ON THE MILLS-SELIGMAN AXIOMS FOR LIE
ALGEBRAS OF CLASSICAL TYPE

BY
RICHARD E. BLOCK

1. Introduction. Mills and Seligman in [8] presented a unified technique for
the classification of those semisimple Lie algebras to which the methods of Killing
and Cartan are applicable. They classified the Lie algebras $L$ (assumed to be
finite-dimensional, as will be also all algebras in the present paper), of character-
istic not 2, 3, 5 or 7, which satisfy the following conditions: $L$ has a Cartan
subalgebra $H$ such that $L$ and $H$ satisfy five axioms, which we may state as

(i) $LL = L$.

(ii) The center of $L$ consists of 0 alone.

(iii) $H$ acts diagonally on $L$.

(iv) If $\alpha$ is a nonzero root then $L_{\alpha}L_{-\alpha}$ is one-dimensional.

(v) If $\alpha$ is a nonzero root and $\beta$ is a linear functional on $H$, then there is a
positive integer $m$ such that $\beta + m\alpha$ is not a root.

Here of course the roots are roots with respect to $H$, and (iii) means that if
$h \in H$ and $a \in L_{\alpha}$, the root space for a nonzero root $\alpha$, then $ah = a(h)a$. By (ii)
and (iii) $H$ is necessarily abelian.

Mills and Seligman showed that if $L$ is over a field $F$ of characteristic $p > 7$
and satisfies the above axioms with respect to some Cartan subalgebra, then $L$
is a direct sum of simple algebras of classical type, that is, each of the simple
direct summands is the analogue over $F$ of one of the simple Lie algebras (in-
cluding the five exceptional algebras) over the complex numbers. More explicitly,
the simple Lie algebras of classical type over $F$ are obtained as follows: start
with a complex simple Lie algebra, take a basis with integral structure constants
as in [4, p. 24], reduce the structure constants modulo $p$, then take the scalar
extension to an algebra over $F$, and divide by the center (which is nonzero only
if the initial algebra is of type $A_r$ with $p \mid r + 1$). The result of Mills and Seligman
was extended by Mills [7] to include the case of characteristics 5 and 7.

Axiom (v) above, although essential for the use of root-string techniques, is
rather artificial in that it does not correspond (because of the finite-dimensionality)
to any step in the proof of the well-known results on complex semisimple Lie
algebras.

Received by the editors January 26, 1965.
Our purpose in the present paper is the determination of the Lie algebras satisfying a set of axioms similar to those of Mills and Seligman, but without an axiom like (v) above; we shall prove that such algebras are direct sums of simple algebras which are either of classical type or of a certain explicitly determined class of algebras of rank one.

The axioms on $L$ and $H$ which we shall assume are

(i) $L^2 = L$.

(ii) The center of $L$ consists of 0 alone.

(A) For every nonzero root $\alpha$, $L_\alpha$ is one-dimensional and $\alpha(L_\alpha L_{-\alpha}) \not= 0$, that is, $L_\alpha + L_{-\alpha} + L_\alpha L_{-\alpha}$ is a (split) three-dimensional simple algebra.

Axiom (A) is formally stronger than (iii) and (iv) of Mills and Seligman, but still corresponds to a natural stage in the classification proof at characteristic 0. Axiom (A) was also used by Jacobson [5], together with (i) and the assumption that $H$ is abelian (which is implied by (ii) and (A)), as a hypothesis in a preliminary investigation of the representation theory of such algebras.

Our classification must take account of the Albert-Zassenhaus algebras. By an Albert-Zassenhaus algebra is meant an algebra over a field $F$ with a basis $\{u_\alpha | \alpha \in G\}$, where $G$ is a finite additive subgroup of $F$, and with multiplication

\begin{equation}
  u_\alpha u_\beta = \{zh(\beta) - \beta h(\alpha) + \alpha - \beta\}u_{\alpha + \beta}, \quad \alpha, \beta \in G,
\end{equation}

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 $u_\alpha$. The algebras satisfy axioms (i), (ii) and (A) above (with respect to $(u_0)$) but not (v) — the roots form an additive elementary $p$-group. These algebras are the only simple ones known which satisfy (i)–(iv) but not (v), as well as the only known simple algebras of rank one other than the three-dimensional algebra. Moreover the author has proved in [2] that if $L$ has a one-dimensional Cartan subalgebra such that $e_\alpha L_{-\alpha} \not= 0$ for every nonzero root $\alpha$ and nonzero $e_\alpha$ in $L_\alpha$, then $L$ is either three-dimensional or an Albert-Zassenhaus algebra, provided that the base field $F$ is algebraically closed of characteristic $p > 3$.

Our principal result, to whose proof almost all of this paper will be devoted, is the following.

**Main Theorem.** Let $L$ be a finite-dimensional Lie algebra of characteristic $p > 5$. Suppose that $L$ has a Cartan subalgebra $H$ such that (i), (ii) and (A) are satisfied. Then $L$ is a direct sum of simple algebras satisfying the same hypotheses, and each such simple algebra is either of classical type or has rank one. If the base field is perfect then the simple summands which are not of classical type are Albert-Zassenhaus algebras.

If in addition $L$ is restricted (that is, is a $p$-algebra) and if a simple direct summand is of rank one but not of classical type, then (as can be seen without using
the summand is the $p$-dimensional Witt algebra, that is, has a basis \( \{u_i \mid i \in F_p\} \) (\( F_p \) the prime field) with \( u_i u_j = (i - j)u_{i+j} \).

Information on representations of the Witt algebra constitutes the chief tool in the proof of the main theorem. We begin our proof in the next section by showing that if (v) fails then there is a root $\alpha$ such that $W_\alpha = \sum_{i \neq 0} L_{i\alpha}$ generates a Witt algebra. In the succeeding section we obtain explicit formulas for all irreducible representations of the Witt algebra of degree not greater than $p$. The remainder of the proof consists principally of the application of these formulas to the representations of $W_\alpha$ on $\sum L_{\beta + i\alpha}$ and $\sum L_{-\beta + i\alpha}$ when, for some $i$, $L_{\beta + i\alpha} L_{-\beta - i\alpha} \neq L_{\alpha} L_{-\alpha}$; this is done to show that certain algebras of rank greater than one cannot exist and that the $L_{\beta}$ with $L_{\beta} L_{-\beta} = L_{\alpha} L_{-\alpha}$ generate a direct summand of $L$ of rank one.

The assumption that $p \neq 5$ is used only in the proofs of Lemmas 2.2 and 4.1. The proof of Lemma 2.2 cannot be extended since when $p = 5$ there actually does exist a representation of the type considered in that proof, in which $v$ is represented by a nonzero scalar. However it seems likely that our theorem remains true when $p = 5$.

2. Proof that $L$ contains the Witt algebra if not of classical type. Throughout the proof of the main theorem we shall assume that $L$ is a finite-dimensional Lie algebra over a field $F$ of characteristic $p > 5$, with a Cartan subalgebra $H$, and that $L$ satisfies Axioms (i), (ii) and (A), with respect to $H$. Until close to the end of the proof, in §5, we shall also assume that $F$ is algebraically closed. All roots considered will be roots with respect to $H$. The letters $i$ and $j$ will always denote integers.

**Lemma 2.1.** If $L$ is not a direct sum of simple algebras of classical type, then there is a nonzero root $\gamma$ such that $2\gamma$ is also a root.

**Proof.** Under the hypotheses, Axiom (v) of [8] must fail, that is, there exist roots $\alpha$ and $\beta$ ($\alpha \neq 0$) such that $\beta + i\alpha$ is a root for all $i$. If $\beta + i\alpha = 0$ for some $i$ then every $i\alpha$ is a root. Thus we may suppose that $\beta + i\alpha \neq 0$ ($i = 0, \ldots, p-1$). Suppose that none of $2\alpha$, $2\beta + 2\alpha$, $2\beta - 2\alpha$ is a root. For each root $\delta$ choose a nonzero element $u_\delta$ in $L_{\delta}$. By the Jacobi identity,

\[
(u_\beta u_{\theta + i\alpha} u_{-\beta} + (u_{\beta + i\alpha} u_{-\beta}) u_\beta + (u_{-\beta} u_\delta) u_{\beta + i\alpha} = 0.
\]

But for $i = \pm 2$, the first two terms vanish, so that $(\beta + i\alpha)(u_\beta u_{-\beta}) = 0$. This implies that $\alpha(L_{\beta} L_{-\beta}) = \beta(L_{\beta} L_{-\beta}) = 0$, which contradicts (A). Hence we may take one of $\alpha, \beta + \alpha$ or $\beta - \alpha$ as $\gamma$, and the lemma is proved.

Now suppose that $\alpha$ is nonzero root such that $i\alpha$ is a root for some $i = 2, \ldots, p-2$. Consider the subspace $K$ of $L$ spanned by all $L_{i\alpha}$ (including $L_0 = H$). Then $K$ is a subalgebra, and its center $I$ clearly is \( \{h \in H \mid \alpha(h) = 0\} \). The quotient algebra $K/I$ has rank one, with Cartan subalgebra $H/I$, and the roots of $K/I$ consist
of those mappings \(i\alpha\) of \(H/I\) which are induced by roots of \(L\) of the form \(i\alpha\).

It then follows easily from [9, pp. 42-47] (see [2, Lemma 3.1]) that \(K/I\) is a Witt algebra, with \(i\alpha\) a root for all \(i\), and that there are nonzero elements \(u_{i\alpha}\) in \(L_{i\alpha}\) such that \(u_{i\alpha}u_{j\alpha} \equiv (i - j)u_{(i + j)\alpha} \pmod{I}\). Since \(I \subseteq H\) and \(L_{i\alpha}L_{j\alpha} \subseteq L_{(i + j)\alpha}\), this implies that

\[
(2.1) \quad u_{i\alpha}u_{j\alpha} = (i - j)u_{(i + j)\alpha} \text{ if } i + j \not\equiv 0 \pmod{p}.
\]

We may assume that \(u_0\) was chosen so that \(u_\alpha u_{-\alpha} = 2u_0\). We may write \(u_{2\alpha} u_{-2\alpha} = 4u_0 + 3\cdot 2 \cdot 1 v\), where \(v\) is some element, possibly 0, in \(I\). We shall show by induction that

\[
(2.2) \quad u_{i\alpha}u_{-i\alpha} = 2iu_0 + (i + 1)i(i - 1)v, \quad i = 0, \ldots, p - 1.
\]

Indeed, for \(i = 3, \ldots, p - 1\), we have \((i - 2)u_{i\alpha}u_{-i\alpha} = (u_{(i - 1)\alpha}u_\alpha)u_{-i\alpha} = (u_{(i - 1)\alpha}u_{-i\alpha}) = -2(2i - 1)u_0 + (1 + i)u_{(i - 1)\alpha}u_{-(i - 1)\alpha} = (i - 2)2iu_0 + (i - 2)(i + 1)i(i - 1)v\), which proves (2.2).

It would be convenient if we could conclude directly that \(v = 0\). However this is not possible without referring to the imbedding in \(L\) and using the assumption that \(L\) is centerless, since (2.1) and (2.2) actually define a \((p + 1)\)-dimensional Lie algebra with center \((v)\) which is a nontrivial central extension of the Witt algebra. In order to show that \(v\) is in the center of \(L\), we shall use a device motivated by the existence in the Witt algebra of two nonconjugate Cartan decompositions, each giving rise to a convenient multiplication table.

The Witt algebra \(W\) over \(F\) may be regarded as the Lie algebra of derivations of the \(p\)-dimensional commutative associative algebra \(F[x]\) with \(x^p = 1\). Thus \(W\) has a basis \(f_0, f_1, \ldots, f_{p-1}\), where \(f_i\) is the derivation of \(F[x]\) determined by \(xf_i = x^{i+1}\), and these basis elements have the multiplication table

\[
(2.3) \quad f_if_j = (i - j)f_{i+j},
\]

where the subscripts are added modulo \(p\). Taking \(y = x - 1\) as a generator of \(F[x]\), so that this algebra becomes \(F[y]\) with \(y^p = 0\), we see that \(W\) also has a basis \(e_{-1}, e_0, \ldots, e_{p-2}\), where \(ye_i = y^{i+1}\), and for \(-1 \leq i, j \leq p - 2\),

\[
(2.4) \quad e_ie_j = (i - j)e_{i+j}, \quad e_k = 0 \text{ if } k > p - 2.
\]

Since \(xe_i = (x - 1)e_i = (x - 1)^{i+1}\), we have

\[
(2.5) \quad e_i = \sum_{j=0}^{i+1} \binom{i+1}{j}(-1)^j f_{i-j}, \quad i = -1, \ldots, p - 2,
\]

and similarly, since \(yf_i = (y + 1)^{i+1}\),

\[
(2.6) \quad f_i = \sum_{j=0}^{i+1} \binom{i+1}{j} e_{i-j}, \quad i = 0, \ldots, p - 1.
\]
LEMMA 2.2. Suppose that \( \alpha \) is a nonzero root such that \( k\alpha \) is a root for some \( k = 2, \ldots, p - 2 \). Then all \( i\alpha \) are roots, and there are nonzero elements \( u_{i\alpha} \) in \( L_{i\alpha} \) for \( i = 0, \ldots, p - 1 \) such that \( u_{i\alpha}u_{j\alpha} = (i - j)u_{(i+j)\alpha} \) for all \( i, j \), that is, \( L_{\alpha} \) and \( L_{k\alpha} \) generate a Witt algebra.

Proof. Choosing the elements \( u_{i\alpha} \) in \( K \) so that (2.1) and (2.2) hold, what we must show is that the element \( v \) in \( I \) is zero. Let \( W_{\alpha} \) be the subalgebra of \( L \) spanned by \( v \) and the \( u_{i\alpha} \), \( i = 0, 1, \ldots, p - 1 \). Suppose that \( \nu \neq 0 \), and set

\[
e_i' = \sum_{j=0}^{i+1} \binom{i+1}{j} (-1)^j u_{(i-j)\alpha}, \quad i = -1, \ldots, p - 2 \quad (e'_{k} = 0 \text{ if } k > p - 2).
\]

Since \( W_{\alpha}/(v) \) is the Witt algebra, we have

\[e_i'e_j' \equiv (i - j)e_{i+j}' \mod(v).\]

Since \( e_0' = u_0 - u_{-\alpha} \), there is no term in \( v \) in \( e_0'e_0' \), and it follows that \( e_0' \) and \( v \) span a Cartan subalgebra of \( W_{\alpha} \) with one-dimensional root spaces spanned by the \( e_i' \), \( i = -1, 1, 2, \ldots, p - 2 \). Therefore \( e_i'e_j' \) has no term in \( v \) unless \( i + j \equiv 0 \mod p \). But \( e_i' \) is \( u_{i\alpha} \) plus terms of lower index, so the only term in \( v \) in \( e_i'e_{i-1}' \) is that of \( u_{i\alpha}u_{(p-i)\alpha} \), that is, \( e_i'e_{p-i}' = i(i + 1)(i - 1)v \). Now suppose that \( \beta(v) \neq 0 \) for some root \( \beta \). Consider the representation space \( M = \sum_{i} L_{\beta + i\alpha} \) for \( W_{\alpha} \) under right multiplication. Since \( \alpha(v) = 0 \), \( (\beta + i\alpha)(v) = \beta(v) \) for all \( i \), and \( v \) is represented by a nonzero scalar. The elements \( e_{(p-1)/2}', e_{(p+1)/2}', e_{p-2}' \) and \( v \) span a subalgebra \( B \) of \( W_{\alpha} \) containing \( v \) in its square.

Let \( N \) be an irreducible \( B \)-submodule of \( M \). Since \( v \) is represented by a nonzero scalar of trace 0, \( N \) has dimension \( p \), \( M = N \), and \( M \) is irreducible under \( B \). But since \( p > 5 \), \( e_{p-2}' \) is in the center of \( B \), and so is represented by a scalar on \( M \). Therefore \( e_{p-2}'e_{p}' \), which is the nonzero multiple of \( v \), is represented by 0, a contradiction. Hence \( \beta(v) = 0 \) for all roots \( \beta \), and \( v \) is in the center of \( L \) and so vanishes. This completes the proof of the lemma.

3. Representations of the Witt algebra. Let \( W \) be the Witt algebra over a field \( F \), with basis \( e_{-1}, e_0, \ldots, e_{p-2} \) and multiplication given by (2.4). Let \( V \) be a vector space over \( F \) with basis \( v_0, v_1, \ldots, v_{p-1} \), and let \( a, b \) be given scalars. For each \( e_j \) define a linear transformation on \( V \) by setting (for \( i = 0, \ldots, p - 1 \))

\[v_i'e_j = [i + (j + 1)a]v_{i+j} \quad \text{if} \quad (i,j) \neq (0,-1); \quad v_k = 0 \quad \text{if} \quad k > p - 1;
\]

\[v_0'e_{-1} = bv_{p-1}.
\]

Note that if \( j > p - 2 \) then either \( v_{i+j} = 0 \) or \( i = 0, j = p - 1 \) and the coefficient of \( v_{i+j} \) vanishes. We claim that the linear mapping \( \Delta = \Delta_{ab} \), determined
by (3.1), of \( W \) to linear transformations on \( V \), is a representation of \( W \). Indeed if \( j \neq k \) and either \( i \neq 0 \) or \( j, k \neq -1 \) then

\[
(v_i e_j) e_k - (v_k e_j) e_i = \left\{ \left[ i + (j + 1)a \right] \left[ i + (j + k + 1)a \right] - \left[ i + (k + 1)a \right] \left[ i + k(j + 1)a \right] \right\} v_{i+j+k} \\
= (j-k) \left[ i + (j + k + 1)a \right] v_{i+j+k} = (j-k) v_i e_{j+k} = v_i (e_j e_k).
\]

Also, if \( k > 0 \) then

\[
(v_0 e_{-1}) e_k - (v_0 e_k) e_{-1} = 0 - k(k+1)a v_{k-1} = (-1-k) v_0 e_{k-1} = v_0 (e_{-1} e_k), \quad \text{and} \quad (v_0 e_{-1}) e_0 - (v_0 e_0) e_{-1} = b(-1+a) - ba v_{p-1} = -v_0 e_{-1} = v_0 (e_{-1} e_0)
\]

Hence \( \Delta \) is a representation.

If \( a = 1 \) and \( b = 0 \) then \( v_0, v_1, ..., v_{p-2} \) span a subspace of \( V \) which is invariant under all \( e_j \). We shall denote by \( A'_{10} \) the restriction of \( A_{10} \) to the representation of \( W \) on this \((p-1)\)-dimensional subspace.

**Lemma 3.1.** Let \( A = A_{ab} \) be the representation of \( W \) defined above, and suppose that \( a \neq 0, 1 \). Then there exists a characteristic vector \( v \) of \( e_0^A \) which is annihilated by \( e_1^A \) and \( e_2^A \), and for any such \( v \), the characteristic value for \( e_0^A \) is \( a - 1 \).

**Proof.** Clearly \( v_{p-1} \) satisfies the conditions for \( v \). Now suppose that \( v \neq 0, v_0 = cv \) and \( v_1 = v_2 = 0 \). Since \( V \) is spanned by characteristic vectors of \( e_0^A \) with distinct characteristic roots, we may suppose that \( v = v_i \) for some \( i \) (\( 0 \leq i \leq p-1 \)), and thus \( c = i + a \). But \( v_1 e_1 = 0 \) only if \( i = p - 1 \) or \( i + 2a = 0 \), while \( v_1 e_2 = 0 \) only if \( i = p - 1 \) or \( i = p - 2 \) or \( i + 3a = 0 \). Therefore the conditions that \( v_i e_1 = v_i e_2 = 0 \) and \( a \neq 0, 1 \) imply that \( i = p - 1 \) and \( c = a - 1 \), and the lemma is proved.

**Theorem 3.1.** Let \( W \) be the Witt algebra over an algebraically closed field \( F \) of characteristic \( p > 3 \). The (nontrivial) irreducible representations of \( W \) of degree not greater than \( p \) are, up to equivalence, the mappings \( A_{ab} \) \((a, b) \neq (0, 0), (1, 0)\) and \( A_0 \) defined above. Two of the irreducible representations \( A_{ab}, A_{cd} \), with \((a, b) \neq (c, d)\), are equivalent if and only if \( b = d \) and either \( a = 1 \), \( c = 0 \) or \( a = 0 \), \( c = 1 \).

**Proof.** The Witt algebra is a restricted Lie algebra, and for the basis elements \( e_i \) (satisfying (2.4)) we have \( e_i^p = 0 \) for \( i = -1, 1, 2, ..., p-2 \), and \( e_0^p = e_0 \). If \( \Delta \) is a (not necessarily restricted) irreducible representation of a restricted Lie algebra \( K \) over \( F \), then for any \( k \) in \( K \), by Schur's Lemma \( (k^A)^p - (k^p)^A \) is a scalar multiple of the identity transformation. In particular if \( \Delta \) is an irreducible representation of \( W \), there are scalars \( e_i = e_i(\Delta) \) such that

\[
(e_0^A)^p - e_0^A = e_0(\Delta)I, \quad (e_1^A)^p = e_1(\Delta)I, \quad i = -1, 1, 2, ..., p-2.
\]

The irreducible representations of \( W \) over \( F \) have been considered by Chang [3]. For any given values of \( e_i \) \((i = -1, ..., p-2)\) he determines the number of
inequivalent irreducible representations \( \Delta \) of \( W \) of each degree whose invariants \( \epsilon_i(\Delta) \) have the given values. His results on the irreducible representations \( \Delta \) of \( W \) of degree not greater than \( p \) \cite[pp. 172, 176]{3} are as follows: \( \epsilon_i(\Delta) = 0 \) for \( i = 1, \ldots, p-2 \); moreover for given values \( \epsilon_{-1}, \epsilon_0, 0, \ldots, 0 \), of the invariants, the number of inequivalent irreducible representations of \( W \) is \( p \), all of degree \( p \), in case \( \epsilon_0 \neq 0 \); \( p-1 \), all of degree \( p \), in case \( \epsilon_0 = 0 \) and \( \epsilon_{-1} \neq 0 \); and, \( p \), of which \( p-2 \) are of degree \( p \), one of degree \( p-1 \) and one (the trivial representation) of degree \( 1 \), in case \( \epsilon_0 = \epsilon_{-1} = 0 \).

Let \( V' \) be an irreducible invariant subspace of \( V \) for the representation \( \Delta = \Delta_{ab} \). Since \( V \) is spanned by characteristic vectors of \( e_0^\Delta \) with distinct characteristic roots, and since \( V' \) contains a characteristic vector of \( e_0^\Delta \), some \( v_i \) (\( 0 \leq i \leq p-1 \)) is in \( V' \). Then \( V' \) is spanned by all \(((v_0^e) \cdots v_r^e)_e\), so that \( V' \) is spanned by some of the \( v_j \). Repeatedly operating with \( e_1^\Delta \), we see that \( v_0, v_1, \ldots, v_t \) are all in \( V' \). But by the result of Chang, the dimension of \( V' \) is \( 1, p-1 \) or \( p \). Hence either \( V' = (v_0) \) or \( V' = (v_0, \ldots, v_{p-2}) \) or \( V' = V \). By (3.1), \( (v_0) \) is invariant only if \( (a, b) = (0, 0) \), and \( (v_0, \ldots, v_{p-2}) \) is invariant only if \( (a, b) = (1, 0) \). Therefore \( \Delta_{ab} \) is irreducible provided \( (a, b) \neq (0, 0), (1, 0) \), and \( \Delta_{10} \) is irreducible.

By (3.1), the representations \( \Delta = \Delta_{ab} \) satisfy (3.2) with \( \epsilon_1(\Delta) = 1 \cdot 2 \cdots (p-1)b \)

\[
= -b, \quad \epsilon_0(\Delta) = a^p - a \quad \text{and} \quad \epsilon_1(\Delta) = \cdots = \epsilon_{p-2}(\Delta) = 0.
\]

Hence for any values \( \epsilon_{-1}, \epsilon_0, 0, \ldots, 0 \), there is a \( \Delta_{ab} \) having invariants with these values, and the representations \( \Delta_{a+k,b} \), for all \( k \) in \( F_p \), also have invariants with the given values, but no other \( \Delta_{cd} \) has this property. Moreover \( \epsilon_0(\Delta_{ab}) = 0 \) if and only if \( a \in F_p \).

By the result of Chang, it will complete the proof to show that \( \Delta_{ab} \) and \( \Delta_{a+k,b} \) (\( k \in F_p, k \neq 0 \)) are equivalent only if \( a = 0 \) and \( k = 1 \) or \( a = 1 \) and \( k = -1 \). But we see that this condition follows immediately from Lemma 3.1, taking into account the fact that if \( a = 0 \) or \( 1 \) then \( v_{p-1} e_1 = v_{p-1} e_2 = 0 \) and \( v_{p-1} e_0 = -v_{p-1} \) or \( 0 \). Thus the theorem is proved.

Since \( \Delta \) is restricted if and only if \( \epsilon_i(\Delta) = 0 \) for \( i = -1, 0, \ldots, p-2 \), we immediately get the following consequence.

**Corollary 3.1.** Any (nontrivial) irreducible restricted representation of the Witt algebra, over an algebraically closed field of characteristic \( p > 3 \), is equivalent to one of the \( p-1 \) representations \( \Delta_{10}, \Delta_{20}, \ldots, \Delta_{-1,0} \), which are irreducible and inequivalent.

4. Application of the representation formulas. If \( \alpha \) is a root such that the root spaces \( L_{i\alpha} \) generate a Witt algebra, we shall denote this Witt algebra by \( W_\alpha \). If also \( \beta \) is a root, then \( \sum_i L_{\beta+i\alpha} \) is a representation space for \( W_\alpha \); we shall write

\[
\sum_i L_{\beta+i\alpha} = M_{\beta\alpha},
\]

and we shall write \( \Gamma_{\beta\alpha} \) for the representation of \( W_\alpha \) on \( M_{\beta\alpha} \). Note that \( M_{\beta\alpha} M_{-\beta\alpha} \subseteq H + W_\alpha \).
Lemma 4.1. Suppose that \( \alpha \) and \( \beta \) are roots and that the root spaces \( L_{\alpha} \) generate a Witt algebra \( W_{\alpha} \). If \( M_{\beta x} M_{-\beta x} \subseteq W_{\alpha} \) then \( M_{\beta x} M_{-\beta x} \subseteq \{ h \in H \mid \alpha(h) = 0 \} \).

Proof. We shall take nonzero elements \( u_{\alpha x} \) in \( L_{\alpha x} \) \((i = 0, \cdots, p - 1)\) such that \( u_{\alpha x} u_{\beta x} = (i - j)u_{(i+j)x} \), and also a basis \( e_1, e_0, \cdots, e_{p-2} \) of \( W_{\alpha} \) such that (2.4) holds.

If \( M_{\beta x} \) or \( M_{-\beta x} \) is one-dimensional then \( M_{\beta x} = L_{\beta} \), \( M_{-\beta x} = L_{-\beta} \), and \( L_{\beta} L_{-\beta} \subseteq H \). Moreover \( L_{\alpha} L_{\beta} = L_{\alpha} L_{-\beta} = 0 \), so that \( L_{\alpha}(L_{\beta} L_{-\beta}) = 0 \), that is \( \alpha(L_{\beta} L_{-\beta}) = 0 \), and the conclusion holds in this case.

Now suppose \( M_{\beta x} \) is not one-dimensional. Then there is a root \( \beta + ix \) distinct from \( \beta \), and so \((\text{ad} u_0)^p \) does not vanish on \( M_{\beta x} \). Hence not all composition factors of \( \Gamma_{\beta x} \) are trivial. Therefore \( \Gamma_{\beta x} \) either is irreducible of degree \( p - 1 \) or \( p \), or contains a composition factor of degree \( p - 1 \).

We shall now consider the possibilities for the representations of \( W_{\alpha} \) on \( M_{\beta x} \) and \( M_{-\beta x} \) in a number of cases, showing that the first three cases cannot occur, and that in the remaining cases the conclusion of the lemma holds. We take a basis \( h_1, \cdots, h_r, u_0 \) of \( H \) such that \( \alpha(h_l) = 0, i = 1, \cdots, r - 1 \). Under the hypothesis, there is an \( h_l \) \((1 \leq l \leq r - 1)\) such that some element in \( M_{\beta x} M_{-\beta x} \) has a nonzero component in \( h_l \). In what follows, 0 and 1 will sometimes denote integers and sometimes elements of \( F \); which is meant should be clear from the context. However \( i, j, k \) and \( n \) will denote integers.

Case 1. \( \Gamma_{\beta x} \) and \( \Gamma_{-\beta x} \) both irreducible of degree \( p \), with \( \Gamma_{\beta x} \cong \Delta_{ab} \) and \( \Gamma_{-\beta x} \cong \Delta_{a',b'} \) where \( a + a' \neq 1 \) and either \( a \neq 0, 1 \) or \( a' \neq 0, 1 \):

By symmetry we may suppose that \( a \neq 0, 1 \). There is a basis \( v_0, \cdots, v_{p-1} \) of \( M_{\beta x} \) such that (3.1) holds, and similarly a basis \( v'_0, \cdots, v'_{p-1} \) of \( M_{-\beta x} \) such that (3.1) holds with \( v_1, a, b \) replaced by \( v'_1, a', b' \). We denote by \( c_{ij} \) the coefficient of \( h_1 \) in the expression for \( v_i v'_j \) as a linear combination of the given basis elements of \( H \) plus elements in other root spaces. Then \( c_{ij} = 0 \) if \( i > p - 1 \) or \( j > p - 1 \). We shall only consider the \( c_{ij} \) with nonnegative subscripts. By the Jacobi identity, \( (v_i v'_j) e_k = (v_i e_k) v'_j + v_i (v'_j e_k) \); taking the terms in \( h_1 \), we get

\[
(4.1) \quad 0 = \left[ i + (k + 1)a \right] c_{i+k,j} + \left[ j + (k + 1)a' \right] c_{i,j+k}, \quad k \neq -1 \text{ or } i, j \neq 0,
\]

and, when \( k = -1 \) and \( i = 0 \),

\[
(4.2) \quad 0 = bc_{p-1,j} + j c_{0,j-1}, \quad j \neq 0.
\]

With \( k = 0 \), (4.1) implies that \( c_{ij} = 0 \) unless \( (i + j)1 + a + a' = 0 \). Since \( c_{ij} \neq 0 \) for some \( i, j \), \( a + a' \in F_p \); we write

\[
a + a' = n 1, \quad 1 \in F, \quad 0 \leq n \leq p.
\]

Hence if \( c_{ij} \neq 0 \) then \( i + j + n = 0, p \) or \( 2p \).

By (4.1), if \( c_{i,j+1} = 0 \) then \( c_{i+1,j} = 0 \) unless \( i1 + 2a = 0 \). In particular, since
a \neq 0, \text{ if } c_{0,j+1} = 0 \text{ then } c_{1,j} = 0. \text{ Also, with } k = 2 \text{ in (4.1) we see that if } c_{i-1,j+2} = 0 \text{ (} i > 0 \text{) then } c_{i+1,j} = 0 \text{ unless } (i-1)1 + 3a = 0. \text{ Since } a \neq 1, \text{ either } i1 + 2a \neq 0 \text{ or } (i-1)1 + 3a \neq 0 \text{ and hence}

\begin{align}
\text{if } c_{i,j+1} = c_{i-1,j+2} = 0 \text{ then } c_{i+1,j} = 0 \text{ (} i > 0 \text{),} \\
(4.3)
\end{align}

\begin{align}
\text{if } c_{0,j+1} = 0 \text{ then } c_{1,j} = 0.
\end{align}

Now suppose that \( i + j + n = 2p \). Then \( c_{ij} \) is one of

\begin{align}
&c_{p-n+p,0}, c_{p-n+p-1,1}, \ldots, c_{p-n,p}, c_{p-n-1,p+1}
\end{align}

(all subscripts are nonnegative). Since the last two terms vanish, repeated application of (4.3) shows that all terms vanish, and \( c_{ij} = 0 \).

Next suppose that \( i + j + n = p \). Then \( c_{ij} \) is one of \( c_{p-n,0}, c_{p-n-1,1}, \ldots, c_{0,p-n} \). Since we have shown that \( c_{p-1,p-n+1} = 0 \), and since \( n \neq 1 \), (4.2) implies that \( c_{0,p-n} = 0 \). Then repeated application of (4.3) again shows that \( c_{ij} = 0 \).

Finally, if \( i + j + n = 0 \), then \( i = j = n = 0 \), and the only relevant \( c_{ij} \) is \( c_{00} \). But (4.2) with \( j = 1 \) implies that \( c_{00} = 0 \). Hence Case 1 cannot occur.

Case 2. Degree \( p \), with one of \( \Gamma_{\beta x}, \Gamma_{-\beta x} \) irreducible, and the other having a \((p-1)\)-dimensional invariant subspace:

By symmetry we may suppose that \( \Gamma_{\beta x} \) is irreducible, and hence \( \Gamma_{\beta x} \cong \Delta_{ab} \) where \( (a,b) \neq (0,0),(1,0) \). Take a basis \( v_0, \ldots, v_{p-1} \) of \( M_{\beta x} \) such that (3.1) holds.

Then \( M_{-\beta x} \) has a basis \( v'_0, \ldots, v'_{p-1} \) such that

\begin{align}
v'_i v_j = (i + j + 1)v'_{i+j}, \quad i = 0, \ldots, p-2,
\end{align}

where \( v'_i = 0 \) if \( i > p-1 \), and \( v'_{p-1}e_0 \) is a linear combination of \( v'_0, \ldots, v'_{p-2} \). Changing \( v'_{p-1} \) by subtracting a suitable linear combination of \( v'_0, \ldots, v'_{p-2} \), we may suppose that \( v'_{p-1}e_0 = 0 \). By a weight argument, there exist scalars \( b'_{-1}, b'_1, b'_2, \ldots, b'_{p-2} \) such that

\begin{align}
v'_{p-1}e_{-1} = b'_1 v'_{p-2}, v'_{p-1}e_{i} = b'_i v'_{i-1}, \quad i = 1, 2, \ldots, p-2.
\end{align}

Write \( (\operatorname{ad} e_{-1})^p = D \). Then \( D \) is a derivation which annihilates \( M_{-\beta x} \) and \( M_{\beta x} M_{-\beta x} \). Therefore \( (M_{\beta x}D)M_{-\beta x} = 0 \). Since \( D \) acts as the scalar \(-bI\) on \( M_{\beta x} \), this implies that \( b = 0 \), and hence \( a 
eq 0, 1 \).

We continue using the notation \( c_{ij} \) of Case 1, and write \( a' = 1 \). In particular with \( n \) defined as before, it follows that \( n 
eq 1, 2 \). Now (4.1) holds provided \( j 
eq p-1 \) or \( k = 0 \). Moreover if \( j \neq p-1 \) then (4.2) and (4.3) hold. If \( j = p-1 \) and \( k = 1 \) or 2 then instead of (4.1) one has

\begin{align}
0 = [i + (k+1)a]c_{i+k,p-1} + b_k c_{i,k-1},
\end{align}

and hence, as in the proof of (4.3), if \( c_{i,0} = c_{i-1,1} = 0 \) (\( i > 0 \)) then \( c_{i+1,p-1} = 0 \), and if \( c_{00} = 0 \) then \( c_{1,p-1} = 0 \). We need only show that \( c_{p-n,0} = c_{p-n-1,1} = 0 \)
in order to carry through in this case the previous proof that \( c_{ij} = 0 \) if \( i + j + n = 2p \). If \( i \neq 0 \), an analogue of (4.2) obtained by taking \( j = 0 \) and \( k = -\) says that \( 0 = ic_{i-1,0} + 0 \). Since \( n \neq 1 \), it follows that \( c_{p-n,0} = 0 \). But then (4.1) with \( i = p - n - 1, j = 0 \) and \( k = 1 \) also gives \( c_{p-n-1,1} = 0 \).

No further use of (4.3) when \( j = p - 1 \) is made in Case 1 unless \( n = 0 \), in which case we must show that \( c_{1,p-1} = 0 = c_{00} \). But since \( b = 0 \), (4.2) with \( j = 1 \) implies that \( c_{00} = 0 \), and we have already noted that this implies that \( c_{1,p-1} = 0 \). Hence Case 2 cannot occur.

Case 3. Degree \( p \), with one \( \Gamma_{\beta a}, \Gamma_{-\beta a} \) irreducible and the other having a one-dimensional invariant subspace:

We may suppose that \( M_{\beta a} \) is as in the proof of Case 2. Let \( v'_{p-1} \) be a basis of the one-dimensional invariant subspace of \( M_{-\beta a} \). Then \( M_{-\beta a}(v'_{p-1}) \) has a basis \( \overline{v}_0, \ldots, \overline{v}_{p-2} \) such that \( \overline{v}_i e_j = (i + j + 1) \overline{v}_{i+j} \), where \( \overline{v}_k = 0 \) if \( k > p - 1 \). Take an element \( v'_i \) in \( \overline{v}_i \), \( i = 0, \ldots, p - 2 \). Then \( v'_i e'_0 = (i + 1)v'_i + d_{i}v'_{p-1} \) for some scalar \( d_i \). Changing \( v'_i \) by adding \( d_i/(i + 1)v'_{p-1} \) to it, we may assume that \( v'_i e'_0 = (i + 1)v'_i \). By a weight argument,

\[
v'_i e_j = \begin{cases} (i + j + 1)v'_{i+j} & \text{if } i + j \neq p - 1 \text{ and } (i, j) \neq (0, -1), (p - 1, -1); \\ 0 & \text{if } k > p - 1, \end{cases}
\]

and there are scalars \( b'_i, i = -1, 1, 2, \ldots, p - 2, \) such that

\[
\overline{v}_0 e_{-1} = b'_{-1}v'_{p-1}, \quad v'_i e_{p-1-i} = b'_i v'_{p-1}, \quad i = 1, \ldots, p - 2.
\]

Write \( a' = 1 \), and define the \( c_{ij} \) and \( n \) as in Case 1. Then as in Case 2, \( b = 0 \) and hence \( a \neq 0, 1 \) and \( n \neq 1, 2 \). Now (4.1) holds with only the coefficient of \( c_{i,j+k} \) changed for certain subscripts, and (4.2) holds except when \( j \neq p - 1 \). It follows that the proof in Case 1 goes through here without change — the exceptional case of (4.2) is not used since \( p - n + 1 \neq p - 1 \) because \( n \neq 2 \). Hence Case 3 cannot occur.

Case 4. \( \Gamma_{\beta a} \) and \( \Gamma_{-\beta a} \) both irreducible of degree \( p \), with \( \Gamma_{\beta a} \cong \Delta_{ab} \) and \( \Gamma_{-\beta a} \cong \Delta_{a'b'} \), where \( a + a' = 1 \) or \( a = a' = 0 \) or \( a = a' = 1 \):

Since the irreducible representations \( \Delta_{ab} \) and \( \Delta_{a'b'} \) are equivalent, we may assume that \( a + a' = 1 \). Let \( v_i \) and \( v'_i \) be as in Case 1. For any integer \( k \), let \( k^* \) denote the integer such that \( -1 \leq k^* < p - 1 \) and \( k \equiv k^* (\text{mod } p) \). For all \( i, j \), \( v_i v_j \) is either 0 or a characteristic vector for \( e_0 \) with characteristic root \( (i + a)(j + a')1 = (i + j + 1) \). Let \( d_{ij} \) denote the coefficient of \( e_{(i+j+1)^*} \) in the expression of \( v_i v_j \) as a linear combination of \( e_{-1}, \ldots, e_{p-2}, h_1, \ldots, h_{p-1} \) (thus \( v_i v_j = d_{ij} e_{(i+j+1)^*} \) unless \( (i + j + 1)^* = 0 \)). In particular, \( d_{ij} = 0 \) if \( i > p - 1 \) or \( j > p - 1 \). As with the \( c_{ij} \), we shall only consider \( d_{ij} \) with nonnegative subscripts.

To prove the conclusion of the lemma, it suffices to show that all \( d_{ij} \) vanish.

We have \( (v_i v'_j)e_k = (v_i e_k)v'_j + v_i(v'_j e_k) \); this gives
\[ [(i + j + 1)^* - k][(i + j + 1)^* + k]^k d_{ij} \]

(4.4)

\[ = [i + (k + 1)a]d_{i+k,j} + [j + (k + 1)a']d_{i,j+k}, \quad k \neq -1 \text{ or } i, j \neq 0, \]

where, for any integer \( i \), we write \( i^\pm = 1 \) if \( i < p - 1 \) and \( i^\pm = 0 \) if \( i \geq p - 1 \). If \( (i + j + 1)^* \neq -1 \) and \( k = -1 \) then the coefficient of \( d_{ij} \) in (4.4) is nonzero, so that if \( d_{i-1,j} = d_{i,j-1} = 0 \) then \( d_{ij} = 0 \) (if \( (i, k) = (0, -1) \) then \( d_{i-1,j} \) is replaced by \( d_{p-1,j} \), since the term in \( d_{i-1,j} \) in (4.4) must be replaced by \( bd_{p-1,j} \); similarly if \( (j, k) = (0, -1) \) then \( d_{i,j-1} \) is replaced by \( d_{i,p-1} \)). It follows by induction that to prove that all \( d_{ij} \) vanish it suffices to prove that \( d_{ij} = 0 \) whenever \( (i + j + 1)^* = -1 \).

Now suppose that \( (i + j + 1)^* = -1 \). With \( k = p - 2 \), (4.4) shows that \( d_{ij} = 0 \) unless one of \( i, j \) is 0 or 1. Hence by symmetry the only remaining \( d_{ij} \) that need to be considered are \( d_{1,p-3} \) and \( d_{0,p-2} \). With \( i = 1, j = p - 4 \) and \( k = 1 \), (4.4) gives \( 0 = (1 + 2a)d_{2,p-4} + (-4 + 2a')d_{1,p-3} \), and hence \( d_{1,p-3} = 0 \) unless \( a' = 2 \cdot 1 \). If \( a' = 2 \cdot 1 \) then, with \( i = 1, j = p - 5 \) (\( > 1 \) since \( p \geq 7 \)) and \( k = 2 \), (4.4) gives \( 0 = 0 + (-5 + 3a')d_{1,p-3} = d_{1,p-3} \). Hence always \( d_{1,p-3} = 0 \). Now with \( i = 0, j = p - 3 \) and \( k = 1 \), (4.4) gives \( 0 = 0 + (-3 + 2a')d_{0,p-2} \). Also with \( i = 0, j = p - 4 \) and \( k = 2 \), (4.4) gives \( 0 = 0 + (-4 + 3a')d_{0,p-2} \). Since either \( -3 + 2a' \neq 0 \) or \( -4 + 3a' \neq 0 \), \( d_{0,p-2} = 0 \). Hence always \( d_{ij} = 0 \) and the conclusion of the lemma holds in Case 4.

In the next three cases \( \Gamma_{\beta x} \) and \( \Gamma_{-\beta x} \) will be reducible of degree \( p \). We will take a basis \( v_0, \ldots, v_{p-1} \) of \( M_{\beta x} \) with multiplication as in the appropriate one of Cases 2 and 3, and similarly for a basis of \( M_{-\beta x} \), without the primes. We may write \( a = a' = 1 \). We shall use the same notation for \( d_{ij, i^*} \) and \( i^\pm \) as in Case 4, except that now since \( a + a' = 2 \) we must replace \( (i + j + 1)^* \) in the definition of \( d_{ij} \) by \( (i + j + 2)^* \).

Case 5. Degree \( p \), \( \Gamma_{\beta x} \) and \( \Gamma_{-\beta x} \) both having an invariant subspace of dimension \( p - 1 \):

The analogue of (4.4) holds, with \( (i + j + 1)^* \) replaced by \( (i + j + 2)^* \), except that the term in \( d_{i+k,j} \) or \( d_{i,j+k} \) is also changed if \( i = p - 1 \) or \( j = p - 1 \). As in Case 4, it suffices to prove that \( d_{ij} = 0 \) whenever \( (i + j + 2)^* = -1 \) and either \( i = 1 \) or \( i = 0 \) or, now, \( i = p - 1 \). Therefore we must consider \( d_{p-1,p-2} \), \( d_{1,p-4} \), and \( d_{0,p-3} \). With \( i = p - 1, j = p - 5 \) and \( k = 3 \), \( ((i + 2)^* + k)^* = 0 \), and the analogue of (4.4) gives \( 0 = b_3 d_{2,p-5} + (-5 + 4) d_{p-1,p-2} \), so that \( d_{p-1,p-2} = 0 \). With \( i = 1, j = p - 5 \) and \( k = 1 \), the analogue of (4.4) gives \( 0 = 0 + (-5 + 2)d_{1,p-4} \) and \( d_{1,p-4} = 0 \). Then with \( i = 0, j = p - 4, k = 1 \) we have \( 0 = 0 + (-4 + 2)d_{0,p-3} \). It follows that always \( d_{ij} = 0 \), and the conclusion of the lemma holds in Case 5.

Case 6. Degree \( p \), \( \Gamma_{\beta x} \) and \( \Gamma_{-\beta x} \) both having an invariant subspace of dimension one:
The analogue of (4.4) holds, with \((i + j + 1)^*\) replaced by \((i + j + 2)^*\), except that the term in \(d_{i+k,j}^1\) or \(d_{i,j+k}^1\) is also changed if \(i + k = p - 1\) or \(j + k = p - 1\). As before, it suffices to prove that \(d_{ij}^1 = 0\) whenever \((i + j + 2)^* = 1\) and either \(i = 1\) or \(i = 0\) (since, with \(k = p - 2\), \(i + k = p - 1\) only if \(i = 1\)). But this is shown exactly as in Case 5, and the conclusion of the lemma holds in Case 6.

Case 7. Degree \(p\), one of \(\Gamma_{\beta^a}\) having an invariant subspace of dimension \(p - 1\), the other having an invariant subspace of dimension one:

This case is handled as in Cases 5 and 6. Suppose \(\Gamma_{\beta^a}\) has the \((p - 1)\)-dimensional invariant subspace. Then we need only show that \(d_{p-1,p-2} = d_{1,p-4} = d_{0,p-3} = 0\), and this is shown exactly as in Case 5. Hence the conclusion of the lemma holds in Case 7.

Case 8. Both \(\Gamma_{\beta^a}\) and \(\Gamma_{-\beta^a}\) have degree \(p - 1\):

We simply set \(v_{p-1} = v_{p-1}' = 0\) and use the proof in Case 5. Hence the lemma’s conclusion holds in Case 8.

We have considered all possibilities for \(\Gamma_{\beta^a}\) and \(\Gamma_{-\beta^a}\). Thus the lemma is proved.

5. Existence of a direct summand of rank one.

**Lemma 5.1.** Suppose that \(\alpha\) and \(\beta\) are roots such that the root spaces \(L_{\alpha^a}\) generate a Witt algebra \(W_x\). If \(\beta + ia\) is also a root for some \(i = 1, \ldots, p - 1\), then all \(\beta + ia\) are roots and (more important) \(L_{\beta^a}L_{-\beta^a} \subseteq W_x\).

**Proof.** We shall use the notation \(M_{\beta^a}, M_{-\beta^a}\) as in Lemma 4.1. Suppose that the hypotheses hold but that \(L_{\beta^a}L_{-\beta^a} \not\subseteq W_x\). Take nonzero elements \(u_\beta\) in \(L_{\beta^a}\), \(u_{\beta + ia}\) in \(L_{\beta + ia}\), and \(u_{-\beta}\) in \(L_{-\beta}\), and write \(u_{\beta}u_{-\beta} = h_\beta\). Then \(\beta(h_\beta) \neq 0\) by (A) but \(\alpha(h_\beta) = 0\) by Lemma 4.1, so that \((\beta + ia)(h_\beta) \neq 0\). By the Jacobi identity,

\[
(u_{\beta}u_{\beta + ia})u_{-\beta} = (u_{\beta}u_{-\beta})u_{\beta + ia} + u_{\beta}(u_{\beta + ia}u_{-\beta}).
\]

But \(u_{\beta + ia}u_{-\beta} \in L_{\alpha^a} \cap M_{\beta^a}M_{-\beta^a}\), which vanishes by Lemma 4.1. Therefore, \((u_{\beta}u_{\beta + ia})u_{-\beta} = h_\beta u_{\beta + ia} = -\beta(\beta + ia)(h_\beta)u_{\beta + ia} \neq 0\) and hence \(2\beta + ia\) is a root. Since \(\dim M_{\beta^a} > 1\), \(\dim M_{-\beta^a} \geq p - 1\). It follows that \(\dim M_{2\beta^a} \geq p - 2\), so that there are distinct roots \(\beta + ja\) and \(\beta + ka\) such that \(2\beta + 2ja\) and \(2\beta + 2ka\) are roots. By Lemma 2.2, \(L_{\beta + ja}\) and \(L_{2\beta + 2ja}\) generate a Witt algebra \(W_{\beta + ja}\), and similarly we get \(W_{\beta + ka}\). By Lemma 4.1, \(\alpha(L_{\beta + ja}L_{-\beta - ja}) = 0\) and so \(L_{\alpha}L_{-\alpha} \not\subseteq W_{\beta + ja}\).

We may now apply Lemma 4.1 to \(W_{\beta + ja}\) and \(M_{\alpha,\beta + ja}M_{-\alpha,\beta + ja}\) and conclude that \((\beta + ja)(L_{\alpha}L_{-\alpha}) = 0\). Similarly we have \((\beta + ka)(L_{\alpha}L_{-\alpha}) = 0\). This implies that \(\alpha(L_{\alpha}L_{-\alpha}) = 0\), contradicting (A). This proves the last statement of the lemma.

If not all \(\beta + ia\) are roots then \(M_{\beta^a}\) and \(M_{-\beta^a}\) both have dimension \(p - 1\) and so are as in Case 8 of the proof of Lemma 4.1. But the treatment of Case 8 did not use the hypothesis of Lemma 4.1 that \(M_{\beta^a}M_{-\beta^a} \not\subseteq W_x\), and showed that \(\alpha(L_{\alpha}L_{-\alpha}) = 0\). But \(L_{\beta}L_{-\beta} \subseteq W_x\), and so, by (A), \(\alpha(L_{\beta}L_{-\beta}) \neq 0\), a contradiction. Thus the lemma is proved.
We are now ready to complete the proof that, under the hypotheses of the main theorem and the assumption that the base field is algebraically closed, \( L \) is a direct sum of algebras which are either simple of classical type or of rank one. Suppose that \( L \) is not a direct sum of simple algebras of classical type. Then by Lemmas 2.1 and 2.2, there is a root \( \alpha \) such that the root spaces \( L_\alpha, L_{2\alpha}, \ldots, L_{(p-1)\alpha} \) generate a Witt algebra \( W_\alpha \). For each nonzero root \( \beta \) let \( h_\beta \) be a nonzero element of \( L_\beta L_{-\beta} \), and write

\[
S = \{ \beta \mid \beta \text{ a root}, \beta \neq 0, \ h_\beta \in (h_\alpha) \}, \quad K = (h_\alpha) + \sum_{\beta \in S} L_\beta.
\]

If \( \beta, \gamma \in S \) and \( L_\beta L_\gamma \neq 0 \) then \( \beta + \gamma \) is a root and \( (L_\beta L_\gamma)L_{-\beta-\gamma} \subseteq (L_\beta L_{-\beta})L_\gamma + L_\beta(L_{-\beta}L_{-\gamma}) \subseteq L_{-\beta}L_\gamma + L_\beta L_{-\gamma} \subseteq (h_\alpha) \). Hence \( K \) is a subalgebra of \( L \). Since \( \beta(h_\alpha) \neq 0 \) if \( \beta \in S \), it follows that \( (h_\alpha) \) is a Cartan subalgebra of \( K \). If \( \beta \in S \) and \( \beta \) is not of the form \( i\alpha \), write

\[
J_\beta = \left( \sum_{i,j} L_{i\alpha + j\beta} \right) \cap K.
\]

Then \( J_\beta \) is a subalgebra of \( K \) and \( (h_\alpha) \) is also a Cartan subalgebra of \( J_\beta \). By a result of Kaplansky [6, Theorem 4, p. 164] on Lie algebras of rank one, the roots form a group, so that \( J_\beta \) has dimension \( p^2 \), and all \( i\beta \) are roots (this may also be proved more directly with the use of the Weyl-Jacobson lemma). If \( \beta \in S, \gamma \notin S \) and \( \gamma \neq 0 \), then \( L_{i\beta} L_{-\gamma} \neq W_\beta \), and so, by Lemma 5.1, \( L_{i\beta} W_\beta = 0 \).

Now let \( K^* \) be the subalgebra of \( L \) generated by all \( L_\gamma \) such that \( \gamma \notin S \) and \( \gamma \neq 0 \). Then \( K^*K = 0 \). Every \( L_\delta (\delta \neq 0) \) is contained in \( K \) or \( K^* \), and since \( H \) is spanned by the \( L_\delta \) because \( L = L^2 \), we have \( K + K^* = L \). Since \( KK^* = 0 \) and \( L \) is centerless, \( K \cap K^* = 0 \), and hence \( L \) is the direct sum of the ideals \( K \) and \( K^* \). It is easy to see that the rank one algebra \( K \) is simple, or this may be concluded by using [2]. Therefore by induction it follows that \( L \) is a direct sum of simple algebras which are either of classical type or have rank one.

Now suppose that the base field \( F \) is not algebraically closed, and let \( E \) be its algebraic closure. It is obvious that \( L_E \) satisfies axioms (i) and (A), with respect to \( H_E \). Since by (ii) the roots span the dual space of \( H \), no nonzero element of \( H_E \) is annihilated by all roots, and it follows that \( L_E \) also satisfies axiom (ii). For each of the simple direct summands \( L^i(E) \) of \( L_E \), let \( L_i \) be the subalgebra of \( L \) generated by all \( L_\alpha \) for nonzero roots such that \( (L_\alpha)_E \) is in \( L^i(E) \). Then \( (L_i)_E = L^i(E), \ L_i \) is simple, and \( L \) is a direct sum of the \( L_i \). Moreover, \( L_i \) is of classical type or of rank one according as \( L^i(E) \) is, and \( L_i \) satisfies our axioms.

The only thing we need to do to complete the proof of the main theorem is to show that if \( F \) is perfect and \( L \) has a one-dimensional Cartan subalgebra \( H = (u_0) \) such that Axiom (A) is satisfied, then \( L \) is an Albert-Zassenhaus algebra.

Let \( E \) be the algebraic closure of \( L \). Then by [2] \( L_E \) is an Albert-Zassenhaus algebra, the roots of \( L \) with respect to \( H \) form a group, and \( L_E \) has a basis \( \{u_\alpha\} \) containing \( u_0 \) and satisfying (1.1), where each root \( \alpha \) is identified with the scalar
\( \alpha(u_0) \) and \( u_a \in (L_a)_F \). The facts in [9, pp. 42-47] used in the proof of Lemma 3.1 of [2] are valid for \( F \) perfect. Hence elements \( u_{ia} \) in \( L_{ia} \) \((i = 0, \ldots, p-1)\), with \( u_0 = u_0 \), may be chosen so that \( u_{ia}u_{ja} = (i - j)\alpha u_{ia+j} \), and this choice is unique even among elements in \( (L_{ia})_F \). It follows that \( u_{ia} = u_{ia} \in L_{ia} \). Hence the basis elements \( u_a \) are in \( L \), so that \( L \) is an Albert-Zassenhaus algebra. This completes the proof of the main theorem.

6. Remarks on representations of the Witt algebra and on algebras of rank one.
We shall now indicate the form that Theorem 3.1, on the representations of the Witt algebra \( W \), takes when the representations are expressed in terms of the basis elements \( f_0, \ldots, f_{p-1} \) of \( W \) having multiplication table (2.3).

Let \( Z \) be a vector space over the base field \( F \) of \( W \), with basis \( z_0, z_1, \ldots, z_{p-1} \), and let \( a \) and \( c \) be given scalars. For each \( f_j \) define a linear transformation on \( Z \) by setting (for \( i = 0, \ldots, p-1 \))

\[
(6.1) z_{i+f_j} = (c + i + ja)z_{i+j},
\]

where all subscripts are taken modulo \( p \). Then we claim that the linear mapping \( \Omega = \Omega_{ac} \), determined by (6.1), of \( W \) to linear transformations on \( Z \), is a representation of \( W \). This may be shown directly, or if \( c \notin F_p \), by the use of part of the multiplication table of a suitable Albert-Zassenhaus algebra, as in [2, p. 22]. If \( c \in F_p \), one of the more general Lie algebras of [1, Theorem 9, p. 133] may be used in the same way to show that \( \Omega \) is a representation.

If \( c = 0 \) and \( a = 1 \) then \( z_1, \ldots, z_{p-1} \) span an invariant \((p-1)\)-dimensional subspace of \( Z \). We shall denote by \( \Omega_{10} \) the restriction of \( \Omega_{10} \) to this subspace. Since the subspace contains no one-dimensional invariant subspace \( \Omega_{10} \) is irreducible and equivalent to \( \Delta_{10} \).

Theorem 6.1. Let \( W \) be the Witt algebra over an algebraically closed field \( F \) of characteristic \( p > 3 \). The nontrivial irreducible representations of \( W \) of degree not greater than \( p \) are, up to equivalence, the mappings \( \Omega_{ac} \) \((a, c \in F; c \notin F_p \) or \( a \neq 0, 1) \) and \( \Omega_{10} \). The irreducible representation \( \Omega_{ac} \) is equivalent to the representation \( \Delta_{ab} \) of Theorem 3.1 where \( b = c^p - a^p - (c - a) \). Two irreducible representations \( \Omega_{a_1c_1} \) and \( \Omega_{a_2c_2} \) are equivalent if and only if \( c_2 = c_1 + i \), for some \( i \) in \( F_p \), and either \( a_1 = a_2 \) or \( (a_1, a_2) = (0, 1) \) or \( (1, 0) \).

Proof. Let \( \Omega = \Omega_{ac} \) be one of the representations defined above. Since \( e_{-1} = f_{-1} \), \( \left[ \Omega_{ac}(e_{-1}) \right]^p = e_{-1}I \) where \( e_{-1} = \prod_i(e + i - a) = c^p - a^p - (c - a) \). Write \( z = z_0 + \cdots + z_{p-1} \). By (2.5), \( e_0 = f_0 - f_{-1} \), \( e_1 = f_1 - 2f_0 + f_{-1} \) and \( e_2 = f_2 - 3f_1 + 3f_0 - f_{-1} \). Thus \( ze_0 = \sum[(e + i)z_{i} - (c + i - a)z_{i-1}] = (a - 1)z \), and similarly it may be seen that \( ze_1 = ze_2 = 0 \). If \( Z \) contains a one-dimensional subspace invariant under all \( \Omega_{ac}(f_j) \) then the subspace is spanned by some \( z_i \) with \( c + i = c + i + a = 0 \). Now suppose that \( c \notin F_p \) or \( a \neq 0 \), and that \( Z \) contains a proper invariant subspace \( Z' \). Then \( Z' \) has dimension \( p-1 \) and is irre-
ducible, the restriction of $\Omega$ to $Z'$ is equivalent to $\Delta'_{10}$, and $ze_0 \in Z'$. If $z \not\in Z'$ then $a = 1$, while if $z \in Z'$ then $z$ must correspond to a scalar multiple of $v_{p-2}$ under the equivalence with $\Delta'_{10}$, so that $a = 0$. But $c^p - a^p - (c-a) = 0$, so that $c \in F_p$.

It follows that if $c \notin F_p$ or $a \neq 0,1$ then $\Omega_{ac}$ is irreducible. Comparing $z$ with $v$ of Lemma 3.1, we see that $\Omega_{ac}$ is equivalent to $\Delta_{ab}$, where $b = e_{-1} = c^p - a^p - (c-a)$. The rest of the theorem follows immediately from Theorem 3.1 and the fact that if $c$ is a root of $(x - a)^p - (x - a) = b$ then the other roots are $c + i$ for $i$ in $F_p$. Thus the theorem is proved.

As with Corollary 3.1, there is an immediate consequence for restricted representations.

**Corollary 6.1.** Any (nontrivial) irreducible restricted representation of the Witt algebra, over an algebraically closed field of characteristic $p > 3$, is equivalent to one of $\Omega_{10}, \Omega_{20}, \ldots, \Omega_{-1,0}$. These $p - 1$ representations are inequivalent and irreducible, and are equivalent to $\Delta_{10}, \Delta_{20}, \ldots, \Delta_{-1,0}$, respectively.

In [2] an important tool in the proof is the use of the formulas (6.1) above for the representations $\Omega_{ac}$ with $c \notin F_p$. The proof in [2], at least for $p > 5$, could be brought into closer relationship with the proof in the present paper by using Theorem 6.1 above. This remark refers principally to the proof in [2, pp. 25–29] that $\Omega$ is skew-symmetric. That proof could be somewhat simplified by using arguments just like that in Case 4 of Lemma 4.1 above to eliminate all except a couple of possible values for $f(\alpha, \beta) + f(-\alpha, \beta)$. For the remaining values the system of $d_{ij}$’s, and hence the $u_{a + i\beta}u_{-a + j\beta}$, are determined uniquely up to scalar multiple. A computation in two ways of $(u_{i\beta}u_{a})u_{-a}$ then leads to the conclusion that $\Omega$ is skew-symmetric.

**References**


University of Illinois, Urbana, Illinois