RESTRICTED LIE ALGEBRAS OF CHARACTERISTIC p

BY

N. JACOBSON

In an earlier paper[1] [3] we noted certain identities which connect addition, scalar multiplication, commutation ($[ab]=ab-ba$), and pth powers in an arbitrary associative algebra of characteristic p ($\neq 0$). These lead naturally to the definition of a class of abstract algebras called restricted Lie algebras which in many respects bear a closer relation to Lie algebras of characteristic 0 than ordinary Lie algebras of characteristic p.

As is shown in the present paper any restricted Lie algebra $\mathfrak{L}$ may be obtained from an associative algebra by using the operations mentioned above. In fact $\mathfrak{L}$ determines a certain associative algebra $\mathfrak{U}$, called its u-algebra, such that $\mathfrak{L}$ is isomorphic to a subalgebra of $\mathfrak{U}_l$, the restricted Lie algebra defined by $\mathfrak{L}$; and if $\mathfrak{B}$ is any associative algebra such that $\mathfrak{B}_l$ contains a subalgebra homomorphic to $\mathfrak{L}$ and $\mathfrak{B}$ is the enveloping algebra of this subset then $\mathfrak{U}$ is homomorphic to $\mathfrak{B}$. The algebra $\mathfrak{U}$ has an anti-automorphism relative to which the elements corresponding to those in $\mathfrak{L}$ are skew. For ordinary Lie algebras an algebra having these properties has been defined by G. Birkhoff [2] and by Witt [5]. In their case however, the associative algebra has an infinite basis even when the Lie algebra has a finite basis whereas here $\mathfrak{U}$ has a finite basis if and only if $\mathfrak{L}$ has. Consequently every restricted Lie algebra $\mathfrak{L}$ with a finite basis has a (1-1) representation by finite matrices. The theory of representations of $\mathfrak{L}$ can be reduced to that of the associative algebra $\mathfrak{U}$. Thus, for example, there are only a finite number of inequivalent irreducible representations.

The most natural way to obtain a restricted Lie algebra is as a derivation algebra of an arbitrary algebra $\mathfrak{A}$, i.e., as the set of transformations $D: a\rightarrow aD$ in $\mathfrak{A}$ such that

$$(a+b)D = aD + bD, \qquad (a\alpha)D = (aD)\alpha, \qquad (ab)D = (aD)b + a(bD).$$

If $\mathfrak{A}=\mathfrak{L}$ is itself restricted ($ab=[ab]$) the derivations which satisfy

$$a^pD = [[aD, \overbrace{a]a]\cdots a}^{p-1}]$$

are called restricted. They are precisely the derivations of $\mathfrak{L}$ which can be extended to derivations of the u-algebra $\mathfrak{U}$. Hence their totality is a restricted Lie algebra $\mathfrak{D}_0$. Using $\mathfrak{D}_0$ and $\mathfrak{L}$ we may define a restricted holomorph $\mathfrak{H}_0$ of $\mathfrak{L}$. $\mathfrak{H}_0$ is a restricted Lie algebra.

Presented to the Society, September 12, 1940; received by the editors June 30, 1940.

(1) Numbers in brackets refer to the bibliography at the end of the paper.

The considerations in the present paper apply for the most part to restricted Lie algebras with an infinite basis as well as to those with a finite basis. A special result, however, for Lie algebras with a finite basis is that the nilpotency of $\mathfrak{L}$ implies that of the u-algebra (§6). In a later paper we hope to discuss certain classes of simple restricted Lie algebras with a finite basis.

1. **Restricted Lie algebras. Definitions.** If $\mathfrak{A}$ is an associative algebra and the commutator $[ab]=ab-ba$, it is well known that

$$[ab] = -[ba], \qquad [a[bc]] + [b[ca]] + [c[ab]] = 0.$$

If, in addition $\mathfrak{A}$ has characteristic p ($\neq 0$) then the following identities hold:

$$(a+b)^p = a^p + b^p + s(a, b), \qquad [\overbrace{[ab]b]\cdots b}^{p}] = [ab^p],$$

where $s(a, b) = s_1(a, b) + s_2(a, b) + \cdots + s_{p-1}(a, b)$ and the $(p-i)s_i(a, b)$ is the coefficient of λ^{p-i-1} in

$$[\cdots [a, \lambda a + b], \lambda a + b], \cdots, \lambda a + b]$$

([3], and [6]). We are thus led to define a *restricted Lie algebra* $\mathfrak{L}$ over a field Φ of characteristic p as a vector space over Φ in which operations $[ab]$ and $a^{[p]}$ are defined such that

$$(1) \qquad [ab] = -[ba], \qquad [a[bc]] + [b[ca]] + [c[ab]] = 0,$$

$$(2) \qquad [a, b_1 + b_2] = [ab_1] + [ab_2],$$

$$(3) \qquad [ab]\alpha = [a, b\alpha] = [a\alpha, b], \qquad \alpha \text{ in } \Phi,$$

$$(4) \qquad (a+b)^{[p]} = a^{[p]} + b^{[p]} + s(a, b),$$

$$(5) \qquad (a\alpha)^{[p]} = a^{[p]}\alpha^p,$$

$$(6) \qquad [\cdots[\overbrace{ab]b]\cdots b}^{p}] = [ab^{[p]}].$$

A subspace $\mathfrak{B}$ of $\mathfrak{L}$ is a *subalgebra* if $\mathfrak{B} \supset b^{[p]}$ and $[b_1b_2]$ for all b, b_1, b_2 in $\mathfrak{B}$. $\mathfrak{B}$ is an *ideal* if it contains also $[ba]$ for all b in $\mathfrak{B}$, a in $\mathfrak{L}$. A correspondence $a \rightarrow a^S$ between two restricted Lie algebras is a *homomorphism* if

$$(7) \qquad \begin{gathered} (a+b)^S = a^S + b^S, \qquad (a\alpha)^S = a^S\alpha, \qquad [ab]^S = [a^Sb^S], \\ (a^{[p]})^S = (a^S)^{[p]}. \end{gathered}$$

If S is (1-1) it is an *isomorphism* and if besides S is a correspondence within $\mathfrak{L}$ it is an *automorphism*.

If $x_1, x_2, \cdots$ (possibly infinite) is a basis for $\mathfrak{L}$, then $[x_ix_j] = \sum x_q\gamma_{qij}$, $x_i^{[p]} = \sum x_r\mu_{ri}$ (finite sums) where

$$(8) \qquad \gamma_{qij} = -\gamma_{qji}, \qquad \sum_q \gamma_{rqk}\gamma_{qij} + \sum_q \gamma_{rqi}\gamma_{qjk} + \sum_q \gamma_{rqj}\gamma_{qki} = 0,$$

$$(9) \qquad \sum_r \gamma_{sir}\mu_{rj} = \sum_q \gamma_{sq_{p-1}j}\gamma_{q_{p-1}q_{p-2}j}\cdots\gamma_{q_1ij}.$$

These equations are equivalent to

$$[x_ix_j] = -[x_jx_i],$$

$$[[x_ix_j]x_k] + [[x_jx_k]x_i] + [[x_kx_i]x_j] = 0, \quad [x_ix_j^{[p]}] = [\cdots[x_ix_j]\cdots x_j],$$

respectively. The γ's and μ's are the *constants of multiplication* of $\mathfrak{L}$. If $a\to a^S$ is an isomorphism between $\mathfrak{L}$ and $\mathfrak{L}^S$, $x_1^S, x_2^S, \cdots$ form a basis for $\mathfrak{L}^S$ and the x_i^S have the same constants of multiplication as the x_i's. On the other hand if $\mathfrak{M}$ is any restricted Lie algebra with basis $y_1, y_2, \cdots$ in (1-1) correspondence with the x_i such that $[y_iy_j]=\sum y_q\gamma_{qij}$, $y_i^{[p]}=\sum y_r\mu_{ri}$ then it is readily seen that the correspondence $\sum x_i\alpha_i\to\sum y_i\alpha_i$ is an isomorphism.

We have noted above that any associative algebra $\mathfrak{A}$ of characteristic p becomes a restricted Lie algebra $\mathfrak{A}_l$ when $[ab]$ is defined as $ab-ba$ and $a^{[p]}=a^p$. A homomorphism between $\mathfrak{L}$ and a subalgebra of Φ_{nl}, Φ_n the algebra of $n\times n$ matrices, is called a *representation*. Irreducibility, decomposability, equivalence, etc., of representations are defined as usual. As is well known these depend on the irreducibility, etc., of the enveloping algebra of the representing matrices.

2. **The u-algebra of a restricted Lie algebra.** Let $x_1, x_2, \cdots$ (possibly infinite) be a basis over Φ of a vector space $\mathfrak{L}$. We set $[x_ix_j]=\sum x_q\gamma_{qij}$ and $x_i^{[p]}=\sum x_r\mu_{ri}$ where the γ's are μ's satisfy (8) and (9). Then for $a=\sum x_i\alpha_i$, $b=\sum x_i\beta_i$ (finite sums) we set $[ab]=\sum x_k\gamma_{kij}\alpha_i\beta_j$. Evidently (8) implies that $\mathfrak{L}$ is a Lie algebra relative to $[ab]$. Equation (9) is equivalent to

$$[x_ix_j^{[p]}] = [\cdots\overbrace{[x_ix_j]\cdots x_j}^{p}].$$

We shall show that $\mathfrak{L}$ is a restricted Lie algebra relative to a suitable definition of $a^{[p]}$.

Let $\mathfrak{A}$ be the vector space with the basis $x_1^{\kappa_1}x_2^{\kappa_2}\cdots x_n^{\kappa_n}$, $\kappa_i\geqq 0$ integers and at least one $\kappa_i>0$, $n=1, 2, \cdots$. If only a finite number of monomials are being considered we may write them in terms of the same x's. A product

$$(x_1^{\kappa_1}x_2^{\kappa_2}\cdots x_n^{\kappa_n})(x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n})$$

is defined by repeated "straightenings," i.e., substitutions for x_ix_j when $i>j$ of the expression $x_jx_i+\sum x_k\gamma_{kij}$. It has been shown by G. Birkhoff [2] and by Witt [5] that this product is uniquely defined in $\mathfrak{A}$ and is associative.

Let $\mathfrak{B}$ be the ideal in $\mathfrak{A}$ having the basis $y_i=x_i^p-x_i^{[p]}$. Since

$$[bx_i^p] = [\cdots[bx_i]x_i]\cdots x_i] = [bx_i^{[p]}], \tag{10}$$

y_i commutes with every linear b and hence with every element of $\mathfrak{A}$.

If the term $x_1^{\kappa_1}\cdots x_n^{\kappa_n}$ has degree $\geqq p$ in x_i we may replace x_i^p by $y_i+x_i^{[p]}$. After a finite number of such substitutions we may write any $a=\sum x_1^{\kappa_1}\cdots x_n^{\kappa_n}$

$\cdot\rho_{\kappa_1\cdots\kappa_n}$ in the form $\sum x_1^{\lambda_1}\cdots x_n^{\lambda_n}u_{\lambda_1\cdots\lambda_n}$ where $\lambda_i<p$ and the u's are polynomials in $y_1, y_2, \cdots, y_n$. Thus any $b=\sum a_iy_i+\sum y_i\alpha_i$ in $\mathfrak{B}$ has the form $\sum x_1^{\lambda_1}\cdots x_n^{\lambda_n}\cdot v_{\lambda_1\cdots\lambda_n}$, v a polynomial in $y_1, y_2, \cdots, y_n$ with no constant term. Now

$$\begin{aligned} x_1^{\lambda_1}\cdots x_n^{\lambda_n}y_1^{m_1}\cdots y_n^{m_n} &= x_1^{\lambda_1}(x_1^p - x_1^{[p]})^{m_1}\cdots x_n^{\lambda_n}(x_1^p - x_1^{[p]})^{m_n} \\ &= x_1^{\lambda_1+pm_1}\cdots x_n^{\lambda_n+pm_n}+\cdots \end{aligned}$$

where the terms not indicated have degree $<\sum\lambda_i+p\sum m_i$. Consider the terms of maximum degree $N=\sum\lambda_i+p\sum m_i$ in b where we suppose $b\neq 0$ and hence one of the v's is $\neq 0$. Since at least one $m>0$, $N>p$. Two terms of maximum degree are different if $(\lambda_1, \cdots, \lambda_n; m_1, \cdots, m_n)\neq(\lambda_1', \cdots, \lambda_n'; m_1', \cdots, m_n')$. Hence these terms occur only once and can not cancel off. It follows that when b is written in its normal form $\sum x_1^{\kappa_1}\cdots x_n^{\kappa_n}\rho_{\kappa_1\cdots\kappa_n}$ at least one of the x's has degree $>p$. Thus the classes $\{x_1^{\lambda_1}\cdots x_n^{\lambda_n}\}$, $\lambda_i<p$, omitting $\{x_1^0\cdots x_n^0\}$, determined by the elements $x_1^{\lambda_1}\cdots x_n^{\lambda_n}$ modulo $\mathfrak{B}$ form a basis for the difference algebra $\mathfrak{U}=\mathfrak{A}/\mathfrak{B}$.

Since the classes $\{x_1\}, \{x_2\}, \cdots$ are linearly independent and $[\{x_i\}\{x_j\}]=\sum\{x_q\}\gamma_{qij}$ the correspondence $\sum x_i\alpha_i\rightarrow\sum\{x_i\}\alpha_i$ is an isomorphism between $\mathfrak{L}$ and an ordinary Lie subalgebra $\{\mathfrak{L}\}$ of $\mathfrak{U}_l$. Since $\{x_i\}^p=\{x_i^p\}=\{x_i^{[p]}\}=\sum\{x_r\}\mu_{ri}$, $\{\mathfrak{L}\}$ is a (restricted) subalgebra of $\mathfrak{U}_l$. Hence if we define $(\sum x_i\alpha_i)^{[p]}$ as the element corresponding to $\{\sum x_i\alpha_i\}^p$, $\mathfrak{L}$ becomes a restricted Lie algebra in which $x_i^{[p]}$ is as originally given.

If $\mathfrak{L}$ is a restricted Lie algebra to begin with, then the correspondence $\sum x_i\alpha_i\rightarrow\{\sum x_i\alpha_i\}$ is an isomorphism. Now suppose $\sum x_i\alpha_i\rightarrow\sum\bar{x}_i\alpha_i$ is a homomorphism between $\mathfrak{L}$ and $\bar{\mathfrak{L}}$, a subalgebra of $\mathfrak{B}_l$, where we suppose that any element of $\mathfrak{B}$ is a polynomial in the elements of $\bar{\mathfrak{L}}$. We have

$$\bar{x}_i\bar{x}_j = \bar{x}_j\bar{x}_i + \sum \bar{x}_q\gamma_{qij}, \qquad \bar{x}_i^p = \sum \bar{x}_r\mu_{ri}.$$

The first set of equations implies that $\sum x_1^{\kappa_1}\cdots x_n^{\kappa_n}\rho_{\kappa_1\cdots\kappa_n}\rightarrow\sum\bar{x}_1^{\kappa_1}\cdots\bar{x}_n^{\kappa_n}\rho_{\kappa_1\cdots\kappa_n}$ is a homomorphism between $\mathfrak{A}$ and $\mathfrak{B}$(2). Because of the second set of equations $x_i^p-x_i^{[p]}$ are mapped into 0 and so our correspondence induces a homomorphism between $\mathfrak{U}=\mathfrak{A}/\mathfrak{B}$ and $\mathfrak{B}$. This mapping is an extension of the homomorphism between $\mathfrak{L}$ and $\bar{\mathfrak{L}}$. Thus we have proved the following theorem.

THEOREM 1. *If $\mathfrak{L}$ is a restricted Lie algebra there exists an associative algebra $\mathfrak{U}$ having the following properties*: 1. *$\mathfrak{L}$ is isomorphic to a subalgebra $\{\mathfrak{L}\}$ of $\mathfrak{U}_l$*. 2. *$\mathfrak{U}$ is the enveloping algebra of $\{\mathfrak{L}\}$*. 3. *If $\mathfrak{L}$ is homomorphic to a subalgebra $\bar{\mathfrak{L}}$ of any $\mathfrak{B}_l$ where $\mathfrak{B}$ is the enveloping algebra of $\mathfrak{L}$, then $\mathfrak{U}$ is homomorphic to $\mathfrak{B}$.*

This theorem shows that conditions (1) to (6) are characteristic of the functions $a+b$, $a\alpha$, $[ab]$ and a^p in an associative algebra of characteristic p. The above considerations show also that equations (8) and (9) on the con-

(2) See [2] or [5].

stants γ and μ insure that the vector space $\mathfrak{L}$ be a restricted Lie algebra. If P is an extension of the field Φ the extended vector space of elements of the form $\sum x_i\xi_i$, ξ in P, is a Lie algebra over P. We denote this extended algebra as $\mathfrak{L}$P since, as is easily shown, it does not depend on the particular choice of basis. In the remainder of the paper we shall denote $a^{[p]}$ by a^p when there is no risk of confusion and shall call $\mathfrak{U}$ the u-algebra of $\mathfrak{L}$.

Suppose $x_{i_1} \cdots x_{i_m}$ is a monomial in $\mathfrak{A}$ and the first x_1 in this product occurs in the r_1th place. Then we may straighten this term by interchanging x_1 successively with the r_1-1 terms in front of it and obtain a polynomial in the x's having one term $x_1x_{j_2} \cdots x_{j_m}$ of degree m. We define the rank of $x_{i_1} \cdots x_{i_m}$ inductively as (r_1-1) plus rank of $x_{j_2} \cdots x_{j_m}$. A monomial of rank 0 is said to be in canonical form. Then $i_1 \geqq i_2 \geqq \cdots \geqq i_m$. Consider the correspondence $a=\sum x_1^{\kappa_1} \cdots x_n^{\kappa_n}\rho_{\kappa_1 \cdots \kappa_n} \rightarrow a^J=\sum(-1)^{\kappa_1+\cdots+\kappa_n}x_n^{\kappa_n} \cdots x_1^{\kappa_1}\rho_{\kappa_1\cdots\kappa_n}$. Evidently J is linear. We wish to show that it is an anti-automorphism. For this purpose it suffices to prove that

$$(x_{i_1} \cdots x_{i_m})^J = (-1)^m x_{i_m} \cdots x_{i_1}.$$

Suppose this holds for all products of $(m-1)$ or less x's and also for products of m x's whose ranks are less than those of the given monomial. Then

$$(x_{i_1} \cdots x_{i_m}) = (x_{i_1} \cdots x_{i_{j+1}}x_{i_j} \cdots x_{i_m}) + (x_{i_1} \cdots [x_{i_j}x_{i_{j+1}}] \cdots x_{i_m}),$$

where we may suppose that if the rank r of the original term is >0 that of $x_{j_1} \cdots x_{i_{j+1}}x_{i_j} \cdots x_{i_m}$ is $r-1$. We have

$$\begin{aligned}(x_{i_1} \cdots x_{i_m})^J &= (x_{i_1} \cdots x_{i_{j+1}}x_{i_j} \cdots x_{i_m})^J + (x_{i_1} \cdots [x_{i_j}x_{i_{j+1}}] \cdots x_{i_m})^J \\ &= (-1)^m(x_{i_m} \cdots x_{i_j}x_{i_{j+1}} \cdots x_{i_1}) \\ &\quad + (-1)^{m-1}(x_{i_m} \cdots [x_{i_j}x_{i_{j+1}}] \cdots x_{i_1}) \\ &= (-1)^m(x_{i_m} \cdots x_{i_1}).\end{aligned}$$

Since $(x_i^{[p]}-x_i^p)^J=-(x_i^{[p]}-x_i^p)$, J sends the ideal $\mathfrak{B}$ into itself and therefore induces an anti-automorphism in $\mathfrak{U}=\mathfrak{A}/\mathfrak{B}$. The elements $\sum\{x_i\}\alpha_i$ of $\{\mathfrak{L}\}$ are skew relative to the anti-automorphism.

By property (3) of $\mathfrak{U}$ any representation of $\mathfrak{L}$ determines a representation of $\mathfrak{U}$ and conversely. Questions of irreducibility, equivalence, etc., for $\mathfrak{L}$ are reducible to the corresponding questions for $\mathfrak{U}$. If $\mathfrak{L}$ has a finite basis x_1, $x_2, \cdots, x_n$, $\mathfrak{U}$ has the basis $\{x_1^{\lambda_1} \cdots x_n^{\lambda_n}\}$ $(\lambda_i<p)$ of p^n-1 elements. Since $\mathfrak{U}$ has a (1-1) representation in some Φ_m, $m \leqq p^n$, the same is true for $\mathfrak{L}$.

THEOREM 2. *Every restricted Lie algebra with a finite basis has a* (1-1) *representation.*

The number of inequivalent irreducible representations $(\neq 0)$ of $\mathfrak{U}$ is equal to the number of simple components of $\mathfrak{U}/\mathfrak{N}$, $\mathfrak{N}$ the radical of $\mathfrak{U}$. This implies

THEOREM 3. *There are only a finite number of inequivalent irreducible representations of a restricted Lie algebra with a finite basis.*

Example. $\mathfrak{L}$, the restricted Lie algebra with the basis x, y, z such that

$$[xy] = z, \qquad [xz] = [yz] = 0, \qquad x^p = y^p = z^p = z.$$

$\mathfrak{U}$ has the basis $x^iy^jz^k$, $i, j, k<p$ such that the above relations hold, it being understood that $[xy]=xy-yx$, etc. It is readily proved that $\mathfrak{U}$ is a direct sum of p algebras with bases x^iy^j such that

$$xy - yx = \zeta, \qquad x^p = y^p = \zeta,$$

where $\zeta=0, 1, \cdots, p-1$ in turn. If $\zeta=0$ this algebra is nilpotent. Otherwise it is isomorphic to Φ_p. Hence there are $(p-1)$ inequivalent irreducible representations of $\mathfrak{L}$.

Theorem 2 is valid for Lie algebras of characteristic 0 though its proof given by Ado [1] is considerably more complicated than the present one. Theorem 3 is not true for algebras of characteristic 0. It is not known whether either of these results holds for ordinary Lie algebras of characteristic p.

3. **Ideals. Nilpotency.** If $\mathfrak{B}$ is an ideal in $\mathfrak{L}$ we define the sum, scalar product and commutator of the classes $\bar{a}$ modulo $\mathfrak{B}$ as usual by

$$\bar{a}_1 + \bar{a}_2 = \overline{a_1 + a_2}, \qquad \bar{a}\alpha = \overline{a\alpha}, \qquad [\bar{a}_1\bar{a}_2] = [\overline{a_1a_2}].$$

If $a_1 - a_2=b\in\mathfrak{B}$ then $a_1^p=a_2^p+b^p+s(a_2, b)$. Since b^p and $s(a_2, b)\in\mathfrak{B}$ we see that $a_1\equiv a_2(\mathfrak{B})$ implies $a_1^p\equiv a_2^p(\mathfrak{B})$. Hence the definition $(\bar{a})^p=\overline{a^p}$ is unambiguous and together with the above operations it defines $\bar{\mathfrak{L}}=\mathfrak{L}/\mathfrak{B}$, the *difference algebra* of $\mathfrak{L}$ relative to $\mathfrak{B}$, as a restricted Lie algebra. The correspondence $a\rightarrow\bar{a}$ is a homomorphism between $\mathfrak{L}$ and $\bar{\mathfrak{L}}$. Conversely we may show in the usual manner that if $\mathfrak{L}$ is homomorphic to the restricted Lie algebra $\bar{\mathfrak{L}}$, $\bar{\mathfrak{L}}=\mathfrak{L}/\mathfrak{B}$ where $\mathfrak{B}$ is the set of elements mapped into 0 by the homomorphism.

If $\mathfrak{B}_1$ and $\mathfrak{B}_2$ are subspaces of $\mathfrak{L}$ we denote their sum as $\mathfrak{B}_1+\mathfrak{B}_2$ and their commutator, i.e., the smallest space containing all $[b_1b_2]$, $b_1\in\mathfrak{B}_1$, $b_2\in\mathfrak{B}_2$ by $[\mathfrak{B}_1\mathfrak{B}_2]$. Conditions (1), (2) and (3) imply

$$(11) \qquad [\mathfrak{B}_1\mathfrak{B}_2] = [\mathfrak{B}_2\mathfrak{B}_1], \qquad [\mathfrak{B}_1[\mathfrak{B}_2\mathfrak{B}_3]] \leqq [\mathfrak{B}_2[\mathfrak{B}_3\mathfrak{B}_1]] + [\mathfrak{B}_3[\mathfrak{B}_1\mathfrak{B}_2]].$$

Set $\mathfrak{L}^{[2]}=[\mathfrak{L}\mathfrak{L}], \cdots, \mathfrak{L}^{[i]}=[\mathfrak{L}^{[i-1]}\mathfrak{L}]$ and define $\mathfrak{L}^{p^k}$ to be the smallest subspace containing all a^{p^k} where $a^{p^k}=(a^{p^{k-1}})^p$. Thus $\mathfrak{L}\geqq\mathfrak{L}^{[2]}\geqq\mathfrak{L}^{[3]}\geqq\cdots$ and $\mathfrak{L}\geqq\mathfrak{L}^p\geqq\mathfrak{L}^{p^2}\geqq\cdots$, $\mathfrak{L}^{p^2}\leqq(\mathfrak{L}^p)^p$, etc. Hence if we define

$$\mathfrak{L}_i = \mathfrak{L}^{[i]} + (\mathfrak{L}^{[i-1]})^p + (\mathfrak{L}^{[i-2]})^{p^2} + \cdots + \mathfrak{L}^{p^{i-1}}$$

we have $\mathfrak{L}=\mathfrak{L}_1\geqq\mathfrak{L}_2\geqq\mathfrak{L}_3\geqq\cdots$. By induction on j one readily establishes

$$[\mathfrak{L}^{[i]}\mathfrak{L}^{[j]}] \leqq \mathfrak{L}^{[i+j]}.$$

Since

$$[b_1^{p^k}, b_2^{p^l}] = [\cdots[b_1^{p^k}\overbrace{b_2]b_2]\cdots b_2]}^{p^l}$$
$$= [[\cdots[\overbrace{b_1[b_1\cdots[b_1b_2]\cdots]}^{p^k}, \overbrace{b_2]b_2]\cdots b_2]}^{p^l-1}$$

we have

$$[\mathfrak{L}^{[i-k]p^k}\mathfrak{L}^{[j-l]p^l}] \leqq \mathfrak{L}^{[(i-k)p^k+(j-l)p^l]} \leqq \mathfrak{L}^{[i+j]}. \tag{12}$$

This leads readily to

$$[\mathfrak{L}_i\mathfrak{L}_j] \leqq \mathfrak{L}_{i+j}, \qquad \mathfrak{L}_i^p \leqq \mathfrak{L}_{i+1}. \tag{13}$$

In particular $\mathfrak{L}_i$ is an ideal in $\mathfrak{L}$ and $\mathfrak{L}_i \geqq [\mathfrak{L}_{i-1}\mathfrak{L}]+\mathfrak{L}_{i-1}^p$. On the other hand from the definition of $\mathfrak{L}_i$ we have $\mathfrak{L}_i \leqq [\mathfrak{L}_{i-1}\mathfrak{L}]+\mathfrak{L}_{i-1}^p$. Hence $\mathfrak{L}_i = [\mathfrak{L}_{i-1}\mathfrak{L}]+\mathfrak{L}_{i-1}^p$. It follows that if $\mathfrak{L}_{i-1}=\mathfrak{L}_i$, $\mathfrak{L}_{i-1}=\mathfrak{L}_i=\mathfrak{L}_{i+1}= \cdots$. If $\mathfrak{L}_N=0$ for N sufficiently large, $\mathfrak{L}$ is *nilpotent*. The smallest N for which this holds is called the *index* of nilpotency. If $\mathfrak{L}_N=0$, $\mathfrak{L}^{p^{N-1}}=0$ and $\mathfrak{L}^{[N]}=0$. Conversely if $\mathfrak{L}^{[r]}=0$ and $\mathfrak{L}^{p^s}=0$ it is readily seen that $\mathfrak{L}_t=0$ for $t=r+s-1$.

4. **Restricted derivations.** The most natural instances of restricted Lie algebras are the derivation algebras(3). We recall that if $\mathfrak{A}$ is an arbitrary algebra (not necessarily associative) then a derivation D is defined to be a transformation $a\rightarrow aD$ in $\mathfrak{A}$ such that

$$(a+b)D = aD + bD, \quad (a\alpha)D = (aD)\alpha, \quad (ab)D = (aD)b + a(bD). \tag{14}$$

If $\mathfrak{A}$ has characteristic p the set $\mathfrak{D}$ of these transformations is closed under addition, scalar multiplication, commutation and pth powers. Thus $\mathfrak{D}$ is a restricted Lie algebra. If $\mathfrak{A}$ is associative

$$a^pD = (aD)a^{p-1} + a(aD)a^{p-2} + \cdots + a^{p-1}(aD) = [\cdots[aD, \overbrace{a]a]\cdots a]}^{p-1}(4).$$

It is therefore natural to confine our attention in the case that $\mathfrak{A}=\mathfrak{L}$ is a restricted Lie algebra to the derivations called *restricted* such that

$$a^pD = [\cdots[aD\overbrace{a]a]\cdots a]}^{p-1}. \tag{15}$$

Suppose D is a linear transformation in $\mathfrak{L}$ such that $[x_ix_j]D=[x_iD, x_j]+[x_i, x_jD]$, $x_1, x_2, \cdots$ a basis for $\mathfrak{L}$. Then D is a derivation. If $x_1^{\kappa_1}\cdots x_n^{\kappa_n}$, $\kappa_i=1, 2, \cdots$, is a basis for the Birkhoff-Witt algebra $\mathfrak{A}$ we define the linear transformation D in $\mathfrak{A}$ by setting

(3) Cf. Jacobson [3].

(4) In general

$$ba^{p-1}+aba^{p-2}+\cdots+a^{p-1}b = [\cdots[b\overbrace{a]a]\cdots a]}^{p-1}.$$

See [3, p. 209].

$$(16)\qquad \begin{aligned}(x_1^{\kappa_1}\cdots x_n^{\kappa_n})D = (x_1D)x_1^{\kappa_1-1}\cdots x_n^{\kappa_n} + \cdots + x_1^{\kappa_1-1}(x_1D)\cdots x_n^{\kappa_n}\\ + \cdots + x_1^{\kappa}\cdots x_n^{\kappa_n-1}(x_nD).\end{aligned}$$

By an induction similar to that of §2 we can show that

$$(17)\qquad (x_{i_1}\cdots x_{i_m})D = (x_{i_1}D)x_{i_2}\cdots x_{i_m} + \cdots + x_{i_1}\cdots (x_{i_m}D),$$

holds. Hence D is a derivation.

Now suppose

$$x_i^{[p]}D = [\cdots [x_iD, \overbrace{x_i]\cdots x_i}^{p-1}].$$

Then $(x_i^{[p]}-x_i^p)D=0$ and D maps the ideal $\mathfrak{B}$ whose basis is $x_i^{[p]}-x_i^p$ into itself. It follows that D induces a derivation in $\mathfrak{U}=\mathfrak{A}/\mathfrak{B}$ and hence is a restricted derivation in $\mathfrak{L}$. We have shown also that any restricted derivation is determined by a derivation of the u-algebra. The converse of this is clear. Hence we have proved

THEOREM 4. *A linear transformation D in $\mathfrak{L}$ is a restricted derivation if and only if $[x_ix_j]D=[x_iD, x_j]+[x_i, x_jD]$ and $x_i^pD=[\cdots[x_iD, x_i]\cdots x_i]$ for any basis $x_1, x_2, \cdots$. Every restricted derivation is induced by a derivation of the associative u-algebra $\mathfrak{U}$ of $\mathfrak{L}$. The set of restricted derivations forms a restricted Lie algebra.*

The last statement follows immediately from the second. The set of restricted derivations will be denoted by $\mathfrak{D}_0$. A consequence of the first part of Theorem 4 is that the restricted derivation algebra of $\mathfrak{L}_P$ is $\mathfrak{D}_{0P}$.

For any three elements a, b, l in $\mathfrak{L}$ we have

$$[a+b, l] = [al]+[bl],\ [a\alpha, l] = [al]\alpha,\ [[ab]l] = [[al]b]+[a[bl]],$$

$$[a^pl] = [\cdots [al]\overbrace{a]a]\cdots a}^{p-1}].$$

Thus the transformations $L\colon a\to[al]$ are restricted derivations which we call *inner*. The other parts of (1) to (6) show that the derivations corresponding to l_1+l_2, $l\alpha$, $[l_1l_2]$, l^p are respectively L_1+L_2, $L\alpha$, $[L_1L_2]$, L^p. Hence the inner derivations form a subalgebra $\mathfrak{J}$ of $\mathfrak{D}_0$ and $\mathfrak{L}$ is homomorphic to $\mathfrak{J}$ under the correspondence $l\to L$. The elements c mapped into 0 are those which satisfy $[ac]=0$ for all a and form the *center* $\mathfrak{C}$ of $\mathfrak{L}$. Hence $\mathfrak{J}\cong\mathfrak{L}/\mathfrak{C}$. Since

$$[al]D - [aD, l] = [a, lD],$$

$[LD]\in\mathfrak{J}$ for every L in $\mathfrak{J}$ and D in $\mathfrak{D}_0$, i.e., $\mathfrak{J}$ is an ideal.

Let $\mathfrak{H}_0$ be the vector space which is a direct sum of $\mathfrak{L}$ and $\mathfrak{D}_0$. The elements U of $\mathfrak{H}_0$ are uniquely representable in the form $a+D$, a in $\mathfrak{L}$, D in $\mathfrak{D}_0$. Hence if $x_1, x_2, \cdots$ is a basis for $\mathfrak{L}$ and $D_1, D_2, \cdots$ one for $\mathfrak{D}_0$, $x_1, x_2, \cdots; D_1, D_2, \cdots$ is a basis for $\mathfrak{H}_0$.

We define commutation in $\mathfrak{H}_0$ by

$$[a + D, b + E] = [ab] + aE - bD + [DE]. \tag{18}$$

It is readily seen that this satisfies conditions (1), (2), (3)([5]). We also have

$$[\cdots[\overbrace{ax_i]\cdots x_i}^{p}] = [ax_i^p], \qquad [\cdots[\overbrace{Dx_i]\cdots x_i}^{p}] = [Dx_i^p],$$

$$[\cdots[aD_j]\cdots D_j] = [aD_j^p], \qquad [\cdots[DD_j]\cdots D_j] = [DD_j^p],$$

or

$$[\cdots[Ux_i]\cdots x_i] = [Ux_i^p], \qquad [\cdots[UD_j]\cdots D_j] = [UD_j^p],$$

for all U in $\mathfrak{H}_0$. Hence, by §2, the definition

$$\left(\sum x_i\alpha_i + \sum D_j\beta_j\right)^p = \sum x_i^p\alpha_i^p + \sum D_j^p\beta_j^p + s(x, D) \tag{19}$$

turns $\mathfrak{H}_0$ into a restricted Lie algebra called the *restricted holomorph* of $\mathfrak{L}$. Thus $(a+D)^p = a^p + D^p + s(a, D)$ in $\mathfrak{H}_0$.

5. **Relations to ordinary Lie algebras.** Suppose $\mathfrak{L}_1$ and $\mathfrak{L}_2$ are restricted Lie algebras and $a \rightarrow a^S$ is a mapping of $\mathfrak{L}_1$ into $\mathfrak{L}_2$ such that

$$(a + b)^S = a^S + b^S, \qquad (a\alpha)^S = a^S\alpha, \qquad [ab]^S = [a^Sb^S].$$

Then

$$[\cdots[xa]\cdots a]^S = [\cdots[x^Sa^S]\cdots a^S] = [x^S(a^S)^p],$$
$$[x, a^p]^S = [x^S(a^p)^S].$$

Hence $(a^p)^S - (a^S)^p \in \mathfrak{C}_2$ the center of $\mathfrak{L}_2$. If $\mathfrak{C}_2 = 0$, S is a homomorphism. Next we suppose D is a derivation in $\mathfrak{L} = \mathfrak{L}_1$. This implies that

$$\begin{aligned}[\cdots[xa]\cdots a]D &= [\cdots[xDa]\cdots a] + [\cdots[[x, aD]a]\cdots a] \\ &\quad + \cdots + [\cdots[[xa]a]\cdots aD] \\ &= [xD, a^p] + [x, [\cdots[aD, a]\cdots a]],\end{aligned}$$

since if A is the transformation $x \rightarrow [xa]$ and B is the transformation $x \rightarrow [x, aD]$,

$$BA^{p-1} + ABA^{p-2} + \cdots + A^{p-1}B = [\cdots[[BA]A]\cdots A]\text{([6])}.$$

On the other hand $[xa^p]D = [xD, a^p] + [x, a^pD]$. Hence $a^pD - [\cdots[aD, a]\cdots a]$ is in the center $\mathfrak{C}$ of $\mathfrak{L}$. If $\mathfrak{C} = 0$ every derivation is restricted.

If $\mathfrak{B}$ is a subset of $\mathfrak{L}$ closed with respect to addition, scalar multiplication and commutation, then $\mathfrak{B}^* = \mathfrak{B} + \mathfrak{B}^p + \mathfrak{B}^{p^2} + \cdots$ is the smallest subalgebra of $\mathfrak{L}$ containing $\mathfrak{B}$. If $[\mathfrak{B}\mathfrak{L}] \leqq \mathfrak{B}$, $\mathfrak{B}^*$ is an ideal.

([5]) Cf. Zassenhaus [6, p. 57].

([6]) See Footnote 4.

An ordinary Lie algebra $\mathfrak{A}$ whose center is 0 may always be imbedded in a restricted Lie algebra. For let $\mathfrak{D}$ be the derivation algebra of $\mathfrak{A}$. Since the center of $\mathfrak{A}$ is 0 the set $\mathfrak{F}$ of inner derivations forms an ideal of $\mathfrak{D}$ (regarded as an ordinary Lie algebra) isomorphic to $\mathfrak{A}$. If $\mathfrak{F}^*=\mathfrak{F}+\mathfrak{F}^p+\cdots$, $\mathfrak{F}^*$ is a restricted Lie algebra containing $\mathfrak{F}$. Since $[u^{p^k}v^{p^l}]=[\cdots[[u[\cdots[uv]\cdots],v]\cdots v]\in\mathfrak{F}$ for any u, v in $\mathfrak{F}$ the ordinary Lie algebra $\mathfrak{F}^*/\mathfrak{F}$ is commutative.

Suppose $\mathfrak{L}$ is a restricted Lie algebra and $a\rightarrow A$ an absolutely irreducible representation of the ordinary Lie algebra determined by $\mathfrak{L}$, i.e., $a\alpha\rightarrow A\alpha$, $a+b\rightarrow A+B$, $[ab]\rightarrow[AB]$. We assume also that the representing matrices all have trace 0 and $p\nmid m$ where $m\times m$ are the dimensions of the matrices. We assert that our representation is one of the restricted Lie algebra. For if $a^p\rightarrow B$ we have $[XB]=[\cdots[XA]\cdots A]=[XA^p]$. Hence $A^p-B=1\rho$ and since tr $A^p=$ tr $B=0$, $A^p=B$.

6. **Algebras with a finite basis.** In this section we suppose $\mathfrak{L}$ has a finite basis. For any element a there is a least integer m such that $a, a^p,\cdots,a^{p^{m-1}}$ are linearly independent but a^{p^m} depends on $a,\cdots,a^{p^{m-1}}$. Then $a^{p^m}+a^{p^{m-1}}\alpha_1+\cdots+a\alpha_m=0$ or $f(a)=0$ where $f(\lambda)=\lambda^{p^m}+\lambda^{p^{m-1}}\alpha_1+\cdots+\lambda\alpha_m$. It follows that $a^{p^{m+1}}=(a^{p^m})^p$, $a^{p^{m+1}},\cdots$ are linear combinations of $a,\cdots,a^{p^{m-1}}$ and hence these elements form a basis for the subalgebra generated by a.

A polynomial having the form of $f(\lambda)$ has been called a p-polynomial by Ore. The following facts were established by Ore: (1) A necessary and sufficient condition that $f(\lambda)$ be a p-polynomial is that its roots form a modulus (group under addition) with each root having multiplicity p^k, k fixed. (2) Any polynomial $\phi(\lambda)$ is a factor of a p-polynomial $f(\lambda)$. The $f(\lambda)$ of least degree with leading coefficient 1 is unique and is a divisor of any other p polynomial divisible by $\phi(\lambda)$(7). Thus suppose $a\rightarrow A$ is a (1-1) representation of $\mathfrak{L}$ and $\phi(\lambda)$ is the minimum polynomial of the linear transformation (or matrix) A. Then the p-polynomial $f(\lambda)$ associated with a is the one of least degree divisible by $\phi(\lambda)$.

An element a is *nilpotent* if $a^{p^m}=0$ for some p^m. The least integer p^m for which this holds is the *index* of a.

THEOREM 5. *If $\mathfrak{L}$ is a Lie algebra with a finite basis and contains only nilpotent elements, then $\mathfrak{L}$ is nilpotent.*

Since $\mathfrak{L}$ has a finite basis the index of any a is $\leqq p^n$ where n is the dimensionality of $\mathfrak{L}$. Hence $a^{p^n}=0$ and if A is the linear transformation $x\rightarrow[xa]$, $A^{p^n}=0$. Thus $\mathfrak{L}^{p^n}=0$ and as has been shown by Zorn [8], $\mathfrak{L}$ is nilpotent when regarded as an ordinary Lie algebra, i.e., $\mathfrak{L}^{[m]}=0$. It follows as in §4 that $\mathfrak{L}$ is nilpotent.

The algebra $\mathfrak{L}>\mathfrak{L}_2=\mathfrak{L}^{[2]}+\mathfrak{L}^p$. If $\mathfrak{M}$ is a subspace such that $\mathfrak{L}\geqq\mathfrak{M}\geqq\mathfrak{L}_2$, $\mathfrak{M}$ is a nilpotent ideal and $\mathfrak{L}/\mathfrak{M}$ is commutative and has all of its elements $\neq 0$ nil-

(7) Ore [4, p. 581].

potent of index p. We choose $\mathfrak{M}$ so that dim $\mathfrak{M}=n-1$ and let $x_2, x_3, \cdots, x_n$ be a basis for $\mathfrak{M}$ with $d, x_2, \cdots, x_n$ a basis for $\mathfrak{L}$.

THEOREM 6. *The u-algebra of a nilpotent Lie algebra with a finite basis is a nilpotent associative algebra.*

The theorem is trivial if $\mathfrak{L}$ has 1 dimension. Suppose it true for algebras of order $n-1$. Choose $\mathfrak{M}$ and $d, x_2, \cdots, x_n$ as indicated. Then the u-algebra $\mathfrak{U}$ is generated by $d, x_2, \cdots, x_n$ and the u-algebra $\mathfrak{V}$ of $\mathfrak{M}$ is generated by $x_2, \cdots, x_n$. $\mathfrak{V}$ is nilpotent. The elements of $\mathfrak{U}$ have the form

$$u = v_0 + dv_1 + \cdots + d^{p-1}v_{p-1} + d\beta_1 + d^2\beta_2 + \cdots + d^{p-1}\beta_{p-1}$$

where $v_i \in \mathfrak{V}$ and $\beta_i \in \Phi$. The *weight* of $d^i v_1^{(\kappa_1)} v_2^{(\kappa_2)} \cdots v_s^{(\kappa_s)}$ where

$$v^{(\kappa)} = [\cdots \overbrace{[vd]d \cdots d]}^{\kappa} \in \mathfrak{V}$$

is defined to be $\geqq i+s+\kappa_1+\cdots+\kappa_s$. Hence the weight of each term of u is $\geqq 1$. Since

$$\begin{aligned} v_1^{(\kappa_1)} v_2^{(\kappa_2)} \cdots v_s^{(\kappa_s)} d = {} & dv_1^{(\kappa_1)} v_2^{(\kappa_2)} \cdots v_s^{(\kappa_s)} + v_1^{(\kappa_1+1)} v_2^{(\kappa_2)} \cdots v_s^{(\kappa_s)} \\ & + \cdots + v_1^{(\kappa_1)} v_2^{(\kappa_2)} \cdots v_s^{(\kappa_s+1)} \end{aligned}$$

the weight of a product $u_1u_2 \cdots u_k$ is $\geqq k$. If the index of nilpotency of $\mathfrak{V}$ is m and $d^{p^t}=0$, then every term of weight $\geqq mp^t$ is 0. Thus $\mathfrak{U}$ is nilpotent of index $\leqq mp^t$.

A consequence of this theorem is that the irreducible representations of a nilpotent restricted Lie algebra are all 0. Hence any representation has matrices in triangular form with diagonal elements 0 if the basis is properly chosen.

BIBLIOGRAPHY

1. I. Ado, Bulletin de la Société Physico-mathématique de Kazan, vol. 6 (1935).

2. G. Birkhoff, *Representability of Lie algebras* $\cdots$, Annals of Mathematics, (2), vol. 38 (1937), pp. 526–532.

3. N. Jacobson, *Abstract derivation and Lie algebras*, these Transactions, vol. 42 (1937), pp. 206–224.

4. O. Ore, *On a special class of polynomials*, these Transactions, vol. 35 (1933), pp. 559–584.

5. E. Witt, *Treue Darstellung Liescher Ringe*, Journal für die reine und angewandte Mathematik, vol. 177 (1937), pp. 152–160.

6. H. Zassenhaus, *Über Liesche Ringe mit Primzahlcharakteristik*, Abhandlungen aus dem mathematischen Seminar der Hansischen Universität, 1939, pp. 1–100.

7. ———, *Endliche p-Gruppe und Lie-Ring mit der Charakteristic p*, ibid., pp. 200–207.

8. M. Zorn, *On a theorem of Lie*, Bulletin of the American Mathematical Society, vol. 42 (1936), p. 485.

UNIVERSITY OF NORTH CAROLINA,
CHAPEL HILL, N. C.