. By Lemma 4.1, $f(2\alpha,\beta) = 2f(\alpha,\beta) + i\beta$ for some i in F_p, and by Lemma 4.2, $f(2\alpha,\beta) = jf(\alpha,\beta)$ for some j in F_p. The lemma follows from this.

It should be noted that until the definition of f is completed, the conclusion of Lemma 4.4 will not always hold. This accounts for much of the difficulty encountered below.

LEMMA 4.5. *Let α,β be independent roots and i,j elements of F_p^* such that neither $f(j\alpha,\beta)/\beta$ nor $f(i\beta,\alpha)/\alpha$ is in F_p^*, and such that $0 \neq if(j\alpha,\beta) + j\alpha$, $jf(i\beta,\alpha) + i\beta$. Then* (4.2) *implies*

$$
c_{ij}c_{2i,2j} = c_{2i,j}c_{i,2j}. \tag{4.5}
$$

Proof. Suppose that (4.2) holds. Then (4.1), with $j\alpha$ in place of α, gives

$$\{jf(i\beta,\alpha)+i\beta\}c)_{ij}c_{i,2j}^{-1}\ \{if(2j\alpha,\beta)+2j\alpha\}$$
$$=\{if(j\alpha,\beta)+j\alpha\}\{jf(2i\beta,\alpha)+2i\beta\}c_{2i,j}c_{2i,2j}^{-1}.$$

Under the hypotheses of the lemma, (4.5) follows from this and Lemma 4.4.

5. **Conditions for f to be skew-symmetric.** In the proofs of this section we shall always assume that the basis elements $u_{i\alpha+j\beta}$ and scalars c_{ij} are chosen so that (4.2) holds.

LEMMA 5.1. *Let α,β be independent roots such that neither $f(\alpha,\beta)/\beta$ nor $f(\beta,\alpha)/\alpha$ is in F_p^*. Then $f(\alpha,\beta)=-f(\beta,\alpha)$.*

Proof. By (3.7) and Lemma 4.4, it is enough to prove the lemma for some $2^i\alpha$ and $2^j\beta$ in place of α and β. Now suppose that α and β satisfy the hypotheses. Note that $f(\alpha,2^i\beta)=-\alpha$ for at most one value of 2^i, so by a change of notation we may assume that this value is neither 1 nor 2, i.e.,

$$f(\alpha,\beta)+\alpha\neq 0,\qquad f(2\alpha,2\beta)+2\alpha\neq 0. \tag{5.1}$$

Similarly we may also assume that

$$f(\beta,\alpha)+\beta\neq 0,\qquad f(2\beta,2\alpha)+2\beta\neq 0, \tag{5.2}$$

if necessary by replacing α by $2^i\alpha$ for some i (this change does not affect (5.1)). Now by Lemma 4.5,

$$c_{11}c_{22}=c_{21}c_{12}. \tag{5.3}$$

In the remainder of the proof of this lemma, ζ and η denote $f(\alpha,\beta)$ and $f(\beta,\alpha)$ respectively. If $if(j\alpha,\beta)+j\alpha-i\beta=-jf(i\beta,\alpha)+j\alpha-i\beta$ for some $i,j=1,2$, then $\zeta=-\eta$. Hence by (4.3) we may assume that $c_{ij}=-(ij\eta-j\alpha+i\beta)(ij\zeta+j\alpha-i\beta)^{-1}$ for $i,j=1,2$. Then (5.3) is equivalent to

$$\begin{aligned}(\eta-\alpha+\beta)(2\eta-\alpha+\beta)(2\beta)\zeta+\alpha-2\beta)(2\zeta+2\alpha-\\ -(2\eta-\alpha+2\beta)(2\eta-2\alpha+\beta)(\zeta+\alpha-\beta)(2\zeta+\alpha-\beta)=0.\end{aligned} \tag{5.4}$$

Obviously (5.4) is satisfied if $\eta=-\zeta$. Consider the left side of (5.4) as a polynomial P in ζ and η over F. A simple computation shows that the coefficient of $\zeta^2\eta$ in P vanishes, and that the coefficient of ζ does not vanish. Hence (5.4) becomes

$$(\zeta+\eta)(a_1\zeta+a_2\eta+a_3)=0, \tag{5.5}$$

where a_1, a_2, a_3 are in F and $a_3\neq 0$. But using the second halves of (5.1) and (5.2), we may replace α by 2α and β by 2β in the above argument. This change requires also that $\zeta=f(\alpha,\beta)$ be replaced by 4ζ, and $\eta=f(\beta,\alpha)$ by 4η. For (5.4), these changes are equivalent to just replacing ζ by 2ζ and η by 2η. Thus (5.5) becomes

$$2(\zeta + \eta)(2a_1\zeta + 2a_2\eta + a_3) = 0.$$

Comparing this with (5.5) we get $\eta = -\zeta$, and the lemma is proved.

In the remainder of this section we shall determine conditions under which the hypotheses of Lemma 5.1 hold. For any t in F_p we shall write

$$t' = (t-2)(t-1).$$

Thus for t_1, t_2 in F_p, $t_1' = t_2'$ if and only if $t_2 = 3 - t_1$ or $t_2 = t_1$.

LEMMA 5.2. *Let α and β be independent roots and suppose that for each i in F_p^*, $f(i\alpha,\beta) = r_i\beta$ and $f(i\beta,\alpha) = s_i\alpha$, where r_i, s_i are in F_p. Then for each i in F_p^*, $r_i' = r'_{-i}$ and $s_i' = s'_{-i}$.*

Proof. Under the given hypotheses we obtain from (4.2) and (2.1), with α,β,γ replaced by $i\alpha + i\beta$, $-i\beta$, $-i\alpha$ respectively,

$$(-ir_i\beta + i\alpha + 2i\beta)(2i\alpha) + (-ir_{-i}\beta + i\beta - i\alpha)n_{i\alpha+i\beta,\,-i\alpha-i\beta} - (-is_i\alpha + 2i\alpha + i\beta)c_{ii}(2i\beta) = 0.$$

Hence, by (4.3),

$$(-r_{-i}\beta - \alpha + \beta)(r_i\beta + \alpha - \beta)n_{i\alpha+i\beta,\,-i\alpha-i\beta} = -2i\alpha(-r_i\beta + \alpha + 2\beta)(r_i\beta + \alpha - \beta) - 2i\beta(-s_i\alpha + 2\alpha + \beta)(s_i\alpha - \alpha + \beta).$$

Replacing i by $-i$ in this equation and noting that the left side of the new equation is the negative of that of the old, we see that

$$\alpha[(2-r_i)\beta + \alpha][(r_i - 1)\beta + \alpha] + \beta[(2-s_i)\alpha + \beta][(s_i - 1)\alpha + \beta]$$

equals the expression obtained from itself by replacing i by $-i$. Hence $r_i'\beta + s_i'\alpha = r'_{-i}\beta + s'_{-i}\alpha$, and the conclusion follows from the independence of α and β.

LEMMA 5.3. *Let the hypotheses of Lemma 5.2 hold and suppose moreover that $\alpha^4/\beta^4 \notin F_p$. Then for any i,j in F_p^*,*

$$(2s_{2j}' - 4)i^4\alpha^4 + Q(r_i, r_{-i}, s_{2j}')(i\alpha j\beta)^2 + 8(r_i + r_{-i})(r_i - 1)(r_{-i} - 1)j^4\beta^4 = 0, \tag{5.6}$$

where $Q = Q(\xi_1,\xi_2,\xi_3)$ is a certain polynomial (not depending on i,j) in three variables with coefficients in F_p.

Proof. For any i,j in F_p^*, (2.1) with α,β,γ replaced by $i\alpha + j\beta, j\beta, -i\alpha$ respectively, gives

$$(jr_i\beta + i\alpha)(-is_{2j}\alpha + 2i\alpha + 2j\beta)c_{2j,i} + (jr_{-i}\beta - i\alpha - j\beta)n_{i\alpha+j\beta,\,-i\alpha+j\beta} = 0$$

By (4.3) this gives

$$n_{i\alpha+j\beta,-i\alpha+j\beta} = (jr_i\beta + i\alpha)(4j^2\beta^2 + 2ij\alpha\beta - s'_{2j}i^2\alpha^2) \cdot [j(r_{-i}-1)\beta - i\alpha]^{-1}[2j(r_i-1)\beta + i\alpha]^{-1}. \tag{5.7}$$

If i is replaced by $-i$ in (5.7), the left side is merely replaced by its negative. Thus if we equate the right side of (5.7) with the negative of the expression obtained from itself by replacing i by $-i$, we get an equation in α and β. By an elementary computation, omitted here, this last mentioned equation reduces to

$$S_{ij} + (r_i - r_{-i})[(r_i + r_{-i} + 1)s'_{2j} - 8]i^3\alpha^3 j\beta + 4(r_i - r_{-i})(r_i r_{-i} - 2r_i - 2r_{-i})i\alpha j^3\beta^3 = 0, \tag{5.8}$$

where S_{ij} denotes the left side of (5.6), with Q as described in the lemma. By Lemma 5.2, $S_{ij} = S_{i,-j}$. Hence, by replacing j by $-j$ in (5.8) and adding, we obtain (5.6).

LEMMA 5.4. *If the hypotheses of Lemma* 5.3 *hold, then* $r_j = s_j = 0$ *for all* j *in* F_p^*.

Proof. Suppose that the hypotheses of Lemma 5.3 hold and that $r_i \neq 0$ for some i. It then follows from Lemma 5.2 that $r_i + r_{-i} \neq 0$. Also $1 \neq r_i, r_{-i}$, since, in the (temporary) definition of f, we assumed that for any nonzero roots γ and δ, $f(\gamma,\delta) \neq \delta$. Hence, for any j in F_p^*, the coefficient of β^4 in (5.6) does not vanish. Now if $s'_{2j} = 2$ for some j, then by (5.6), $\beta^2/\alpha^2 \in F_p$, a contradiction. Therefore for any j, $s'_j \neq 2$, so that $s_j \neq 0, 3$. If $f(i\alpha,\beta) = 2\beta$ then by Lemma 3.4 we may change notation and instead take $f(i\alpha,\beta) = \beta$, i.e., $r_i = 1$; this change does not alter any s_j. In that case (5.6) remains valid and implies that $\alpha^2/\beta^2 \in F_p$, a contradiction. Hence $r_i \neq 1, 2$, so by symmetry, for any j in F_p^*, $s_j \neq 1, 2$.

Thus we have proved

$$\{s_j \mid j \in F_p^*\} \leqq \{4, 5, \cdots, p-1\}. \tag{5.9}$$

Note that the coefficient of $\alpha^2\beta^2$ in (5.6) is nonzero since otherwise $\alpha^4/\beta^4 \in F_p$. Now if $s'_{2j} = s'_{2k}$ for some j, k in F_p^*, then $j = \pm k$, since, otherwise, replacing j by k in (5.6) and subtracting, we would get $\alpha^2/\beta^2 \in F_p$. Hence the set $\{s'_1, s'_2 \cdots, s'_{p-1}\}$ has $(p-1)/2$ elements. But $\{4', 5', \cdots, (p-1)'\}$ contains fewer than $(p-1)/2$ elements, since if $k \in \{4, 5, \cdots, p-1\}$ then $3-k$ is also in this subset of F_p, and $(3-k)' = k'$, while $k = 3-k$ only for one element of F_p. This contradicts (5.9). Therefore, under the hypotheses of Lemma 5.3, $r_j = 0$ for all j in F_p^*. By symmetry the same conclusion holds for all s_j, and the lemma is proved.

We now define a relation R in the set of nonzero roots by writing $\alpha R \beta$ if, for each i in F_p^*, $f(i\alpha,\beta)/\beta \notin F_p^*$. We also write $\alpha R' \beta$ if we do not have $\alpha R \beta$. By (3.7), if $\alpha R \beta$ then $(i\alpha + j\beta) R (k\beta)$ for any i, j, k in F_p^*.

LEMMA 5.5. *If* α *and* β *are nonzero roots such that* $\alpha^4/\beta^4 \notin F$, *then either* $\alpha R \beta$ *or* $\beta R \alpha$.

Proof. If $f(i\alpha,\beta)/\beta \notin F_p$ for some i, then, by Lemma 4.1, $\alpha R\beta$. Similarly, $\beta R\alpha$ if $f(i\beta,\alpha)/\alpha \notin F_p$ for some i. But if $\alpha^4/\beta^4 \notin F_p$ and if $f(i\alpha,\beta)/\beta$, $f(i\beta,\alpha)/\alpha$ are in F_p for all i, then $\alpha R\beta$ and $\beta R\alpha$ by Lemma 5.4.

LEMMA 5.6. *In the additive subgroup of roots generated by any two independent roots, there exist independent roots α and β for which $\alpha R\beta$ and $\beta R\alpha$.*

Proof. Let γ,δ be any independent roots. First note that there is some k in F_p^* such that $(k\gamma+\delta)^4/\delta^4 \notin F_p$. Indeed if $(k\gamma+\delta)^4/\delta^4 \in F_p$ for $k = \pm 1, \pm 2$, then, by replacing k by $-k$ and subtracting, we have $(k^3\gamma^3\delta + k\gamma\delta^3)/\delta^4 \in F_p$ for $k = 1,2$, whence $\gamma/\delta \in F_p$, a contradiction. Hence without loss of generality we may assume that $\gamma^4/\delta^4 \notin F_p$, with, say, $\delta R\gamma$. Suppose that $\gamma R'\delta$. Pick k in F_p^* such that $(k\gamma+\delta)^4/\delta^4 \notin F_p$. Then also $(k\gamma+\delta)R'\delta$, so by Lemma 5.5, $\delta R(k\gamma+\delta)$ and hence $(-k\gamma)R(k\gamma+\delta)$. But $(k\gamma+\delta)R(-k\gamma)$ also since $\delta R\gamma$. Hence we may take $\alpha = -k\gamma$ and $\beta = k\gamma+\delta$, and the lemma is proved.

6. Determination of the multiplication.

LEMMA 6.1. *Let α and β be independent roots such that $\alpha R\beta$ and $\beta R\alpha$. Then the basis element $u_{i\alpha+j\beta}$ may be chosen so that*

$$n_{i\alpha+j\beta,k\alpha+l\beta} = (il-jk)f(\alpha,\beta) + (i-k)\alpha + (j-l)\beta, \qquad i,j,k,l \in F_p. \tag{6.1}$$

Proof. Suppose that α and β satisfy the hypotheses. By (3.7) and Lemma 5.1 $f(i\alpha,\beta) = if(\alpha,\beta) = -if(\beta,\alpha) = -f(i\beta,\alpha)$ for any i. Let the elements $u_{i\alpha+j\beta}$ be chosen so that (4.2) holds. By (4.3), $c_{ij} = 1$ except possibly when $0 = ijf(\alpha,\beta) + j\alpha - i\beta$, $0 \neq i,j$. In the latter case, $if(j\alpha,\beta) + j\alpha$, $jf(i\beta,\alpha) + i\beta$ and $klf(\alpha,\beta) + l\alpha - k\beta$ are nonzero for $(k,l) = (2i,2j)$, $(2i,j)$, $(i,2j)$, and by Lemma 4.5, $c_{ij} = 1$. Hence (4.2) becomes

$$\begin{aligned} n_{i\alpha+j\beta,k\beta} &= ikf(\alpha,\beta) + i\alpha + (j-k)\beta, \\ n_{i\alpha+j\beta,k\alpha} &= -jkf(\alpha,\beta) + (i-k)\alpha + j\beta, \qquad i,j,k \in F_p. \end{aligned} \tag{6.2}$$

By (2.1),

$$\begin{aligned} n_{i\alpha,j\beta}n_{i\alpha+j\beta,k\alpha+l\beta} + n_{j\beta,k\alpha+l\beta}n_{k\alpha+(j+l)\beta,i\alpha} \\ + n_{k\alpha+l\beta,i\alpha}n_{(i+k)\alpha+l\beta,j\beta} = 0, \qquad i,j,k,l \in F_p. \end{aligned} \tag{6.3}$$

For a given value of $f(\alpha,\beta)$, (6.3) and (6.2) uniquely determine $n_{i\alpha+j\beta,k\alpha+l\beta}$ unless

$$0 = n_{i\alpha,j\beta} = ijf(\alpha,\beta) + i\alpha - j\beta. \tag{6.4}$$

But also $n_{k\alpha+l\beta,i\alpha+j\beta}$ is uniquely determined unless

$$0 = klf(\alpha,\beta) + k\alpha - l\beta. \tag{6.5}$$

Suppose that (6.4) and (6.5) hold, and that $0 \neq i,j,k,l$. Now $kl = mij$ $(m \in F_p)$,

whence, by (6.4) and (6.5), $mi\alpha - mj\beta = k\alpha - l\beta$, $mi = k$ and $mj = l$, so that $m = 1$ and $n_{i\alpha+j\beta,k\alpha+l\beta} = 0$.

For any value of $f(\alpha,\beta)$, there is an Albert-Zassenhaus algebra A having α and β as roots such that $\alpha h(\beta) - \beta h(\alpha) = f(\alpha,\beta)$. Since all $n_{i\alpha+j\beta,k\alpha+l\beta}$ are determined by $f(\alpha,\beta)$, they must coincide with the corresponding structure constants of A, so that (6.1) holds and the lemma is proved.

We may now complete the definition of f. Let γ, δ be independent roots. By Lemmas 5.6 and 6.1, we may choose independent roots α,β in the subgroup of roots generated by γ, δ, such that (6.1) holds. Let A be the Albert-Zassenhaus algebra used in the proof of Lemma 6.1. It follows from the definition of f that if $f(\gamma,\delta) \neq \delta, 2\delta$, then $f(\gamma,\delta) = \gamma h(\delta) - \delta h(\gamma)$. In the case in which $f(\gamma,\delta)$ could be either δ or 2δ, one of these two values equals $\gamma h(\delta) - \delta h(\gamma)$, and we now *define* $f(\gamma,\delta)$ *to be this value.* Then $f(\gamma,\delta) = -f(-\gamma,\delta)$, so the value of $f(\gamma,\delta)$ does not depend on the particular α,β chosen.

We now obviously have the following result.

LEMMA 6.2. *For any independent roots α and β, the conclusion of Lemma* 6.1 *holds.*

LEMMA 6.3. *For any roots α, β and γ,*

$$f(\alpha+\beta,\gamma) = f(\alpha,\gamma) + f(\beta,\gamma) + k_{\alpha\beta\gamma}\gamma \tag{6.6}$$

for some $k = k_{\alpha\beta\gamma}$ in F_p, where $k = 0$ if α,β,γ are dependent. Moreover, f is skew-symmetric.

Proof. By Lemmas 4.1 and 6.2, the only statement requiring proof is (6.6) in the case in which $L_\alpha L_\beta = 0$, $\alpha \neq \beta$. But then, with respect to a suitable basis, $n_{2\alpha,2\beta} = f(2\alpha,2\beta) + 2\alpha - 2\beta = 4n_{\alpha\beta} - 2(\alpha-\beta) \neq 0$, so (6.6) holds for $2\alpha,2\beta$ in place of α,β, and hence (6.6) holds for α,β also.

LEMMA 6.4. *The mapping f is biadditive.*

Proof. We must show that the $k_{\alpha\beta\gamma}$ appearing in (6.6) vanishes when α,β,γ are independent. Note that

$$f(\gamma,\alpha+\beta) = f(\gamma,\alpha) + f(\gamma,\beta) - k_{\alpha\beta\gamma}\gamma.$$

One also sees easily that

$$k_{-\alpha,-\beta,\gamma} = -k_{\alpha\beta\gamma}, \quad k_{\alpha\beta\gamma} = k_{\alpha,\beta,-\gamma}, \quad k_{\alpha\beta\gamma} = k_{\beta\alpha\gamma}. \tag{6.7}$$

Now expanding $f(\alpha+\beta,\gamma+\delta) - f(\alpha,\gamma) - f(\alpha,\delta) - f(\beta,\gamma) - f(\beta,\delta)$ in two different ways, we get

$$-(\alpha+\beta)k_{\gamma,\delta,\alpha+\beta} + \gamma k_{\alpha\beta\gamma} + \delta k_{\alpha\beta\delta} = (\gamma+\delta)k_{\alpha,\beta,\gamma+\delta} - \alpha k_{\gamma\delta\alpha} - \beta k_{\gamma\delta\beta}.$$

Taking $\delta = \alpha + \beta$ (so that $k_{\gamma,\delta,\alpha+\beta} = k_{\alpha\beta\delta} = 0$) and assuming (without loss of generality) that α,β,γ are independent, we find that

$$k_{\alpha\beta\gamma} = k_{\alpha,\beta,\alpha+\beta+\gamma} = k_{\gamma,\alpha+\beta,\alpha}.$$

It follows from this and (6.7) that $k_{-\gamma,\gamma-\beta,\alpha} = k_{\alpha,-\beta,-\gamma} = -k_{-\alpha,\beta,\gamma}$. But also $k_{-\gamma,\gamma-\beta,\alpha} = -k_{\gamma,-\gamma+\beta,\alpha} = -k_{\alpha\beta\gamma}$. Hence $k_{\alpha\beta\gamma} = k_{-\alpha,\beta,\gamma} = k_{-\alpha,-\beta,\gamma} = -k_{\alpha\beta\gamma}$, so that $k_{\alpha\beta\gamma}$ always vanishes, and the lemma is proved.

We are now ready to complete the proof of the theorem. We choose the basis elements u_β (β a nonzero root) such that (3.1) holds for all α. By Lemma 3.1, these basis elements are uniquely determined. We have shown that for any roots α and β, basis elements $u'_{i\alpha+j\beta}$ ($i,j \in F_p$) may be chosen, with respect to which (6.1) holds. But (3.1), with any $i\alpha + j\beta$ in place of β, is a special case of (6.1), so $u'_{i\alpha+j\beta} = u_{i\alpha+j\beta}$ for all i,j. Hence (2.2) holds. Since f is skew-symmetric and bi-additive, the proof of the theorem is complete.

References

1. A. A. Albert and M. S. Frank, *Simple Lie algebras of characteristic p*, Univ. e Politec. Torino Rend. Sem. Mat. **14** (1954–1955), 117–139.

2. R. Block, *New simple Lie algebras of prime characteristic*, Trans. Amer. Math. Soc. **89** (1958), 421–449.

3. Ho-Jui Chang, *Über Wittsche Lie-ringe*, Abh. Math. Sem. Univ. Hamburg **14** (1941), 151–184.

4. N. Jacobson, *Restricted Lie algebras of characteristic p*, Trans. Amer. Math. Soc. **50** (1941), 15–25.

5. I. Kaplansky, *Lie algebras of characteristic p*, Trans. Amer. Math. Soc. **89** (1958), 149–183.

6. R. Ree, *On generalized Witt algebras*, Trans. Amer. Math. Soc. **83** (1956), 510–546.

7. H. Zassenhaus, *Über Lie'sche Ringe mit Primzahlcharakteristik*, Abh. Math. Sem. Univ. Hamburg **13** (1939), 1–100.

California Institute of Technology,
Pasadena, California
Yale University,
New Haven, Connecticut