THE REPRESENTATIONS OF LIE ALGEBRAS OF PRIME CHARACTERISTIC

by HANS ZASSENHAUS

(Received 22nd January, 1953)

There are some simple facts which distinguish Lie-algebras over fields of prime characteristic from Lie-algebras over fields of characteristic zero. These are

(1) The degrees of the absolutely irreducible representations of a Lie-algebra of prime characteristic are bounded whereas, according to a theorem of H. Weyl, the degrees of the absolutely irreducible representations of a semi-simple Lie-algebra over a field of characteristic zero can be arbitrarily high.*

(2) For each Lie-algebra of prime characteristic there are indecomposable representations which are not irreducible, whereas every indecomposable representation of a semi-simple Lie-algebra over a field of characteristic zero is irreducible (*cf.* [4]).

(3) The quotient ring of the embedding algebra of a Lie-algebra over a field of prime characteristic is a division algebra of finite dimension over its center, whereas this is not the case for characteristic zero. (*cf.* [4]).

(4) There are faithful fully reducible representations of every Lie-algebra of prime characteristic, whereas for characteristic zero only ring sums of semi-simple Lie-algebras and abelian Lie-algebras admit faithful fully reducible representations (*cf.* [6], [2], [4]).

These facts have been established for special cases for many years, and some of them have been considered in the general case by N. Jacobson recently in [4]. They are at the basis of every investigation aiming at a theory of Lie-algebras of prime characteristic embedded into their enveloping algebras.

In this paper I attempt to work out such a theory up to the point where (1)–(4) and a number of deeper-lying properties of Lie-algebras of prime characteristic become connected with the central fact that if one wants to study the representations of a Lie-algebra of prime characteristic, one is concerned with specializations of an algebraic variety. This is an illustration of the significance of a remark of A. Weil that the tools and results of algebraic geometry are capable of being applied with great advantage in the study of Lie-algebras. Furthermore the method of elementary ideals introduced by E. Steinitz proves its value once again.

The following is a summary of the present paper.

It is proved that the enveloping algebra $A(L)$ of a Lie-algebra L of dimension n over a field F of characteristic $p>0$ is a maximal order of a division algebra of dimension p^{2m} over the quotient field of the center $\mathfrak{Z}$ of $A(L)$ and that $\mathfrak{Z}$ is a normal algebraic variety of dimension n over F.

* This property of Lie-algebras of prime characteristic is implicitly contained in [3], [7] and [4] and explicitly, for special cases, in [6], [8] and [2]. The following is a brief account of a proof, given by N. Jacobson in a letter to I. Kaplansky, communicated to the author on 12th November, 1952.

Let L be a finite-dimensional Lie-algebra over an algebraically closed field F of characteristic $p>0$, and let A be its Birkhoff-Witt algebra. For any linear element x of A there exists by Jacobson a polynomial f such that $f(x)$ is in the center $\mathfrak{Z}$ of A. Let there be given an irreducible representation of L on a finite-dimensional vector space over F. Then in the induced representation of A, $f(x)$ must go into a scalar c. Let $x_1, x_2, \ldots, x_n$ be a basis of L with corresponding f_i and c_i. Let f_i have degree r_i. Let I be the ideal in A generated by all $f(x_i)-c_i$. Then the representation is really one of A/I. But A/I is really finite-dimensional with dimension at most $r_1 r_2 \ldots r_n$. Hence this is a bound for the degrees of the irreducible representations.

Every specialization θ of $\mathfrak{Z}$ onto an algebra† Φ over F determines a specialization of $A(L)$ onto a finitely-generated Φ-ring Ψ, which is uniquely determined up to isomorphisms over Φ. The indecomposable representations of L are in (1–1)-correspondence with the faithful indecomposable representations of all algebras Ψ for which Φ is a primary ring over F. In other words, for characteristic $p>0$, the theory of the representations of Lie-algebras allows a structural reduction to the theory of representations of associative algebras.

To every absolutely irreducible representation of L there corresponds a specialization of the algebraic variety $\mathfrak{Z}$ onto F. Only a finite number of classes of equivalent absolutely irreducible representations lead to the same specialization of $\mathfrak{Z}$. The degree of these representations is less than or equal to p^m. Except for a subvariety characterized by the vanishing of the specialized discriminant ideal of $A(L)$ over $\mathfrak{Z}$, the correspondence between the classes of equivalent absolutely irreducible representations and the specializations of $\mathfrak{Z}$ onto F is 1–1 and the degree is equal to p^m.

The irreducible constituents of an indecomposable representation lead to equivalent specializations of $\mathfrak{Z}$. Conversely, for every specialization of $\mathfrak{Z}$ onto a finite extension of F over F there are indecomposable representations of arbitrarily high degree, in the sense indicated above.

The F-module

$$L^* = L + FL^p + FL^{p^2} + \dots$$

generated by the set of all the elements a^{p^j}, with $a \in L$ and j ranging from zero to infinity, turns out to be an F-Lie-ring containing L as an ideal with abelian difference ring.

The ring $\mathfrak{Z}$ is finitely-generated over the subring $\mathfrak{o}$ which is generated by the unit element 1 and the intersection $\mathfrak{Z} \cap L^*$ of $\mathfrak{Z}$ and L^*. Two representations are called members of the same family if they induce equivalent specializations of $\mathfrak{o}$ over F.

The representations of L over F are distributed into families, each consisting of a certain number of classes with at most a finite number of irreducible ones among them. Any two families are coprime.

The Lie-Kronecker product induces an addition of the families corresponding to the specializations of $\mathfrak{o}$ over F onto F ; so these specializations form a module of characteristic p.

I take this opportunity of expressing my appreciation of the generous support which I have received from the Canadian National Research Council, under whose auspices the investigations presented in this paper were begun in the summer of 1950 and concluded in the summer of 1952 at the Summer Research Institute at Kingston, Ont.

§ 1. Let L be a Lie-algebra with basis $a_1, a_2, \dots, a_n$ over the field F. Let $A(L)$ be the enveloping algebra of L over F, *i.e.*, the associative F-ring with the basis elements

$$a_1^{\mu_1} a_2^{\mu_2} \dots a_n^{\mu_n} \quad (\mu_i \geqslant 0)$$

over F and multiplication defined by juxtaposition and application of the straightening procedure of G. Birkhoff which is derived from the commutation rule

$$a_i a_k = a_k a_i + \sum_{l=1}^{n} \gamma_{ik}^l a_l,$$

† The word " algebra ", without any qualifying adjective, will be used to mean associative algebra of finite dimension.

which itself is obtained from the multiplication rule

$$a_i \circ a_k = \sum_{l=1}^{n} \gamma_{ik}^{l} a_l \quad (i, k = 1, 2, \dots, n;\ \gamma_{ik}^{l} \in F)$$

for the Lie-multiplication of the basis elements of L (*cf.* [1]).

LEMMA 1. *$A(L)$ has no divisors of zero.*

Proof: Define the degree of the monomial expression

$$a_1^{\mu_1} a_2^{\mu_2} \dots a_n^{\mu_n}$$

to be the sum of the exponents, according to the formula

$$d(a_1^{\mu_1} a_2^{\mu_2} \dots a_n^{\mu_n}) = \mu_1 + \mu_2 + \dots + \mu_n,$$

and the degree $d(X)$ of a linear combination X of the basis elements to be the maximum of the degrees of all the basis elements of $A(L)$ having non-vanishing coefficients in X. The zero element 0 is not given a degree. The sum $s(X)$ of all contributions to X from the basis elements of degree $d(X)$, which we may call the highest terms, is called the *leading member* of X; *e.g.*,

$$s(a_1 a_2^2 + a_1^2 a_2 + a_1 a_2 + a_1) = a_1 a_2^2 + a_1^2 a_2.$$

Since the application of the straightening procedure of Birkhoff to XY, where X and Y are linear combinations of the basis elements of $A(L)$, only permutes factors and creates new products of less than $d(X) + d(Y)$ basis elements of L, it follows that if

$$s(X) = \sum_{\lambda_1 + \lambda_2 + \dots + \lambda_n = d(X)} \alpha_{\lambda_1 \lambda_2 \dots \lambda_n} a_1^{\lambda_1} a_2^{\lambda_2} \dots a_n^{\lambda_n}$$

and

$$s(Y) = \sum_{\mu_1 + \mu_2 + \dots + \mu_n = d(Y)} \beta_{\mu_1 \mu_2 \dots \mu_n} a_1^{\mu_1} a_2^{\mu_2} \dots a_n^{\mu_n},$$

then

$$XY = \sum \alpha_{\lambda_1 \lambda_2 \dots \lambda_n} \beta_{\mu_1 \mu_2 \dots \mu_n} a_1^{\nu_1} a_2^{\nu_2} \dots a_n^{\nu_n} + \text{terms of lower degree},$$

where summation is over all sets of non-negative integral values of $\lambda_1, \lambda_2, \dots, \lambda_n$ such that $\lambda_1 + \lambda_2 + \dots + \lambda_n = d(X)$ and all sets of non-negative integral values of $\mu_1, \mu_2, \dots, \mu_n$ such that $\mu_1 + \mu_2 + \dots + \mu_n = d(Y)$, and $\nu_j = \lambda_j + \mu_j$ $(j = 1, 2, \dots, n)$. In other words, there is an operator isomorphism ϕ between $A(L)$ and the polynomial ring $F[x_1, x_2, \dots, x_n]$ in n polynomial variables $x_1, x_2, \dots, x_n$, both $A(L)$ and $F[x_1, x_2, \dots, x_n]$ being considered as F-modules only, such that

$$\phi\left(\sum \xi_{\rho_1 \rho_2 \dots \rho_n} a_1^{\rho_1} a_2^{\rho_2} \dots a_n^{\rho_n}\right) = \sum \xi_{\rho_1 \rho_2 \dots \rho_n} x_1^{\rho_1} x_2^{\rho_2} \dots x_n^{\rho_n},$$

and under this operator isomorphism the leading member of X corresponds to the leading member of $\phi(X)$ and the leading member of XY corresponds to the leading member of $\phi(X)\phi(Y)$. Consequently

$$d(XY) = d(X) + d(Y),$$
$$s(XY) = s(s(X)s(Y)),$$
$$\phi(s(XY)) = \phi(s(X))\phi(s(Y)).$$

Thus if $X \neq 0$ and $Y \neq 0$, $XY \neq 0$; q.e.d.

From now on we assume that F is a field of characteristic $p > 0$, where p is a prime number.

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

LEMMA 2. *The elements*

$$a_i^{p^j} (i = 1, 2, \dots, n\,;\ j = 0, 1, 2, \dots)$$

are the basis elements of an F-Lie ring L^* contained in the universal embedding ring $A(L)$ of L over F such that the Lie-algebra L is an ideal of L^* with Abelian difference ring.

Proof: The linear independence of the elements $a_i^{p^j}$ over F follows from the construction of $A(L)$. The rest of lemma 2 follows from repeated application of the formula

$$\begin{aligned} (1) \qquad x^p \circ y &= -y \circ x^p = x^p y - y x^p \\ &= x \circ (x \circ \dots (x \circ y) \dots), \text{ where } x \text{ occurs } p \text{ times to the left of } y, \\ &= -(\dots (y \circ x) \dots \circ x) \circ x, \text{ where } x \text{ occurs } p \text{ times to the right of } y, \end{aligned}$$

in rings of characteristic p (*cf.* [3]).

LEMMA 3. *L^* is independent of the choice of the basis of L over F, since*

$$L^* = L + FL^p + FL^{p^2} + \dots \ ,$$

where L^{p^j} denotes the module generated by all the elements a^{p^j} with a contained in L.

Furthermore, the elements $a_1^{p^i}, a_2^{p^i}, \dots, a_n^{p^i}$ form a basis of the F-module $L + FL^p + \dots + FL^{p^i}$ modulo the F-module $L + FL^p + \dots + FL^{p^{i-1}}$ over F.

The proof follows from repeated application of the formula

$$(2) \qquad (x+y)^p = x^p + \sum_{i=1}^{p-1} \Lambda_i(x, y) + y^p,$$

in rings of characteristic p, where $\Lambda_i(x, y)$ denotes a certain sum of Lie-products with i factors x and $p-i$ factors y (*cf.* [4]).

LEMMA 4. *Let M be an F-Lie-ring contained in L^* and satisfying the condition*

$$M^p \subseteq M \neq (0).$$

Let

$$\begin{aligned} M_k &= M \cap (L + FL^p + \dots + FL^{p^k}), \quad (k = 0, 1, 2, \dots) \\ M'_k &= M_{k-1} + FM_{k-1}^p, \quad (k = 1, 2, \dots), \\ M'_0 &= (0). \end{aligned}$$

Then it follows that

(*a*) $$0 < \mu = \sum_{k=0}^{\infty} \dim_F (M_k - M'_k) \leqq n.$$

(*b*) *There are μ elements $u_1, u_2, \dots, u_\mu$ in M such that the elements*

$$u_i^{p^j} \quad (1 \leqq i \leqq \mu\,;\ j = 0, 1, 2, \dots)$$

form a basis of M over F.

(*c*) *The elements*

$$u_1^{\alpha_1} u_2^{\alpha_2} \dots u_n^{\alpha_n} \quad (0 \leqq \alpha_i)$$

form an F-basis of the F-ring $\langle M \rangle$ generated by M and the unit element.

(*d*) $$\langle M \rangle \cap L^* = M.$$

(*e*) *The F-module $L^* - M$ is of finite dimension over F if and only if $\mu = n$. In this case*

$$\dim_F (L^* - M) = \sum_{k=0}^{\infty} k \dim_F (M_k - M'_k).$$

(*f*) *Considering $A(L)$ as an $\langle M \rangle$-ring, there is a basis of $A(L)$ over $\langle M \rangle$, provided that F is a perfect field. In this case, if $\mu = n$, there is a basis consisting of p^l elements, where $l = \dim_F (L^* - M)$.*

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

For the proof, let us assume first that F is a perfect field of characteristic $p>0$, *i.e.*, that every equation $\xi^p=\alpha$ with α in F has a solution ξ in F. This solution is uniquely determined by α and may be denoted by $\alpha^{p^{-1}}$. We define recursively

$$\alpha^{p^{-i}}=(\alpha^{p^{-(i-1)}})^{p^{-1}} \quad (i=2, 3, \ldots).$$

Then it follows by repeated application of the formulas (1), (2) and

$$(\lambda x)^p=\lambda^p x^p \quad (\lambda \epsilon F) \tag{3}$$

that

$$\lambda_1 x_1^{p^i}+\lambda_2 x_2^{p^i}+\ldots+\lambda_r x_r^{p^i}\equiv(\lambda_1^{p^{-i}}x_1+\lambda_2^{p^{-i}}x_2+\ldots+\lambda_r^{p^{-i}}x_r)^{p^i} \tag{4}$$

modulo $L+L^p+\ldots+L^{p^{i-1}}$, for $i=1, 2, \ldots$; $x_1, x_2, \ldots, x_r \epsilon L$.

We adapt the choice of the basis $a_1, a_2, \ldots, a_n$ of L over F to the situation of M and L^* relative to each other. Let $a_1, a_2, \ldots a_{\mu_0}$ be a basis of M_0 over F, where, of course, $\mu_0=0$ if $M_0=(0)$.

By lemma 3 the elements $a_1^p, a_2^p, \ldots, a_{\mu_0}^p$ are linearly independent modulo L over F. Since $M_0^p \subseteq M_0+\sum_{i=1}^{\mu_0} Fa_i^p$, it follows that $M_1'=M_0\dot{+}\sum_{i=1}^{\mu_0} Fa_i^p$, where $\dot{+}$ and $\dot{\sum}$ denote direct summation. There is a basis $a_{\mu_0+1}^{(1)}, \ldots, a_{\mu_0+\mu_1}^{(1)}$ of M_1 modulo M_1' over F. According to (4), we find that

$$a_{\mu_0+j}^{(1)}\equiv a_{\mu_0+j}^p \pmod{L},$$

with $a_{\mu_0+j}\epsilon L$; $j=1, 2, \ldots, \mu_1$.

The elements $a_1, a_2, \ldots, a_{\mu_0+\mu_1}$ of L are linearly independent over F, since a linear relation

$$\sum_{i=1}^{\mu_0+\mu_1}\lambda_i a_i=0$$

would imply in succession

$$\sum_{i=1}^{\mu_0+\mu_1}\lambda_i^p a_i^p\equiv 0 \pmod{L},$$

$$\sum_{i=\mu_0+1}^{\mu_0+\mu_1}\lambda_i^p a_i^{(1)}\equiv 0 \pmod{M_1'},$$

$$\lambda_{\mu_0+1}^p=\ldots=\lambda_{\mu_0+\mu_1}^p=0,$$

$$\lambda_{\mu_0+1}=\ldots=\lambda_{\mu_0+\mu_1}=0,$$

$$\sum_{i=1}^{\mu_0}\lambda_i a_i=0,$$

$$\lambda_1=\lambda_2=\ldots=\lambda_{\mu_0}=0.$$

Note that

$$\mu_0=\dim_F(M_0-M_0'),$$

$$\mu_1=\dim_F(M_1-M_1').$$

Set

$$\mu_i=\dim_F(M_i-M_i').$$

Continuing the above process, we find $\mu_0+\mu_1+\ldots+\mu_\rho$ elements $a_1, a_2, \ldots, a_{\mu_0+\mu_1+\ldots+\mu_\rho}$ of L, linearly independent over F, and $\mu_0+\mu_1+\ldots+\mu_\rho$ elements

$$a_1, a_2, \ldots, a_{\mu_0}\,;\ a_{\mu_0+1}^{(1)}, \ldots, a_{\mu_0+\mu_1}^{(1)}\,;\ \ldots\ ;\ a_{\mu_0+\mu_1+\ldots\mu_{\rho_0-1}+1}^{(\rho)}, \ldots, a_{\mu_0+\mu_1+\ldots+\mu_\rho}^{(\rho)}$$

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

of M such that

$$M_\rho = M'_\rho \dot{+} \sum_{j=1}^{\mu_\rho} F a^{(\rho)}_{\mu_0+\mu_1+\ldots+\mu_{\rho-1}+j}$$

and furthermore

$$a^{(\rho)}_{\mu_0+\mu_1+\ldots+\mu_{\rho-1}+j} \equiv a^{p^\rho}_{\mu_0+\mu_1+\ldots+\mu_{\rho-1}+j} \pmod{L+L^p+\ldots+L^{p^{\rho-1}}}, \qquad (j=1, 2, \ldots, \mu).$$

Since certainly

$$\mu_0+\mu_1+\ldots+\mu_\rho \leqq \dim_F L = n,$$

the construction will terminate after a finite number of steps ; say

$$\mu_\sigma > 0, \ \mu_{\sigma+1} = \mu_{\sigma+2} = \ldots = 0.$$

Let

$$\mu = \mu_0+\mu_1+\ldots+\mu_\sigma = \sum_{i=0}^{\infty} \mu_i.$$

Extend the set of linearly independent elements $a_1, a_2, \ldots, a_\mu$ to form a basis $a_1, a_2, \ldots, a_n$ of L over F. If $\mu_i > 0$, define

$$(\mu_0+\mu_1+\ldots+\mu_{i-1}+j)' = i \quad (j=1, 2, \ldots, \mu_i).$$

From the construction it follows that

$$a^{(h')}_h = a^{p^{h'}}_h + \sum_{k=1}^{n} \sum_{l=0}^{h'-1} \lambda_{hkl} a^{p^l}_k \quad (\lambda_{hkl} \in F). \tag{5}$$

The elements

$$v_i = a^{(i')}_i \quad (i=1, 2, \ldots, \mu),$$

with $a^{(0)}_i = a_i$ for $i=1, 2, \ldots, \mu_0$, are elements of M with the property that the elements

$$v^{p^j-h'}_h \quad (h' \leqq j)$$

form a basis of M_j modulo M_{j-1} over F ($j=0, 1, 2, \ldots, M_{-1}=(0)$) and that

$$0 \leqq 1' \leqq 2' \leqq \ldots \leqq \mu' = \sigma.$$

If there were a linear relation

$$\sum_{i=1}^{\mu} \sum_{k=0}^{\nu} \lambda_{ik} v^{p^k}_i = 0$$

with some non-zero coefficients, then among the non-zero coefficients λ_{ik} there would be one with maximum value of $i'+k$, say m ; and it would follow that

$$0 \equiv \sum_{i'+k=m} \lambda_{ik} v^{p^k}_i \pmod{M_{m-1}},$$

which contradicts the linear independence of the elements $v^{p^k}_i$, with $i'+k=m$, modulo M_{m-1} over F. Hence the elements

$$v^{p^k}_i \quad (i=1, 2, \ldots, \mu ; \ k=0, 1, \ldots)$$

are linearly independent over F.

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

If there were an element x in M not a linear combination of the elements $v_i^{p^k}$, then

$$x \in L^*,$$
$$x \in L + L^p + \ldots + L^{p^h}, \text{ for some } h \geqslant 0,$$
$$x \in M_h.$$

Among all such elements there would be one with minimum value of h. If $h=0$, then

$$x \in M_0 = \sum_{i=1}^{\mu_0} {}^{\bullet} Fa_i,$$

contrary to the first property of x. If $h>0$, then

$$x \equiv \sum_{i \leqslant h} {}^{\bullet} \lambda_i v_i^{p^{h-i'}} \pmod{M_{h-1}}, \quad (\lambda_i \in F),$$

and thus the element

$$x' = x - \sum_{i \leqslant h} {}^{\bullet} \lambda_i v_i^{p^{h-i'}}$$

could not be a linear combination of the elements $v_i^{p^k}$. But the fact that x' is in M_{h-1} contradicts the minimum property of x. Consequently the elements $v_i^{p^k}$ form a basis of M over F. This proves (a) and (b) for perfect ground fields.

The F-Lie-ring M has the basis elements

$$v_1, v_1^p, v_1^{p^2}, \ldots,$$
$$v_2, v_2^p, v_2^{p^2} \ldots,$$
$$\ldots\ldots\ldots\ldots$$
$$v_\mu, v_\mu^p, v_\mu^{p^2}, \ldots.$$

Applying the straightening procedure of Birkhoff to any linear combination of higher products of the basis elements of M, we arrive at the fact that the F-ring $\langle M \rangle$ generated by M and the unit element consists of all linear combinations of the elements

$$v_1^{\alpha_1} v_2^{\alpha_2} \ldots v_\mu^{\alpha_\mu} \quad (0 \leqslant \alpha_i). \tag{7}$$

From (5) it follows that the degree of the basis element $v_1^{\alpha_1} v_2^{\alpha_2} \ldots v_\mu^{\alpha_\mu}$ is equal to $\sum_{i=1}^{\mu} {}^{\bullet} \alpha_i p^{i'}$ and that the highest term is equal to $a_1^{p^{1'}\alpha_1} a_2^{p^{2'}\alpha_2} \ldots a_\mu^{p^{\mu'}\alpha_\mu}$.

For a non-trivial linear combination

$$x = \sum {}^{\bullet} \lambda_{\alpha_1 \alpha_2 \ldots \alpha_\mu} v_1^{\alpha_1} v_2^{\alpha_2} \ldots v_\mu^{\alpha_\mu}$$

of the elements (7), denote by d the maximum of all the numbers $\sum_{i=1}^{\mu} {}^{\bullet} \alpha_i p^{i'}$ with $\lambda_{\alpha_1 \alpha_2 \ldots \alpha_\mu} \neq 0$.

It follows that $d(x) = d$

and $$s(x) = \sum {}^{\bullet} \lambda_{\alpha_1 \alpha_2 \ldots \alpha_\mu} a_1^{p^{1'}\alpha_1} a_2^{p^{2'}\alpha_2} \ldots a_\mu^{p^{\mu'}\alpha_\mu},$$

summation being over all sets of values of $\alpha_1, \alpha_2, \ldots \alpha_\mu$ for which $\sum_{i=1}^{\mu} {}^{\bullet} \alpha_i p^{i'} = d$.

From this it follows that the elements (7) form a basis of $\langle M \rangle$ over F. This proves (c) for perfect ground fields.

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

Now assume that

$$\langle M\rangle \frown L^* \neq M.$$

Then there is an element

$$x = \sum \lambda_{\alpha_1\alpha_2\dots\alpha_\mu} v_1^{\alpha_1} v_2^{\alpha_2} \dots v_\mu^{\alpha_\mu}$$

in L^* which is not in M. Since x is not in M, it follows that $x \neq 0$. Among all the elements in $\langle M\rangle \frown L^*$ but not in M, let x be one of minimum degree. It follows that

$$s(x) = \sum \lambda_{\alpha_1\alpha_1\dots\alpha_\mu} a_1^{p^{1'}\alpha_1} a_2^{p^{2'}\alpha_2} \dots a_\mu^{p^{\mu'}\alpha_\mu},$$

summation being over those sets of values of $\alpha_1, \alpha_2, \dots, \alpha_\mu$ for which $\sum_{i=1}^{\mu} \alpha_i p^{i'} = d(x)$. But since $x \in L^*$, it follows that $d(x) = p^\nu$ and that $s(x) = \sum_{i=1}^{\mu} \lambda_i a_i^{p^\nu}$. Thus $\lambda_{\alpha_1\alpha_2\dots\alpha_\mu} = 0$ whenever $\sum_{i=1}^{\mu} \alpha_i p^{i'} = d(x)$ and two indices α_i and α_j do not vanish. Furthermore

$$x = \sum_{i' \leqq \nu} \lambda_i v_i^{p^\nu - i'} + \sum \lambda_{\alpha_1\alpha_2\dots\alpha_\mu} v_1^{\alpha_1} v_2^{\alpha_2} \dots v_\mu^{\alpha_\mu}$$

the second summation being over all sets of values of $\alpha_1, \alpha_2, \dots, \alpha_\mu$ for which $\sum_{i=1}^{\mu} \alpha_i p^{i'} < p^\nu$. Thus $x' = x - \sum_{i' \leqq \nu} \lambda_i v_i^{p^\nu - i'}$ is not contained in M, but $x' \in \langle M\rangle \frown L^*$ and $d(x') < d(x)$. This contradicts the minimum property of x. It follows that

$$\langle M\rangle \frown L^* = M.$$

This proves (d) for perfect fields.

We now prove that the elements

$$\text{(8)} \qquad \begin{cases} a_i^{p^k}, & 0 \leqq k < i',\ \mu_0 < i \leqq \mu, \\ a_i^{p^k}, & i > \mu \end{cases}$$

form a basis of L^* modulo M over F.

Suppose that the elements (8) do not span L^* modulo M over F. Then there is an element

$$x = \sum_{i=1}^{n} \sum_{k=0}^{\infty} \lambda_{ik} a_i^{p^k}$$

of L^* which is not a linear combination of the elements (8) modulo M. It follows that $x \neq 0$. Among all such elements choose an element x of minimum degree, p^ν say. If for any coefficient $\lambda_{ik} \neq 0$, either $0 \leqq k < i'$, $\mu_0 < i \leqq \mu_i$ or $i > \mu$, then we could subtract the corresponding term from x and the remainder would have the same property and would have one less non-vanishing term. Continuing this reduction we find that among all the competing elements of the same degree, the element x may be chosen so that no contribution is made to it by the elements (8). It follows that

$$x = \sum_{i=1}^{\mu} \sum_{k=i'}^{\infty} \lambda_{ik} a_i^{p^k} \equiv \sum_{i' \leqq \nu} \lambda_{i\nu} v^{p^\nu - i'} \pmod{L + L^p + \dots + L^{p^{\nu-1}}},$$

$$d\left(x - \sum_{i' \leqq \nu} \lambda_{i\nu} v_i^{p^\nu - i'}\right) < d(x).$$

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

Since x and the element

$$x' = x - \sum_{i' \leqslant \nu} \lambda_{i\nu} v_i^{p^\nu - i'}$$

both belong to L, and since $d(x') < d(x)$, it follows from the minimal property of x that x' is congruent to a linear combination of the elements (8) modulo M. The same then applies to

$$x = x' + \sum_{i' \leqslant \nu} \lambda_{i\nu} v_i^{p^\nu - i'},$$

so that we arrive at a contradiction. We conclude that the elements (8) span L^* modulo M over F.

Now assume that there is a non-trivial congruence relation

$$x = \sum_{i=1}^{n} \sum_{k<i'} \lambda_{ik} a_i^{p^k} \equiv 0 \pmod{M},$$

where, for convenience, we define $(\mu+1)' = (\mu+2)' = \ldots = \infty$. Let m be the maximum of all the indices k for which an inequality $\lambda_{ik} \neq 0$ holds. It follows that x belongs to M_m and so

$$x = \sum_{i \leqslant \mu_0 + \mu_1 + \ldots + \mu_m} \sum_{k=0}^{m-i'} \eta_{ik} v_i^{p^{m-k}},$$

$$s(x) = \sum_{m<i'} \lambda_{im} a_i^{p^m} = \sum_{m \geqslant i'} \eta_{i0} a_i^{p^m},$$

which contradicts the linear independence of the elements $a_1^{p^m}, \ldots, a_\mu^{p^m}$.

Hence the elements (8) form a basis of L^* modulo M over F.

Inspecting this basis, we find that $\dim_F(L^* - M) < \infty$ if and only if $\mu = n$. The number of basis elements is then given by the formula indicated under (e).

We now prove that the elements

$$a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n} \quad \text{with } 0 \leqslant \alpha_i < p^{i'} \tag{9}$$

form a basis of $A(L)$ over $\langle M \rangle$.

Assume that there is an element x in $A(L)$ which is not a linear combination of the elements (9) over $\langle M \rangle$. It follows that $x \neq 0$. Let x have minimal degree. Writing

$$x = \sum \lambda_{\alpha_1 \alpha_2 \ldots \alpha_n} a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n},$$

we may subtract any term contributed by the elements (9). Hence we are allowed to make the additional assumption that at least one of the inequalities $\alpha_i \geqslant p^{i'}$ holds in each case in which $\lambda_{\alpha_1 \alpha_2 \ldots \alpha_n} \neq 0$. Then, by the Euclidian algorithm,

$$\alpha_i = q_i p^{i'} + r_i \quad \text{with } 0 \leqslant r_i \leqslant p^{i'}, \text{ for } i = 1, 2, \ldots, \mu.$$

Now

$$s(a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n}) = s(v_1^{q_1} v_2^{q_2} \ldots v_\mu^{q_\mu} a_1^{r_1} a_2^{r_2} \ldots a_\mu^{r_\mu} a_{\mu+1}^{\alpha_{\mu+1}} \ldots)$$

Hence x has the same highest terms as the linear combination

$$y = \sum_{\alpha_1 + \alpha_2 + \ldots + \alpha_\mu = d(x)} \lambda_{\alpha_1 \alpha_2 \ldots \alpha_n} v_1^{q_1} \ldots v_\mu^{q_\mu} a_1^{r_1} \ldots a_\mu^{r_\mu} a_{\mu+1}^{\alpha_{\mu+1}} \ldots$$

of the elements (9) over $\langle M \rangle$. It follows that $x - y$ has lower degree than x. Hence it must be

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

a linear combination of the elements (9) over $\langle M\rangle$. The same must then apply to x. Since this contradicts our assumption concerning x, it follows that every element of $A(L)$ is a linear combination of the elements (9) with coefficients in $\langle M\rangle$. For any non-trivial linear combination

$$x=\sum_{0\leqq\alpha_i\leqq p^{i'}} \Lambda_{\alpha_1\alpha_2\dots\alpha_n}\, a_1^{\alpha_1}a_2^{\alpha_2}\dots a_n^{\alpha_n} \tag{10}$$

of the elements (9) with coefficients $\Lambda_{\alpha_1\alpha_2\dots\alpha_n}$ in $\langle M\rangle$, there are some coefficients $\neq 0$. For the corresponding terms we find

$$s(\Lambda_{\alpha_1\alpha_2\dots\alpha_n})=\sum{}' \lambda_{\alpha_1\alpha_2\dots\alpha_n;\ \beta_1\beta_2\dots\beta_\mu}\, a_1^{\beta_1 p^{1'}}a_2^{\beta_2 p^{2'}}\dots a_\mu^{\beta_\mu p^{\mu'}},$$

where the accent on the summation symbol indicates that only those μ-tuples $\beta_1, \beta_2, \dots, \beta_\mu$ are admitted for which

$$\sum_{i=1}^{\mu}{}' \beta_i p^{i'}=d(\Lambda_{\alpha_1\alpha_2\dots\alpha_n})$$

It follows that

$$s(\Lambda_{\alpha_1\alpha_2\dots\alpha_n}a_1^{\alpha_1}a_2^{\alpha_2}\dots a_n^{\alpha_n})=\sum{}' \lambda_{\alpha_1\alpha_2\dots\alpha_n;\ \beta_1\beta_2\dots\beta_\mu}\, a_1^{\alpha_1+\beta_1 p^{1'}}\dots a_\mu^{\alpha_\mu+\beta_\mu p^{\mu'}}a_{\mu+1}^{\alpha_{\mu+1}}\dots . \tag{11}$$

Under what circumstances does it occur that in the development (11) for the leading members of two summands on the right hand side of (10) there are proportional terms $\neq 0$? Suppose that in the development of $s(\Lambda_{\alpha_1\alpha_2\dots\alpha_n}a_1^{\alpha_1}a_2^{\alpha_2}\dots a_n^{\alpha_n})$ there is a term

$$\lambda_{\alpha_1\alpha_2\dots\alpha_n;\ \beta_1\beta_2\dots\beta_\mu}\, a_1^{\alpha_1+\beta_1 p^{1'}}\dots a_\mu^{\alpha_\mu+\beta_\mu p^{\mu'}}a_{\mu+1}^{\alpha_{\mu+1}}\dots\neq 0,$$

and in the development of $s(\Lambda_{\gamma_1\gamma_2\dots\gamma_n}a_1^{\gamma_1}a_2^{\gamma_2}\dots a_n^{\gamma_n})$ there is a term

$$\lambda_{\gamma_1\gamma_2\dots\gamma_n;\ \delta_1\delta_2\dots\delta_\mu}\, a_1^{\gamma_1+\delta_1 p^{1'}}\dots a_\mu^{\gamma_\mu+\delta_\mu p^{\mu'}}a_{\mu+1}^{\gamma_{\mu+1}}\dots\neq 0,$$

such that

$$\alpha_i+\beta_i p^{i'}=\gamma_i+\delta_i p^{i'}\quad (i=1, 2, \dots, \mu),$$
$$\alpha_{\mu+j}=\gamma_{\mu+j}\quad (j=1, 2, \dots, n-\mu),$$

and hence there hold the congruences

$$\alpha_i\equiv\gamma_i \pmod{p^{i'}},\quad (i=1, 2, \dots, \mu).$$

From these congruences and the conditions

$$0\leqq\alpha_i<p^{i'},\ 0\leqq\gamma_i<p^{i'},\quad (i=1, 2, \dots, \mu),$$

it follows that $\alpha_i=\gamma_i (i=1, 2, \dots, \mu)$ and hence that $\beta_i=\delta_i (i=1, 2, \dots, \mu)$. In other words, the highest terms of the summands on the right hand side of (10) are linearly independent. This shows that x does not vanish. Therefore the elements (9) form a basis of $A(L)$ over $\langle M\rangle$, which proves (e).

Inspecting the number of basis elements in the case in which $\mu=n$, we obtain for the number of such basis elements the value $p^{1'+2'+\dots+\mu'}$.

This completes the proof of the lemma for perfect ground fields.

Now let F be an arbitrary field of characteristic p. Then there is a perfect extension $\tilde{F}$ of F.

We determine a basis $u_1, u_2, \dots, u_{\mu_0}$ of M_0 modulo M_0' over F, a basis $u_{\mu_0+1}, \dots, u_{\mu_0+\mu_1}$ of M_1 modulo M_1' over F, a basis $u_{\mu_0+\mu_1+1}, \dots, u_{\mu_0+\mu_1+\mu_2}$ of M_2 modulo M_2' over F, and so on, the number μ_i being defined as the dimension of M_i-M_i' over F.

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

On the other hand, we construct the extension $A(L)_{\tilde{F}}$ of $A(L)$ as the product ring of $A(L)$ and $\tilde{F}$ over F. This contains the Lie-algebra $L\tilde{F}$ over $\tilde{F}$ and in fact

$$A(L)_{\tilde{F}} = A(L\tilde{F}).$$

We find that $M\tilde{F}$ satisfies the requirements of the lemma with respect to $\tilde{F}$. Hence we may construct $v_1, v_2, \dots, v_\mu$ as previously, where

$$\mu_i = \dim_F[(M\tilde{F})_i - (M\tilde{F})'_i] = \dim_F(M_i - M'_i).$$

We find that

$$\mu = \sum_{i=0}^{\infty} \mu_i = \sum_{i=0}^{\infty} \dim_F(M_i - M'_i) = \sum_{i=0}^{\infty} \dim_{\tilde{F}}[(M\tilde{F})_i - (M\tilde{F})'_i],$$

and therefore $0 < \mu \leqslant n$. This proves (a).

We prove (b) exactly as before.

It is easily shown that

$$\langle M\tilde{F}\rangle = \langle M\rangle\tilde{F},$$
$$(L\tilde{F})^* = L^*\tilde{F},$$
$$\langle M\tilde{F}\rangle \cap (L\tilde{F})^* = [\langle M\rangle\tilde{F}] \cap [L^*\tilde{F}] = (\langle M\rangle \cap L)\tilde{F}.$$

We have proved that $\langle M\tilde{F}\rangle \cap (L\tilde{F})^* = M\tilde{F}$. Since $\langle M\rangle \cap L \supseteq M$ and $(\langle M\rangle \cap L)\tilde{F} = M\tilde{F}$, it follows that $\langle M\rangle \cap L = M$, which proves (d).

We prove exactly as before that the elements $u_1^{\alpha_1} u_2^{\alpha_2} \dots u_n^{\alpha_n}$ $(0 \leqslant \alpha_i)$ span $\langle M\rangle$ over F. In order to prove the linear independence of the elements $u_1^{\alpha_1} u_2^{\alpha_2} \dots u_n^{\alpha_n}$ over F, we proceed as follows. From the construction of the elements $u_1, u_2, \dots, u_\mu$ and $v_1, v_2, \dots, v_\mu$ there follow relations

$$u_h = \sum_{i' \leqslant h'} \sum_{j=0}^{p^{h'-i'}} \xi_{hij} v_i^{p^j}, \tag{12}$$

$$v_h = \sum_{i' \leqslant h'} \sum_{j=0}^{p^{h'-i'}} \eta_{hij} u_i^{p^j}. \tag{13}$$

We consider the subset S_f formed by 0 and all elements of $\langle M\tilde{F}\rangle$ of degree f or less with respect to the basis $a_1, a_2, \dots, a_n$ of $L\tilde{F}$ over $\tilde{F}$. Obviously S_f is an $\tilde{F}$-module containing all linear combinations of the elements

$$v_1^{\alpha_1} v_2^{\alpha_2} \dots v_\mu^{\alpha_\mu} \tag{14}$$

satisfying

$$\sum_{i=1}^{\mu} \alpha_i p^{i'} \leqslant f. \tag{14a}$$

If the element

$$x = \sum \lambda_{\alpha_1\alpha_2\dots\alpha_\mu} v_1^{\alpha_1} v_2^{\alpha_2} \dots v_\mu^{\alpha_\mu}$$

of S_f is not a linear combination of the elements (14) satisfying (14a), then let x be chosen so that no contribution is made to x by the elements (14) satisfying (14a). It follows from the construction of the elements $v_1, v_2, \dots, v_\mu$ that

$$s(x) = s\left(\sum \lambda_{\alpha_1\alpha_2\dots\alpha_\mu} v_1^{\alpha_1} v_2^{\alpha_2} \dots v_\mu^{\alpha_\mu}\right),$$

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

where not only

$$\sum_{i=1}^{\mu} \alpha_i p^{i'} = d(x)$$

but also $\sum_{i=1}^{\mu} \alpha_i p^{i'} > f$ for any coefficient $\lambda_{\alpha_1 \alpha_2 \dots \alpha_\mu} \neq 0$. Hence $d(x) > f$, contrary to our assumption. Hence the elements (14) satisfying (14a) form a basis of S_f over $\tilde{F}$. From (12) it follows that $d(u_h) \leqslant p^{h'}$. Hence all the elements

$$u_1^{\alpha_1} u_2^{\alpha_2} \dots u_\mu^{\alpha_\mu} \tag{15}$$

satisfying

$$\sum_{i=1}^{\mu} \alpha_i p^{i'} \leqslant f$$

belong to S_f. From the construction of the elements $u_1, u_2, \dots, u_\mu$ there follow commutation rules

$$u_i \circ u_j = \sum_{l+k' < i'+j'} \chi_{ijkl} u_k^{p^l}.$$

Using these rules, we may substitute the right hand side of (13) in (14) and straighten out the expression so that each element (14) will be expressed as a linear combination of the elements (15) over $\tilde{F}$. Since the two sets (14) and (15) have the same number of elements, it follows that the set (14) forms another basis of $\tilde{F}$. Consequently the elements (14) are linearly independent over F.

Since f is arbitrary, it follows that the elements

$$u_1^{\alpha_1} u_2^{\alpha_2} \dots u_\mu^{\alpha_\mu} \quad (0 \leqslant \alpha_i)$$

are linearly independent over F.

The statement (e) follows from the corresponding statement for the difference module $(L\tilde{F})^* - M\tilde{F}$. This completes the proof of lemma 4.†

From lemma 2 it follows that to each element x of L there corresponds a derivation $\underset{\sim}{x}$ defined by the formula

$$\underset{\sim}{x} = \begin{pmatrix} u \\ x \circ u \end{pmatrix}, \quad (u \in L).$$

The correspondence

$$x \to \underset{\sim}{x}$$

yields a representation P^* of the F-Lie-ring L^* by linear transformations of L. Since there are at most n^2 linearly independent linear transformations of the Lie-algebra L, since it is of dimension n over F, it follows that the difference ring of L modulo the kernel $L^*_{P^*}$ is of finite dimension.

Each element of $L^*_{P^*}$ is permutable with each element of L. Since L generates the ring $A(L)$, it follows that $L^*_{P^*}$ is contained in the center $\mathfrak{Z}$ of $A(L)$. Conversely, each element of $\mathfrak{Z} \cap L^*$ belongs to the kernel of P^* and so

$$L^*_{P^*} = \mathfrak{Z} \cap L^*.$$

† This proof can be used to cover more ground by using the language of filtered and graded rings (see Colby Summer Institute Lectures, Appendix to Zassenhaus, "Representation Theory of Lie-algebras of prime characteristic").

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

We denote by $\mathfrak{o}$ the F-ring generated by the unit element and $\mathfrak{Z} \cap L^*$, *i.e.*,

$$\mathfrak{o} = \langle F, \mathfrak{Z} \cap L^* \rangle.$$

Now $\mathfrak{o}$ appears as a subring of the center of $A(L)$. By lemma 4, $\mathfrak{o}$ is isomorphic over F to the polynomial ring in n variables over F.

There are n elements $u_1, u_2, \ldots, u_n$ of $\mathfrak{Z} \cap L^*$ such that every element of $\mathfrak{o}$ can be expressed uniquely as a polynomial in $u_1, u_2, \ldots, u_n$ with coefficients in F. The elements $u_i^{p^j}$ $(i = 1, 2, \ldots, n\ ;\ j = 0, 1, 2, \ldots)$ form a basis of $\mathfrak{Z} \cap L^*$ over F.

If F is perfect, then, according to lemma 4, there is a basis of $A(L)$ over $\mathfrak{o}$ consisting of p^l elements, where $l = \dim_F(L^* - \mathfrak{Z} \cap L^*)$.

§ 2. In this section we introduce the new concept of a quotient ring, which is needed in the sequel. Since the results are of some independent interest, they will be developed somewhat more fully than is strictly necessary for the present purpose.

Definition : A *scalar* of a semi-ring† $\mathfrak{D}$ is any single-valued mapping ν of $\mathfrak{D}$ into itself satisfying the conditions

$$\text{(i)}\quad \nu(a+b) = \nu a + \nu b$$
$$\text{(ii)}\quad \nu(ab) = (\nu a)b = a(\nu b)$$

for any two elements a, b of $\mathfrak{D}$.

The set of all scalars forms a semi-ring of operators of the additive semi-group of $\mathfrak{D}$ with the identity mapping 1 as unit element. If $\mathfrak{D}$ is a module, then the scalars form a ring of operators of the additive group of $\mathfrak{D}$. If $\mathfrak{D}\mathfrak{D} = \mathfrak{D}$, the scalars form a commutative ring. At any rate, the scalars of $\mathfrak{D}$ induce a commutative semi-ring on the additive semi-group of $\mathfrak{D}\mathfrak{D}$.

Definition : A scalar ν of $\mathfrak{D}$ is called a *denominator* if

(i) $\nu a = 0$ implies $a = 0$,

(ii) $\nu\mu = \mu\nu$ for any scalar μ.

The set of all denominators of $\mathfrak{D}$ forms a multiplicative abelian semi-group with unit element and cancellation law.

Definition : The *quotient ring* $Q(\mathfrak{D})$ of a semi-ring $\mathfrak{D}$ consists of the set of all quotient symbols

$$\frac{a}{\nu}$$

with $a \in \mathfrak{D}$ and ν a denominator of $\mathfrak{D}$.

Equality of two quotient symbols is defined by the rule

$$\frac{a}{\nu} = \frac{b}{\mu} \quad \text{if and only if} \quad \mu a = \nu b.$$

Addition and multiplication of two of these symbols is defined by the rules

$$\frac{a}{\nu} + \frac{b}{\mu} = \frac{\mu a + \nu b}{\nu\mu},$$

$$\frac{a}{\nu} \cdot \frac{b}{\mu} = \frac{ab}{\nu\mu}.$$

† A *semi-ring* is defined to be a commutative additive semi-group (*i.e.*, a semi-module) in which there is defined a multiplication assigning to any two elements a, b of the semi-module a third element ab of the semi-module, such that from $a = a'$ and $b = b'$ it follows that $ab = a'b'$, and furthermore the two distributive laws $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$ hold.

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

It follows that the quotient ring of a semi-ring $\mathfrak{D}$ is itself a semi-ring.

There is an isomorphism

$$a \to \frac{a}{1}$$

between $\mathfrak{D}$ and a subsemi-ring of the quotient ring. This isomorphism is used to embed $\mathfrak{D}$ into its quotient ring, by replacing the quotient symbol $\frac{a}{1}$ in $Q(\mathfrak{D})$ by the element a of $\mathfrak{D}$ without interfering with the laws of equality, addition and multiplication governing the semi-ring $Q(\mathfrak{D})$. Every scalar ν of $\mathfrak{D}$ is extended to a scalar of the quotient ring by the definition

$$\nu\left(\frac{a}{\mu}\right) = \frac{\nu a}{\mu}.$$

The scalars of $\mathfrak{D}$ then form a subsemi-ring of the semi-ring of scalars of $Q(\mathfrak{D})$ such that the semi-ring of scalars of $Q(\mathfrak{D})$ of the form $\frac{\nu}{\mu}$, where ν is derived from a scalar of $\mathfrak{D}$ and μ is derived from a denominator of $\mathfrak{D}$, is isomorphic to the quotient ring of the scalar semi-ring of $\mathfrak{D}$. Here $\frac{\nu}{\mu}$ is defined by the rule

$$\frac{\nu}{\mu}\left(\frac{a}{\lambda}\right) = \frac{\nu a}{\mu\lambda}.$$

The scalar $\frac{\nu}{\mu}$ of $Q(\mathfrak{D})$ is a denominator of $Q(\mathfrak{D})$ if and only if ν is a denominator of $\mathfrak{D}$. The set of all the denominators of $Q(\mathfrak{D})$ of the form $\frac{\nu}{\mu}$, where ν and μ are denominators of $\mathfrak{D}$, forms an abelian group which is isomorphic to the quotient group of the multiplicative semi-group constituted by the denominators of $\mathfrak{D}$.

If $\mathfrak{D}$ is finitely determined, *i.e.*, if there is a finite number of elements $a_1, a_2, \ldots, a_r$ of $\mathfrak{D}$ such that $\mathfrak{D}$ is the smallest two-sided ideal of $\mathfrak{D}$ containing $a_1, a_2, \ldots, a_r$, then every scalar of $Q(\mathfrak{D})$ is a quotient of a scalar of $\mathfrak{D}$ and a denominator of $\mathfrak{D}$. If $\mathfrak{D}$ has a unit element, then $\mathfrak{D}$ is finitely determined.

We call a semi-ring *closed with respect to quotients* if it coincides with its own quotient ring. This happens if and only if its denominators form an abelian multiplicative group. The quotient ring of a finitely determined semi-ring is closed with respect to quotients.

If a given semi-ring $\mathfrak{D}$ is embedded into a semi-ring $\mathfrak{D}_1$ in such a way that any denominator of $\mathfrak{D}$ is induced by a denominator of $\mathfrak{D}_1$, then for each denominator ν of $\mathfrak{D}$ there is a denominator ν' of $Q(\mathfrak{D}_1)$ such that $\nu'\nu$ induces the identity operator of $\mathfrak{D}$. It then follows that the correspondence

$$\frac{a}{\nu} \to \nu' a$$

is an isomorphism between $Q(\mathfrak{D})$ and a subsemi-ring of $Q(\mathfrak{D}_1)$ over $\mathfrak{D}$.

If $\mathfrak{D}$ is a semi-ring over a commutative ring $\mathfrak{o}$ with a unit element*, then the scalars form an associative $\mathfrak{o}$-semi-ring. We usually impose the additional condition

$$\lambda\nu = \nu\lambda \quad (\lambda \in \mathfrak{o}) \tag{16}$$

on the scalars ν of $\mathfrak{D}$, a condition which is automatically satisfied in the case when $\mathfrak{D}\mathfrak{D} = \mathfrak{D}$.

* This means that for every element of λ of $\mathfrak{o}$ and every element a of $\mathfrak{D}$, there is uniquely defined the product λa as an element of $\mathfrak{D}$, such that $(\lambda_1 + \lambda_2)a = \lambda_1 a + \lambda_2 a$, $\lambda(a_1 + a_2) = \lambda a_1 + \lambda a_2$, $(\lambda_1\lambda_2)a = \lambda_1(\lambda_2 a)$, $1a = a$, where 1 is the unit element of $\mathfrak{o}$.

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

The previous definitions are used as before.

The quotient ring of $\mathfrak{D}$ is again an o-semi-ring.

If the elements of the semi-ring $\mathfrak{D}$ form an additive group and hence a module, the same is true for the quotient ring $Q(\mathfrak{D})$.

If the semi-ring $\mathfrak{D}$ is associative, then $Q(\mathfrak{D})$ is also associative. If $\mathfrak{D}$ is an associative semi-ring with a unit element, then the scalars of $\mathfrak{D}$ are realised by the multiplications by elements of the center of $\mathfrak{D}$. The denominators of $\mathfrak{D}$ are realised by the non zero-divisors in the center of $\mathfrak{D}$.

This shows that our concept of a quotient ring coincides with the usual concept, for commutatve rings with a unit element.

An algebra over a field F is closed with respect to quotients. This, of course, only holds if the scalars are restricted by the condition (16).

If $\mathfrak{D}$ is a semi-algebra over a field F, *i.e.*, if $\mathfrak{D}$ is a linear space with basis $a_1, a_2, \ldots, a_n$ over F with the multiplication rule

$$\left(\sum \lambda^i a_i\right)\left(\sum \mu^k a_k\right) = \sum \gamma_{ik}^j \lambda^i \mu^k a_j$$

with arbitrary multiplication constants $\gamma_{ik}^j \in F$, then the scalars of $\mathfrak{D}$ (restricted by (16)!) form an algebra over F and $\mathfrak{D}$ is closed with respect to quotients.

If o is an integral domain, then the quotient ring of o is a field, the quotient field of o.

If the o-semi-ring $\mathfrak{D}$ has the finite basis $a_1, a_2, \ldots, a_n$ over the *commutative* ring o with a unit element*, then $Q(\mathfrak{D})$ has the basis $a_1, a_2, \ldots, a_n$ over $Q(\mathfrak{o})$ and the rule of multiplication for $Q(\mathfrak{D})$ over $Q(\mathfrak{o})$ turns out to be the same as the rule for multiplication for $\mathfrak{D}$ over o.

But even when we do not know of a basis of an o-semi-ring $\mathfrak{D}$ over a commutative ring o with a unit element, it may happen that the quotient ring of $\mathfrak{D}$ is a $Q(\mathfrak{o})$-semi-ring. In other words, we may raise the question under what circumstances it is possible to define a product ΛU for any element Λ of $Q(\mathfrak{o})$ and any element U of $Q(\mathfrak{D})$, such that $Q(\mathfrak{D})$ becomes a $Q(\mathfrak{o})$-semi-ring and the new multiplication coincides with the old one if $\Lambda \in \mathfrak{o}$ and $U \in \mathfrak{D}$. We shall give an answer under the assumption that o is an integral domain.

As a necessary condition we find that $\mathfrak{D}$ must be an o-semi-module without torsion ; *i.e.*, from $\lambda \neq 0$ in o and $\lambda u = \lambda v$ it must follow that $u = v$. In fact if $Q(\mathfrak{D})$ is a $Q(\mathfrak{o})$-semi-ring of the kind described above, then from $\lambda \neq 0$ in o and $\lambda u = \lambda v$, with $u, v \in \mathfrak{D}$ it follows that

$$u = 1u = (\lambda^{-1}\lambda)u = \lambda^{-1}(\lambda u) = \lambda^{-1}(\lambda v) = (\lambda^{-1}\lambda)v = 1v = v.$$

Conversely, if $\mathfrak{D}$ is an o-module without torsion, then to each element $\lambda \neq 0$ of o there corresponds a denominator of $\mathfrak{D}$ and hence $Q(\mathfrak{D})$ has a denominator λ' satisfying $\lambda'\lambda = 1$, which proves that $Q(\mathfrak{D})$ is a $Q(\mathfrak{o})$-semi-algebra if $\mathfrak{D}$ is a finite o-module without torsion over the integral domain o.

The quotient-ring of a Lie-ring is itself a Lie-ring.

After these preliminary remarks we make an application to the universal embedding algebra $A(L)$ of a Lie-algebra L over a field F of characteristic $p > 0$.

Since $A(L)$ is without divisors of zero, it follows that $A(L)$ is an o-module without torsion. Hence the quotient ring K of $A(L)$ is a $Q(\mathfrak{o})$-ring. It has no divisors of zero ; for from

$$0 \neq X \in K, \quad 0 \neq Y \in K$$

it follows that

$$X = \frac{x}{\lambda}, \quad Y = \frac{y}{\mu},$$

* *I.e.*, $\mathfrak{D}$ is a vector-module with basis $a_1, a_2, \ldots, a_n$ over o.

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

where $0 \neq \lambda \in \mathfrak{o}$, $0 \neq \mu \in \mathfrak{o}$, $0 \neq x \in A(L)$, $0 \neq y \in A(L)$. Hence

$$XY = \frac{xy}{\lambda\mu} \neq 0,$$

since $xy \neq 0$.

Since $\mathfrak{o}$ belongs to the center of $A(L)$, we may consider $Q(\mathfrak{o})$ as a subfield of the center of K. Furthermore

$$K = Q(\mathfrak{o})A(L).$$

Hence there is a basis B of K over $Q(\mathfrak{o})$ contained in $A(L)$.

Let $\tilde{F}$ be a perfect algebraic extension of F. Then we find that the product ring $L \times \tilde{F}$ of L and $\tilde{F}$ over F is a Lie-algebra of dimension n over F which has as its universal embedding algebra $A(L \times \tilde{F})$, the product ring of $A(L)$ and $\tilde{F}$ over F. The center $\tilde{\mathfrak{Z}}$ of $A(L \times \tilde{F})$ is the product ring of $\mathfrak{Z}$ and $\tilde{F}$ over F and furthermore

$$\begin{aligned}(L \times \tilde{F})^* &= L^* \times \tilde{F} = L^*\tilde{F},\\ (L \times \tilde{F})^* \cap \tilde{\mathfrak{Z}} &= (L \cap \mathfrak{Z}) \times \tilde{F} = (L \cap \mathfrak{Z})\tilde{F},\\ \langle (L\tilde{F})^* \cap \tilde{\mathfrak{Z}} \rangle &= \mathfrak{o} \times \tilde{F} = \mathfrak{o}\tilde{F}.\end{aligned}$$

The quotient ring K of $A(L \times \tilde{F})$ contains the quotient ring K of $A(L)$, with the natural embedding. It follows that $Q(\mathfrak{o})\tilde{F} = Q(\mathfrak{o}) \times \tilde{F}$ has no divisors of zero. Since $\tilde{F}$ is algebraic over F, it follows that $(Q(\mathfrak{o}) \times \tilde{F})_F$ is a field. Hence $(Q(\mathfrak{o}) \times \tilde{F})_F = Q((\mathfrak{o} \times \tilde{F})_F)$.

From lemma 4 it follows that $A(L \times \tilde{F})$ has a finite basis B over $\mathfrak{o} \times \tilde{F}$; hence $\tilde{K}$ is an algebra over $Q((\mathfrak{o} \times \tilde{F})_F)$. It follows that

$$\begin{aligned}K &= A(L \times \tilde{F})Q(\mathfrak{o} \times \tilde{F}) = A(L)Q(\mathfrak{o})\tilde{F} = K\tilde{F}\\ &= K \times \tilde{F} = (BF \times Q(\mathfrak{o})) \times \tilde{F} = BF \times (Q(\mathfrak{o}) \times \tilde{F})\\ &= BF \times Q(\mathfrak{o} \times \tilde{F});\end{aligned}$$

i.e., B is a basis of $\tilde{K}$ over $Q(\mathfrak{o} \times \tilde{F})$. Since any basis of $\tilde{K}$ over $Q(\mathfrak{o} \times \tilde{F})$ is finite, it follows that B is finite; in fact it consists of p^l elements, where $l = \dim_F(L^* - L^* \cap \mathfrak{Z})$. Hence K is an algebra of dimension p^l over $Q(\mathfrak{o})$ and has no divisors of zero; *i.e.*, it is a division algebra.

The center of K is the quotient field $Q(\mathfrak{Z})$ of the center $\mathfrak{Z}$ of $A(L)$. According to the general theory, the dimension of a division algebra over its centre is a square number. On the other hand,

$$[K : Q(\mathfrak{o})] = [K : Q(\mathfrak{Z})]\,[Q(\mathfrak{Z}) : Q(\mathfrak{o})] = p^l.$$

Hence

$$[K : Q(\mathfrak{Z})] = p^{2m},$$

where m is a non-negative rational integer.

§ 3. LEMMA 5. *$A(L)$ is a maximal order of K.*

Proof: We have to prove that $A(L)$ coincides with any subring Ω of K satisfying

$$A(L) \subseteq \Omega \subseteq \Lambda^{-1}A(L),$$

with $\Lambda \neq 0$ an element of $\mathfrak{Z}$.

Here we may replace Λ by an element $\zeta \neq 0$ of $\mathfrak{o}$.

Denoting the regular representation of K over $Q(\mathfrak{o})$ by R, we find that

$$R(\Lambda)R(\Lambda^{-1}) = R(1) = I_{[K : Q(\mathfrak{o})]},$$

$$\text{Det } R(\Lambda) \neq 0.$$

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

If F is a perfect field we use a basis of $A(L)$ over $\mathfrak{o}$ for computation of $R(\Lambda)$.

If F is not a perfect field, let $\tilde{F}$ be a perfect extension of F and use a basis of $A(L \times \tilde{F})$ over $\mathfrak{o} \times \tilde{F}$. At any rate, the coefficients of the characteristic equation of $R(\Lambda)$ are in $\mathfrak{o} \times (\tilde{F} \cap K) = \mathfrak{o}$. Since the last coefficient is equal to the determinant of $R(\Lambda)$, up to a factor ± 1, it follows that it is an element $\zeta \neq 0$ of $\mathfrak{o}$. Furthermore, since the highest coefficient in the characteristic equation of $R(\Lambda)$ is 1, there is an equation $\zeta = \Lambda\Lambda_1$ with Λ_1 a polynomial expression in Λ with all its coefficients in $\mathfrak{o}$. Hence $\Lambda_1 \in \mathfrak{Z}$. Thus

$$\zeta^{-1}A(L) \supseteq \zeta^{-1}\Lambda_1 A(L) = \Lambda^{-1}\Lambda_1^{-1}\Lambda_1 A(L) = \Lambda^{-1}A(L) \supseteq \Omega \supseteq A(L),$$

so that, in fact, ζ may take the place of Λ.

Assume now that, for a certain subring Ω of K, $A(L) \subset \Omega \subseteq \zeta^{-1}A(L)$. Then

$$\zeta\Omega \subseteq A(L).$$

Among all the elements of Ω not contained in $A(L)$, choose X such that $d(\zeta X)$ is minimal. Let

$$Y = \zeta X.$$

For $\nu = 2, 3, \ldots$, we have

$$Y^\nu = (\zeta X)^\nu = \zeta^\nu X^\nu = \zeta^{-1}(\zeta X^\nu) \in \zeta^{\nu-1}(\zeta\Omega) \subseteq \zeta^{\nu-1}A(L),$$

and, in the notation of lemma 1,

$$\phi(s(Y))^\nu \in \phi(s(\zeta))^{\nu-1} F[x_1, x_2, \ldots, x_n],$$

$$\left(\frac{\phi(s(Y))}{\phi(s(\zeta))}\right)^\nu \in \phi(s(\zeta))^{-1} F[x_1, x_2, \ldots, x_n],$$

$$F[x_1, x_2, \ldots, x_n] \subseteq \left\langle F[x_1, x_2, \ldots, x_n] \frac{\phi(s(Y))}{\phi(s(\zeta))} \right\rangle \subseteq \phi(s(\zeta))^{-1} F[x_1, x_2, \ldots, x_n].$$

Since $F[x_1, x_2, \ldots, x_n]$ is integrally closed, it follows that

$$\frac{\phi(s(Y))}{\phi(s(\zeta))} \in F[x_1, x_2, \ldots, x_n],$$

$$U = \phi^{-1}\left(\frac{\phi(s(Y))}{\phi(s(\zeta))}\right) \in A(L).$$

Since both polynomials $\phi(s(Y))$ and $\phi(s(\zeta))$ are homogeneous, their quotient is also homogeneous; hence $U = s(U)$ and so

$$\phi(s(\zeta U)) = \phi(s(\zeta))\phi(s(U)) = \phi(s(\zeta))\phi(U) = Q(s(\zeta))\frac{\phi(s(Y))}{\phi(s(\zeta))} = \phi(s(Y)).$$

Hence $Y = \zeta U + V$, where either $V \in A(L)$ and $d(V) < d(Y)$ or $V = 0$. But since $X = \zeta^{-1}Y$ is not in $A(L)$ it follows that $V \neq 0$, $d(V) < d(Y)$,

$$\zeta^{-1}V = \zeta^{-1}(Y - \zeta U) = X - U.$$

Since X is not in $A(L)$ and U is in $A(L)$, it follows that $\zeta^{-1}V$ is not in $A(L)$. But then

$$d(\zeta \,.\, \zeta^{-1}V) = d(V) < d(Y) = d(\zeta X),$$

contrary to the minimal property of X. Consequently our assumption concerning Ω must have been wrong. Hence $\Omega = A(L)$; q.e.d.

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

LEMMA 6. *$\mathfrak{Z}$ is an algebraic variety of dimension n over F.*

We have to show that

(1) $\mathfrak{Z}$ is an integrally closed integral domain,

(2) F is a subfield of $\mathfrak{Z}$ such that every element of $\mathfrak{Z}$ which is algebraic over F belongs to F,

(3) $\mathfrak{Z}$ is finitely-generated over F,

(4) There are n algebraically independent elements $u_1, u_2, \dots, u_n$ in $\mathfrak{Z}$ such that

$$Q(\mathfrak{Z}) : F(u_1, u_2, \dots, u_n) < \infty.$$

Proof: (1) $\mathfrak{Z}$, being the center of the integrally closed ring $A(L)$ without divisors of zero, must itself be integrally closed and hence must be an integral domain; in fact, if there is a subring Ω of $Q(\mathfrak{Z})$ satisfying $\mathfrak{Z} \subset \Omega \subseteq \Lambda^{-1}\mathfrak{Z}$ for some Λ contained in $\mathfrak{Z}$, then there is a subring $\Omega A(L)$ of $Q(A(L))$ satisfying $A(L) \subset \Omega A(L) \subseteq \Lambda^{-1} A(L)$, contrary to lemma 5. A consequence of this statement is the customary statement: $\mathfrak{Z}$ is integrally closed in the sense that every element of $Q(\mathfrak{Z})$ which satisfies an algebraic equation with all its coefficients in $\mathfrak{Z}$ and highest coefficient 1 must belong to $\mathfrak{Z}$.

(2) Obviously F is a subfield of $\mathfrak{Z}$. Let x be an arbitrary element of $A(L)$ which does not belong to F. It follows that $d(x) > 0$. Now if

$$\lambda_i \in F \text{ and } \lambda_m \neq 0,\ d(\lambda_m x^m + \lambda_{m-1} x^{m-1} + \dots + \lambda_0) = m\, d(x).$$

Hence x is not algebraic over F.

(4) By lemma 4, $\mathfrak{o}$ is generated by n algebraically independent elements $u_1, u_2, \dots, u_n$ over F. We have already seen that $Q(\mathfrak{Z}) : Q(\mathfrak{o}) < \infty$; observing that $Q(\mathfrak{o}) = F(u_1, u_2, \dots, u_n)$, we have (4).

(3) We observe that $A(L)$ is finitely-generated over $\mathfrak{o}$. Let $a_1, a_2, \dots, a_n$ be a basis of L over F. The derivations $\underline{a_i}, \underline{a_i^p}, \underline{a_i^{p^2}}, \dots$ of L are not all linearly independent over F. Hence there is a linear relation

$$\underline{a_i^{p^{l_i}}} + \sum_{j=0}^{l_i-1} \lambda_{ij} \underline{a_i^{p^j}} = 0 \quad (\lambda_{ij} \in F),$$

i.e.,

$$a_i^{p^{l_i}} + \sum_{j=0}^{l_i-1} \lambda_{ij} a_i^{p^j} = b_i \in \mathfrak{Z} \cap L^*.$$

According to lemma 4, the elements

$$a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n}, \text{ with } 0 \leqslant \alpha_i < p^{l_i}$$

form a basis of $A(L)$ over the ring generated by F and $b_1, b_2, \dots, b_n$. These $p^{l_1} + p^{l_2} + \dots + p^{l_n}$ elements generate $A(L)$ over $\mathfrak{o}$. Furthermore, by Hilbert's theorem, $\mathfrak{o}$ satisfies the maximal condition for ideals. From the theorem of Lasker-Macaulay it follows that the $\mathfrak{o}$-subring $\mathfrak{Z}$ of the finitely-generated $\mathfrak{o}$-ring $A(L)$ is itself finitely-generated over $\mathfrak{o}$. Since $\mathfrak{o}$ is finitely-generated over F, it follows that $\mathfrak{Z}$ is finitely-generated over F; q.e.d.

We summarise the results of lemmas 1–6 in

THEOREM 1. *The universal embedding ring $A(L)$ of a Lie-algebra L over a field F of characteristic $p > 0$ is a maximal order of a division algebra K of dimension p^{2m} over the quotient field of the center $\mathfrak{Z}$ of $A(L)$; furthermore, $\mathfrak{Z}$ is an algebraic variety of dimension n over F.*

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

§ 4. Let P be a commutative F-ring with a unit element, and let $\mathfrak{M}$ be a P-module.

A homomorphism θ of P onto another F-ring θP is called a *homomorphism over* F if $\theta(\lambda 1) = \lambda\theta(1)$ for all $\lambda \in F$. The ring θP is a commutative ring over F with $\theta 1$ as unit element, such that

$$\theta(\lambda x) = \theta(\lambda 1 \,.\, x) = \theta(\lambda 1)\theta(x) = \lambda\theta 1 \,.\, \theta x = \lambda\theta x.$$

We want to define a homomorphism $\theta^{(\mathfrak{m})}$ of $\mathfrak{M}$ onto a θP-module $\theta^{(\mathfrak{m})}\mathfrak{M}$ in as general a manner as possible. For this purpose we define $\theta^{(\mathfrak{m})}\mathfrak{M}$ to be the module with generators

$$\theta^{(\mathfrak{m})}u, \quad (u \in \mathfrak{M}),$$

and the defining relations

$$\theta^{(\mathfrak{m})}(u+v) = \theta^{\mathfrak{m}}u + \theta^{\mathfrak{m}}v, \quad (u, v \in \mathfrak{M}),$$

$$\theta^{(\mathfrak{m})}(Au) = 0 \text{ if } A \text{ belongs to the kernel } P_\theta \text{ of } \theta.$$

Since the correspondence

$$\theta^{(\mathfrak{m})}u \to A\theta^{(\mathfrak{m})}u = \theta^{(\mathfrak{m})}(Au), \quad (A \in P,\ u \in \mathfrak{M}),$$

carries over each defining relation of $\theta^{(\mathfrak{m})}\mathfrak{M}$ into a consequential relation, as can easily be seen, it follows that there is assigned to each element θA of θP an operator of $\theta^{(\mathfrak{m})}\mathfrak{M}$. Furthermore it follows easily that in the correspondence defined above A may have added to it any element of the kernel of P without changing the operator of $\theta^{(\mathfrak{m})}\mathfrak{M}$ assigned to θA. Hence there is uniquely assigned to each element of θP an operator of $\theta^{(\mathfrak{m})}\mathfrak{M}$. It is not difficult to see that this assignment also satisfies all the other rules which are imposed on θP-modules.

If ϕ is any operator-homomorphism of $\mathfrak{M}$ onto a θP-module $\phi\mathfrak{M}$ such that

$$\phi(Au) = \theta A\ \phi u \text{ for all } A \in P,\ u \in \mathfrak{M},$$

then it follows that the relations

$$\left.\begin{aligned} \phi(u+v) &= \phi u + \phi v \\ \phi(Au) &= 0 \end{aligned}\right\} (u, v \in \mathfrak{M},\ A \in P_\theta)$$

hold and hence that there is mapping $\theta^{(\mathfrak{m})}u \to \phi u\,(u \in \mathfrak{M})$ which is an operator homomorphism of the θP-module $\theta^{(\mathfrak{m})}\mathfrak{M}$ onto the θP-module $\phi\mathfrak{M}$. Hence $\theta^{(\mathfrak{m})}\mathfrak{M}$ is the most general θP-module which is operator homomorphic to $\mathfrak{M}$.

The operator-homomorphism between $\mathfrak{M}$ and a θP-module is called a specialization of $\mathfrak{M}$ over θ.

Let $\mathfrak{M}$ be a P-ring, *i.e.*, let $\mathfrak{M}$ be a ring and let there be defined, for any pair of elements $A \in P$ and $u \in \mathfrak{M}$, a product element Au in $\mathfrak{M}$, satisfying, besides the conditions for a P-module, namely,

(1) $Au = A'u'$ if $A = A'$, $u = u'$,
(2) $A(u+v) = Au + Av$,
(3) $(A+A')u = Au + A'u$,
(4) $(AA')u = A(A'u)$,

the following further conditions

(5) $A(uv) = (Au)v = u(Av)$
(6) $1_P u = u$.

The correspondence

$$\theta^{(\mathfrak{m})}v \to \theta^{(\mathfrak{m})}(uv), \quad (u \text{ fixed, } v \text{ arbitrary}),$$

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

between $\theta^{(\mathfrak{m})}(\mathfrak{M})$ and a subset of $\theta^{(\mathfrak{m})}\mathfrak{M}$ carries over each defining relation of $\theta^{(\mathfrak{m})}\mathfrak{M}$ into a consequential relation. Hence to each element $u \in \mathfrak{M}$ there is assigned an operator $\underline{u}$ of $\theta^{(\mathfrak{m})}\mathfrak{M}$ carrying $\theta^{(\mathfrak{m})}v$ into $\theta^{(\mathfrak{m})}(uv)$. The rules

$$\left.\begin{aligned} \underline{u_1+u_2} &= \underline{u_1}+\underline{u_2}, \\ \underline{Au} &= A\underline{u}, \\ \underline{\underline{Au}} &= \underline{0}, \end{aligned}\right\} (u, u_1, u_2 \in \mathfrak{M},\ A \in P,\ \Lambda \in P_\theta)$$

can easily be verified. Hence the correspondence

$$\theta^{(\mathfrak{m})}u \to \underline{u}$$

establishes an operator homomorphism between $\theta^{(\mathfrak{m})}\mathfrak{M}$ and the θP-module $\underline{\theta^{(\mathfrak{m})}\mathfrak{M}}$ formed by all the operators $\underline{u}$ acting on $\theta^{(\mathfrak{m})}\mathfrak{M}$; in fact in $\theta^{(\mathfrak{m})}\mathfrak{M}$ there is defined a unique multiplication by the formula

$$\theta^{(\mathfrak{m})}u\theta^{(\mathfrak{m})}v = \underline{u}\theta^{(\mathfrak{m})}(v) = \theta^{(\mathfrak{m})}(uv).$$

Consequently $\theta^{(\mathfrak{m})}\mathfrak{M}$ is a ring homomorphic to the ring $\mathfrak{M}$. In fact $\theta^{(\mathfrak{m})}\mathfrak{M}$ is a θP-ring, as follows from the following computations :

$$\theta A\,(\theta^{(\mathfrak{m})}u\theta^{(\mathfrak{m})}v) = \theta A\theta^{(\mathfrak{m})}(uv) = \theta^{(\mathfrak{m})}(Auv) = (\theta A\theta^{(\mathfrak{m})}u)\theta^{(\mathfrak{m})}v = \theta^{(\mathfrak{m})}u(\theta A\theta^{(\mathfrak{m})}v),$$
$$\theta 1\theta^{(\mathfrak{m})}u = \theta^{(\mathfrak{m})}(1u) = \theta^{(\mathfrak{m})}u.$$

We call $\theta^{(\mathfrak{m})}$ a specialization of the P-ring $\mathfrak{M}$ over θ.

It may happen that P is a part of the P-ring $\mathfrak{M}$ in the sense that $\mathfrak{M}$ possesses a unit element $1_{\mathfrak{M}}$ and that $A1_{\mathfrak{M}} = 0$, with $A \in P$, implies that $A = 0$. The correspondence $A \to A1_{\mathfrak{M}}\,(A \in P)$ then provides an isomorphism between P and a subring in the centre of $\mathfrak{M}$.

If this happens it cannot be inferred in general that θP is a part of $\theta^{(\mathfrak{m})}\mathfrak{M}$ in the same sense.

Example. Let F have characteristic not equal to 2, let

$$\mathfrak{M} = F \dotplus Fz_1 \dotplus Fz_2 \dotplus Fa_1 \dotplus Fa_2$$

with multiplication table

	z_1	z_2	a_1	a_2
z_1	0	0	z_2	0
z_2	0	0	0	0
a_1	z_2	0	0	z_2
a_2	0	0	$-z_2$	0

and let

$$P = F \dotplus Fz_1 \dotplus Fz_2,$$
$$\theta(\zeta) = \zeta \pmod{Fz_1} \text{ for } \zeta \in P,$$
$$P_\theta = Fz_1,$$
$$\theta^{(\mathfrak{m})}(\mathfrak{M}) = \mathfrak{M}/(Fz_1 + Fz_2).$$

Then $z_2\theta^{(\mathfrak{m})}1 = 0$ but $z_2\theta 1 \neq 0$.

We call θ an extendable homomorphism of P over F if θP is part of $\theta^{(\mathfrak{m})}\mathfrak{M}$ in the sense considered above.

If $\mathfrak{M}$ has a basis B over P, *i.e.*, if there is a set B of elements of $\mathfrak{M}$ such that for each element x of $\mathfrak{M}$ there is one and only one equation

$$x = \sum_{v \in B} A_v v$$

with all but a finite number of the coefficients vanishing and the non-vanishing ones belonging to P, then $\theta^{(\mathfrak{m})}\mathfrak{M}$ has the basis $\theta^{(\mathfrak{m})}B$ over θP. We prove this as follows.

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

Each element u of $\mathfrak{M}$ is equal to a linear combination of elements of B:

$$u = \sum_{v \in B} A_v v, \ (A_v \in P);$$

Hence

$$\theta^{(\mathfrak{m})} u = \sum_{v \in B} \theta A_v \theta^{(\mathfrak{m})} v.$$

On the other hand there is a θP-module $\overline{\mathfrak{M}}$ with basis elements $\bar{v} (v \in B)$. We define an operator homomorphism between $\mathfrak{M}$ and $\overline{\mathfrak{M}}$ by the formula

$$u = \sum_{v \in B} A_v v \to \bar{u} = \sum_{v \in B} \theta A_v \bar{v}.$$

Since the elements $\bar{u}$ satisfy the defining relations of $\theta^{(\mathfrak{m})}\mathfrak{M}$, it follows that there is an operator-homomorphism

$$\sum_{v \in B} \theta A_v \theta^{(\mathfrak{m})} v \to \sum_{v \in B} \theta A_v \bar{v}$$

between $\theta^{(\mathfrak{m})}\mathfrak{M}$ and $\overline{\mathfrak{M}}$, which proves that from $\sum_{v \in B} \theta A_v \theta^{(\mathfrak{m})} v = 0$ it follows that $\theta A_v = 0$ for all $v \in B$. The elements $\theta^{(\mathfrak{m})} v$ therefore form a basis of the θP-module $\theta^{(\mathfrak{m})}\mathfrak{M}$.

If $\mathfrak{M}$ is finitely-generated over P, then to each set of generators $u_1, u_2, \ldots, u_r$ of $\mathfrak{M}$ over P there belongs the P-module $R(u_1, u_2, \ldots, u_r; P)$ consisting of the set of all r-rows $(A_1, A_2, \ldots, A_r)$ $(A_i \in P, i = 1, 2, \ldots, r)$ which satisfy the relation $A_1 u_1 + A_2 u_2 + \ldots + A_r u_r = 0$. Using such a relation module $R(u_1, u_2, \ldots, u_r; P)$, one defines the elementary ideals

$$\mathfrak{E}_0(\mathfrak{M}; P), \ \mathfrak{E}_1(\mathfrak{M}; P), \ldots$$

as follows:

If $0 \leqslant i < r$, $\mathfrak{E}_i(\mathfrak{M}; P)$ is defined to be the ideal of P generated by the set of all $(r-i)$-rowed minors of all matrices consisting of $(r-i)$ rows of $R(u_1, u_2, \ldots, u_r; P)$; if $i \geqslant r$, $\mathfrak{E}_i$ is defined to be P. It follows that

$$\mathfrak{E}_0 \subseteq \mathfrak{E}_1 \subseteq \mathfrak{E}_2 \subseteq \cdots$$

and that the elementary ideals depend only on $\mathfrak{M}$ and not on the special set of generators $u_1, u_2, \ldots, u_r$ which we had to choose in order to be able to give a definition of $\mathfrak{E}_0, \mathfrak{E}_1, \mathfrak{E}_2, \ldots$. Hence we may write $\mathfrak{E}_i = \mathfrak{E}_i(\mathfrak{M}; P)$ without any ambiguity resulting from the particular choice of the system of generators $u_1, u_2, \ldots, u_r$ (see [9], p. 87).

$\mathfrak{E}_0$ is usually called the *order ideal* of $\mathfrak{M}$ over P; it always satisfies the relation $\mathfrak{E}_0 \mathfrak{M} = (0)$ (*cf.* [9], p. 89). The *rank of* $\mathfrak{M}$ *over* P is the number $\rho = \rho(\mathfrak{M}; P)$ defined by $\mathfrak{E}_0 = \mathfrak{E}_1 = \ldots = \mathfrak{E}_{\rho-1} = 0$, $\mathfrak{E}_\rho \neq 0$; if $\mathfrak{E}_0 \neq 0$, the rank is defined to be 0. If $\mathfrak{M}$ has a basis $u_1, u_2, \ldots, u_r$ over P, then $R(u_1, u_2, \ldots, u_r; P) = 0$ and hence $\mathfrak{E}_0 = \mathfrak{E}_1 = \ldots = \mathfrak{E}_{r-1} = 0$, $\mathfrak{E}_r = P$, so that the rank in this case is equal to the number of basis elements, *i.e.*, the dimension of the vector module $\mathfrak{M}$ over P.

If P is a field, then $\mathfrak{M}$ will have a basis over P and so the rank of $\mathfrak{M}$ over P is equal to the dimension of $\mathfrak{M}$ over P.

In the more general case of semiprimary rings we can state

THEOREM 2. *A module $\mathfrak{M}$ finitely-generated over a commutative semiprimary ring P with a unit element is a P-vector module of dimension ρ if and only if*

$$\mathfrak{E}_0(\mathfrak{M}; P) = \mathfrak{E}_1(\mathfrak{M}; P) = \ldots = \mathfrak{E}_{\rho-1}(\mathfrak{M}; P) = 0, \ \mathfrak{E}_\rho(\mathfrak{M}; P) = P. \tag{17}$$

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

Proof: A ring P is called semiprimary if the difference ring of P over its radical R (*i.e.*, its maximal two-sided nilideal) is semi-simple; *e.g.*, fields and direct sums of fields with finitely many summands are semiprimary.

We have already seen that (17) is a necessary condition for $\mathfrak{M}$ to be a vector module of dimension ρ over P. Let P be a commutative semiprimary ring with a unit element and let $\mathfrak{M}$ be a finitely-generated P-module for which (17) holds. We have to prove that $\mathfrak{M}$ has a basis of ρ elements over P.

Let $u_1, u_2, \dots, u_\sigma$ be a system of as few as possible generators of $\mathfrak{M}$ over P. In view of (17) it follows that $\sigma \geqslant \rho$.

Since the difference ring of P modulo R is semi-simple, and hence a principal ideal ring, we may transform the matrix of all relations between the given σ generators by suitable elementary transformations to its canonical form modulo R, thus showing that there is a certain set of σ generators $v_1, v_2, \dots, v_\sigma$ of $\mathfrak{M}$ over P between which there are relations of the form

$$\epsilon_i v_i + \sum_{k \neq i}^{\sigma} r_{ik} v_k = 0 \quad (i = 1, 2, \dots, \sigma),$$

with $r_{ik} \in R$, $\mathfrak{E}_{\sigma-j}(\mathfrak{M}; P) + R = P\epsilon_1\epsilon_2 \dots \epsilon_j + R$ (*cf.* [9], p. 92).

Now assume that $\sigma > \rho$; we then have

$$\mathfrak{E}_{\sigma-1}(\mathfrak{M}; P) = P \subseteq P\epsilon_1 + R.$$

Since P has a unit element it follows that $P\epsilon_1 = P$ and so $1 = \xi\epsilon_1$ for some $\xi \in P$. On multiplying the relation

$$\epsilon_1 v_1 + \sum_{k=2}^{\sigma} r_{ik} v_k = 0$$

by ξ, we obtain a relation by means of which v_1 may be eliminated from the set of generators, thus establishing the existence of a set of less than σ elements which generate $\mathfrak{M}$ over P. This contradicts the minimal property of σ; hence $\sigma \not> \rho$, and therefore $\sigma = \rho$. But from

$$\mathfrak{E}_{\rho-1}(\mathfrak{M}; P) = 0$$

it follows that $R(u_1, u_2, \dots, u_\rho;\ P) = 0$, *i.e.*, the elements $u_1, u_2, \dots, u_\rho$ constitute a basis of $\mathfrak{M}$ over P.

If P is an integral domain and the finitely-generated P-module $\mathfrak{M}$ is torsion free (*i.e.*, such that $\Lambda u = 0$, with $\Lambda \in P$ and $0 \neq u \in \mathfrak{M}$, implies that $\Lambda = 0$) then the rank of $\mathfrak{M}$ over P turns out to be equal to the dimension of the extended module $Q(P)\mathfrak{M}$ over the quotient field $Q(P)$. This follows from the obvious fact that any system of generators of $\mathfrak{M}$ over P is also a system of generators of $Q(P)\mathfrak{M}$ over $Q(P)$ and any relation between such generators with coefficients in $Q(P)$ is a multiple of a relation with coefficients in P. Hence

$$\mathfrak{E}_i(Q(P)\mathfrak{M};\ Q(P)) = Q(P)\mathfrak{E}_i(\mathfrak{M};\ P) = \begin{cases} Q(P) & \text{if } \mathfrak{E}_i(\mathfrak{M}; P) \neq 0, \\ 0 & \text{if } \mathfrak{E}_i(\mathfrak{M}; P) = 0. \end{cases}$$

For a homomorphism θ of P over F it follows that the set of all rows $(\theta A_1, \theta A_2, \dots, \theta A_r)$ with $(A_1, A_2, \dots, A_r) \in R(u_1, u_2, \dots, u_r;\ P)$ forms a θP-module $\theta R(u_1, u_2, \dots, u_r;\ P)$ contained in $R(\theta^{(\mathfrak{M})}u_1, \dots, \theta^{(\mathfrak{M})}u_r;\ \theta P)$. On the other hand let $\overline{\mathfrak{M}}$ be the difference module of

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

the θP-module of all r-rows with coefficients in θP, modulo $\theta R(u_1, u_2, \dots, u_r;\ P)$. Then $\overline{\mathfrak{M}}$ is a P-module and the mapping

$$\sum_{i=1}^{r} \theta A_i \theta^{(\mathfrak{m})} u_i \to (\theta A_1, \theta A_2, \dots, \theta A_r) + \theta R(u_1, \dots, u_r;\ P)/\theta R(u_1, u_2, \dots, u_r;\ P)$$

defines an operator-homomorphism between $\theta^{(\mathfrak{m})}\mathfrak{M}$ and $\overline{\mathfrak{M}}$. It therefore follows from

$$\sum_{i=1}^{r} \theta A_1 \theta^{(\mathfrak{m})} u_1 = 0$$

that

$$(\theta A_1, \theta A_2, \dots, \theta A_r) \in \theta R(u_1, u_2, \dots, u_r;\ P).$$

Hence

$$R(\theta^{(\mathfrak{m})} u_1, \theta^{(\mathfrak{m})} u_2, \dots, \theta^{(\mathfrak{m})} u_r;\ \theta P) = \theta R(u_1, u_2, \dots, u_r;\ P),$$
$$\mathfrak{E}_i(\theta^{(\mathfrak{m})}\mathfrak{M};\ \theta P) = \theta \mathfrak{E}_i(\mathfrak{M};\ P).$$

The order ideal of the specialised module $\theta^{(\mathfrak{m})}\mathfrak{M}$ is obtained by applying θ to the order ideal of $\mathfrak{M}$.

The rank of the specialised module $\theta^{(\mathfrak{m})}\mathfrak{M}$ is not less than the rank of $\mathfrak{M}$:

$$\rho(\theta^{(\mathfrak{m})}\mathfrak{M};\ \theta P) \geqslant \rho(\mathfrak{M};\ P).$$

We recall that a bilinear form on the P-module $\mathfrak{M}$ is defined to be any function $f(u, v)$ ranging over $\mathfrak{M}$ with values in P such that

$$\left.\begin{aligned} f(u_1 + u_2, v) &= f(u_1, v) + f(u_2, v), \\ f(u, v_1 + v_2) &= f(u, v_1) + f(u, v_2) \\ f(Au, v) &= f(u, Av) = Af(u, v) \end{aligned}\right\}, \quad (u, v, u_1, u_2, v_1, v_2 \in \mathfrak{M};\ A \in P).$$

It follows trivially that $f(0, v) = f(u, 0) = 0$. The bilinear form is called symmetric if

$$f(u, v) = f(v, u) \quad \text{for all} \quad u, v \in \mathfrak{M}.$$

The h-th *discriminant ideal* of f is defined to be the ideal $\mathfrak{D}_{\mathfrak{m}/P, h, f}$ of P generated by the set of all the determinants

$$|f(u_i, v_k)|, \quad (i, k = 1, 2, \dots, h;\ u_1, u_2, \dots, u_h, v_1, v_2, \dots, v_h \in \mathfrak{M}).$$

$\mathfrak{D}_{\mathfrak{m}/P, 0, f}$ is defined to be P.

It follows from the Laplace development of the determinants concerned that

$$\mathfrak{D}_{\mathfrak{m}/P, h_1+h_2, f} \subseteq \mathfrak{D}_{\mathfrak{m}/P, h_1, f} \cdot \mathfrak{D}_{\mathfrak{m}/P, h_2, f};$$

in particular

$$P = \mathfrak{D}_{\mathfrak{m}/P, 0, f} \supseteq \mathfrak{D}_{\mathfrak{m}/P, 1, f} \supseteq \mathfrak{D}_{\mathfrak{m}/P, 2, f} \supseteq \cdots.$$

If $\mathfrak{M}$ is generated by a subset B over P then we may restrict the elements $u_1, u_2, \dots, u_h$, $v_1, v_2, \dots, v_h$ occurring in the determinants generating $\mathfrak{D}_{\mathfrak{m}/P, h, f}$ to the elements of B. Hence, if B consists of a finite number of elements, say r elements, it follows that $\mathfrak{D}_{\mathfrak{m}/P, h, f}$ is finitely-generated over P and that

$$\mathfrak{D}_{\mathfrak{m}/P, r+1, f} = \mathfrak{D}_{\mathfrak{m}/P, r+2, f} = \dots = 0,$$

while $\mathfrak{D}_{\mathfrak{m}/P, r, f}$ is the principal ideal generated by $|f(b_i, b_k)|$, $b_1, b_2, \dots, b_r$ being r elements of B.

If θ is a homomorphism of the F-ring P onto the F-ring θP over F, then the bilinear form f on $\mathfrak{M}$ is mapped by θ onto the bilinear form θf on $\theta^{(\mathfrak{m})}\mathfrak{M}$ defined by

$$\theta f(\theta^{(\mathfrak{m})} u, \theta^{(\mathfrak{m})} v) = \theta f(u, v),$$

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

and accordingly for the discriminant ideals we have

$$\mathfrak{D}_{\theta(\mathfrak{m})\mathfrak{M}/\theta P,\, h,\, \theta f} = \theta \mathfrak{D}_{\mathfrak{M}/P,\, h,\, f}.$$

If $\mathfrak{M}$ is torsion free over P, then P must be an integral domain. $\mathfrak{M}$ can then be uniquely extended to a $Q(P)$-module generated by $\mathfrak{M}$ over $Q(P)$, which is bound to be $Q(P)\mathfrak{M}$. The bilinear form f can be uniquely extended to a bilinear form f on $Q(P)\mathfrak{M}$ according to the formula

$$f\left(\sum_{i=1}^{r} A_i u_i, \sum_{k=1}^{s} B_k v_k\right) = \sum_{i=1}^{r} \sum_{k=1}^{s} A_i B_k f(u_i, v_k),$$

for arbitrary $A_i, B_k \in Q(P)$ and $u_i, v_k \in \mathfrak{M}$.

The h-th discriminant ideal of f on $Q(P)\mathfrak{M}$ is generated by the h-th discriminant ideal of f on $\mathfrak{M}$:

$$\mathfrak{D}_{Q(P)\mathfrak{M}/Q(P),\, h, f} = Q(P)\mathfrak{D}_{\mathfrak{M}/P,\, h, f}.$$

If $\mathfrak{M}$ is finitely-generated over P, then it has a rank r which is equal to the dimension of $Q(P)\mathfrak{M}$ over $Q(P)$. It follows that

$$\mathfrak{D}_{\mathfrak{M}/P,\, r+1,\, f} = \mathfrak{D}_{\mathfrak{M}/P,\, r+2,\, f} = \ldots = 0.$$

The bilinear form f is called *degenerate* or *non-degenerate* according as $\mathfrak{D}_{\mathfrak{M}/P,\, r,\, f} = 0$ or $\mathfrak{D}_{\mathfrak{M}/P,\, r,\, f} \neq 0$. The bilinear form f is degenerate if and only if there are elements $u \neq 0$ in $\mathfrak{M}$ such that $f(u, v) = 0$ for all v in $\mathfrak{M}$; an equivalent condition is of course that there are elements $u \neq 0$ in $\mathfrak{M}$ such that $f(v, u) = 0$ for all v in $\mathfrak{M}$.

The ideal $\mathfrak{D}_{\mathfrak{M}/P,\, r,\, f}$ is called simply the discriminant ideal f defined on $\mathfrak{M}$ over F ; we denote the discriminant ideal by $\mathfrak{D}_{\mathfrak{M}/P,\, f}$. More generally, if $\mathfrak{M}$ is finitely-generated and of rank r over the commutative ring P with a unit element, then for any bilinear form f on $\mathfrak{M}$ over P, the ideal $\mathfrak{D}_{\mathfrak{M}/P,\, r,\, f}$ is called simply the discriminant ideal of f and is denoted by $\mathfrak{D}_{\mathfrak{M}/P,\, f}$.

§ 5. In this section we study the representations of a Lie-algebra L over a field F of characteristic p, a representation Δ of L being a single-valued mapping $a \to \Delta a$ of the elements a of L onto a set of matrices Δa of a certain degree f and with coefficients in F, such that

$$\begin{aligned} \Delta(a+b) &= \Delta a + \Delta b, \\ \Delta(\lambda a) &= \lambda \Delta a, \\ \Delta(a \circ b) &= \Delta a \,.\, \Delta b - \Delta b \,.\, \Delta a = \Delta a \circ \Delta b. \end{aligned}$$

The representation Δ of L induces a representation $\Delta^{(A(L))}$ of degree f of the enveloping algebra $A(L)$, mapping each element a of L onto Δa and the unit element of $A(L)$ onto the identity matrix of degree f ; hence every proper representation of finite degree over F of $A(L)$ induces a representation of L, by which it is itself induced as described above.

For every proper representation Δ of $A(L)$ by matrices of finite degree over F we obtain a specialisation θ of the center $\mathfrak{Z}$ of $A(L)$ by an algebra $\Delta(\mathfrak{Z})$ over F. The representation Δ appears as an extension of the specialisation θ to a specialisation of $A(L)$ onto the algebra $\Delta A(L)$ over F. Hence every representation of finite degree over F of $A(L)$ may be obtained in the following way.

(1) Find extendable specialisations θ of $\mathfrak{Z}$ by an algebra $\theta\mathfrak{Z}$ over F such that $\theta\mathfrak{Z}$ can be considered as part of the center of $\theta^{(A(L))}A(L)$. The latter also will be an algebra over F.

(2) Form all proper representations of finite degree over F of the algebra $\theta^{(A(L))}A(L)$ obtained under (1). These induce proper representations of finite degree over F of $A(L)$ and hence representations of L.

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

An indecomposable proper representation Δ of $A(L)$ of finite degree over F is, according to the theory, characterised by the fact that the ring of all matrices commuting with Δ is primary. Since $\Delta\mathfrak{Z}$ is part of this ring, $\Delta\mathfrak{Z}$ itself will be a primary ring. Accordingly, in the construction just described, it is only necessary to consider specialisations of $\mathfrak{Z}$ by primary algebras over F.

It is now necessary to take up the question whether every specialisation of $\mathfrak{Z}$ by a primary ring over F is extendable to a specialisation of $A(L)$ over F and, if this is not the case, whether there is a criterion for extendability.

An irreducible representation Δ of $A(L)$ of finite degree over F, which is not the null representation, is certainly proper, and for it the set of all matrices commuting with Δ forms a division algebra over F. Consequently $\Delta\mathfrak{Z}$ is an extension of F.

Let us now consider a specialisation θ over F of $\mathfrak{Z}$ onto an extension $\theta\mathfrak{Z}$ of F. Since $\mathfrak{Z}$ is finitely-generated over $\mathfrak{o}$, it follows that $\Delta\mathfrak{Z}$ is finitely-generated over $\Delta\mathfrak{o}$, an integral domain contained in $\Delta\mathfrak{Z}$.

Quite generally we have

THEOREM 3. *If a ring $\mathfrak{S}$ with a unit element coincides with its quotient ring and if $\mathfrak{S}$ is finitely generated over an integral domain $\mathfrak{o}$, then $\mathfrak{o}$ is a field and consequently $\mathfrak{S}$ is an algebra over $\mathfrak{o}$.*

Proof: We have

$$\mathfrak{S} = \sum_{i=1}^{s} \mathfrak{o}\, a_i$$

with a finite number of generating elements $1 = a_1, a_2, \ldots, a_s$ of $\mathfrak{S}$ over $\mathfrak{o}$. Since $\mathfrak{o}$ is contained in the center of $\mathfrak{S}$, it follows that $Q(\mathfrak{o}) \subseteq Q(\mathfrak{S}) = \mathfrak{S}$. In fact, $Q(\mathfrak{o})$ even belongs to the center of $\mathfrak{S}$. Since $\mathfrak{S} = \sum_{i=1}^{s} Q(\mathfrak{o}) a_i$ and since $Q(\mathfrak{o})$, as the quotient ring of an integral domain, is a field, it follows that $\mathfrak{S}$ is an algebra over $Q(\mathfrak{o})$. It is possible to choose the basis $1 = a_1, a_2, \ldots, a_s$ of $\mathfrak{S}$ over $\mathfrak{o}$ so that $1 = a_1, a_2, \ldots, a_r$ is a basis of $\mathfrak{S}$ over $Q(\mathfrak{o})$; then

$$a_i = \sum_{k=1}^{r} \frac{\lambda_{ik}}{\mu_{ik}} a_k, \text{ with } \lambda_{ik}, \mu_{ik} \in \mathfrak{o}, \quad \text{for } i = r+1, r+2, \ldots, s.$$

Introducing

$$0 \neq \mu = \Pi_{i=r+1}^{s} \Pi_{k=1}^{r} \mu_{ik},$$

we see that all the elements $a_1, a_2, \ldots, a_s$ are contained in the $\mathfrak{o}$-module with basis $\frac{a_1}{\mu}, \frac{a_2}{\mu}, \ldots, \frac{a_r}{\mu}$. It follows that $\mathfrak{S}$, *i.e.*, the set of all linear combinations of $a_1, a_2, \ldots, a_s$ over $\mathfrak{o}$, is contained in this $\mathfrak{o}$-module. For an arbitrary element Λ of $Q(\mathfrak{o})$, we find that

$$\begin{aligned} \frac{\Lambda}{\mu} &= \Lambda \cdot \frac{1}{\mu} + 0 \cdot \frac{a_2}{\mu} + \ldots \quad + 0 \frac{a_r}{\mu} \\ &= \lambda_1 \cdot \frac{a_1}{\mu} + \lambda_2 \frac{a_2}{\mu} + \ldots \quad + \lambda_r \frac{a_r}{\mu}, \end{aligned}$$

with coefficients $\lambda_1, \lambda_2, \ldots, \lambda_r$ in $\mathfrak{o}$. Since the elements $\frac{1}{\mu} = \frac{a_1}{\mu}, \frac{a_2}{\mu}, \ldots, \frac{a_r}{\mu}$ form a basis of $\mathfrak{S}$ over $Q(\mathfrak{o})$ it follows that $\Lambda = \lambda_1, \lambda_2 = \lambda_3 = \ldots = \lambda_r = 0$, and hence Λ belongs to $\mathfrak{o}$. Hence $Q(\mathfrak{o}) = \mathfrak{o}$, *i.e.*, $\mathfrak{o}$ is a field.

For the special case under consideration, we conclude that $\theta\mathfrak{o}$ is an extension of F. In

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

other words, every specialisation θ of $\mathfrak{Z}$ onto an extension $\theta\mathfrak{Z}$ of F over F induces a specialisation ϕ of $\mathfrak{o}$ onto an extension $\phi\mathfrak{o} = \theta\mathfrak{o}$ of F over F.

Since the rank of $A(L)$ over $\mathfrak{Z}$ is p^{2m}, it follows from the theory developed in § 4 that the rank of $\theta^{(A(L))}A(L)$ over $\theta\mathfrak{Z}$ must be at least p^{2m}. Consequently we have $\theta^{(A(L))}A(L) \neq 0$, $\theta^{(A(L))}1 \neq 0$. Since there is an operator-homomorphism between $\theta\mathfrak{Z}$ and $\theta^{(A(L))}\mathfrak{Z} \neq 0$ and since $\theta\mathfrak{Z}$ is a field, we have in fact an operator-isomorphism ; *i.e.*, $\theta^{(A(L))}$ extends to θ.

We know that $A(L)$ is finitely-generated over $\mathfrak{Z}$, say

$$A(L) = \sum_{i=1}^{s} \mathfrak{Z} a_i$$

It follows that

$$\theta^{(A(L))}A(L) = \sum_{i=1}^{s} \theta\mathfrak{Z} \cdot \theta^{(A(L))}a_i$$

and that θ maps the general element

$$a = \sum_{i=1}^{s} x_i a_i$$

of $A(L)$ over $\mathfrak{Z}$ onto the general element

$$\theta a = \sum_{i=1}^{s} \theta x_i \cdot \theta^{(A(L))}a_i$$

of $\theta^{(A(L))}A(L)$ over $\theta\mathfrak{Z}$.

Since $\mathfrak{Z}$ is the center of an integrally closed ring, it is itself integrally closed, as we have seen before. Since the quotient ring of $A(L)$ is centrally simple of dimension p^{2m} over $Q(\mathfrak{Z})$, it follows that there is a minimal polynomial

$$P(t) = t^{p^m} + \sum_{i=1}^{p^m} (-1)^i P_i(x_1, x_2, \ldots, x_s) t^{p^m - i}$$

of the general element a over $\mathfrak{Z}$, where $P_i(x_1, x_2, \ldots, x_s)$ is a homogeneous polynomial of degree i contained in $\mathfrak{Z}[x_1, x_2, \ldots, x_n]$ (*cf.* Deuring, *Algebren*, p. 50). The homomorphism θ maps $P(t)$ onto the polynomial

$$\theta P(t) = t^{p^m} + \sum_{i=1}^{p^m} (-1)^i \theta P_i(x_1, x_2, \ldots, x_s) t^{p^m - i}.$$

From $P(a) = 0$ it follows that $P(\theta a) = 0$.

Hence θP is divisible by the minimal polynomial of θa over $\theta\mathfrak{Z}$.

The degree of any minimal polynomial of $\theta^{(A(L))}A(L)$ over $\theta\mathfrak{Z}$ is consequently at most p^m.

The discriminant ideal of $A(L)$ over $\mathfrak{Z}$ can be defined in the usual fashion (*cf.* Deuring, *Algebren*, p. 87). It does not vanish, since K is centrally simple, and so separable, over the quotient field of $\mathfrak{Z}$. It is known that the degree f of the minimal equation of a separable algebra $\mathfrak{S}$ over a field F satisfies the inequality $f^2 \geqslant \dim_F \mathfrak{S}$, equality holding if and only if $\mathfrak{S}$ is centrally simple over F. From these and other known results, we deduce

THEOREM 4. *Any specialisation θ over F of the center $\mathfrak{Z}$ of $A(L)$ onto an extension $\theta\mathfrak{Z}$ of F can be extended to a specialisation $\theta^{(A(L))}$ of $A(L)$ over F onto an algebra $\theta^{(A(L))}A(L)$ of dimension not less than p^{2m} over $\theta\mathfrak{Z}$. There is a general element of $A(L)$ over $\mathfrak{Z}$ and it is mapped by θ onto a multiple of the minimal polynomial of the corresponding general element of $\theta^{(A(L))}A(L)$ over $\theta\mathfrak{Z}$. The algebra $\theta^{(A(L))}A(L)$ is separable over $\theta\mathfrak{Z}$ if and only if it is centrally simple of dimension*

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

p^{2m} over $\theta\mathfrak{Z}$. In this case, θ maps any minimal polynomial of $A(L)$ over $\mathfrak{Z}$ onto a minimal polynomial of $\theta^{(A(L))}A(L)$ over $\theta\mathfrak{Z}$. The discriminant ideal of $A(L)$ over $\mathfrak{Z}$ does not vanish.

Furthermore we have

THEOREM 5. *Let θ be a specialisation over F of $\mathfrak{Z}$ onto an extension $\theta\mathfrak{Z}$ of F. Then*

$$\theta(\mathfrak{D}_{A(L)/\mathfrak{Z}} \neq 0,$$

where $\mathfrak{D}_{A(L)/\mathfrak{Z}}$ is the discriminant ideal of $A(L)$ over $\mathfrak{Z}$, if and only if $\theta^{(A(L))}A(L)$ is centrally simple of dimension p^{2m} over $\theta\mathfrak{Z}$.

Proof :* (1) Let $\theta^{(A(L))}A(L)$ be centrally simple over $\theta\mathfrak{Z}$. Then, according to theorem 4, the dimension of $\theta^{(A(L))}A(L)$ over $\theta\mathfrak{Z}$ is p^{2m} and any minimal polynomial of $A(L)$ over $\mathfrak{Z}$ is mapped onto a minimal polynomial of $\theta^{(A(L))}A(L)$ over $\theta\mathfrak{Z}$. The second highest coefficient of the minimal polynomial is the linear form which is used to define the discriminant ideal. It follows that

$$\theta\mathfrak{D}_{A(L)/\mathfrak{Z}} = \mathfrak{D}_{\theta^{(A(L))}A(L)/\theta\mathfrak{Z}},$$

and since $\theta^{(A(L))}A(L)$ is separable over $\theta\mathfrak{Z}$, it follows that $\mathfrak{D}_{\theta^{(A(L))}A(L)/\theta\mathfrak{Z}} \neq 0$.

Conversely, let $\theta\mathfrak{D}_{A(L)/\mathfrak{Z}} \neq 0$. The discriminant ideal $\mathfrak{D}_{A(L)/\mathfrak{Z}}$ is obtained as the p^{2m}-th discriminant ideal of a bilinear form $f(a, b) = \operatorname{tr}(ab)$ on $A(L)$ over $\mathfrak{Z}$, where $\operatorname{tr} x$ is defined to be the trace of x for an absolutely irreducible representation of $Q(A(L))$ over $Q(\mathfrak{Z})$. Hence

$$f(a, b) = f(b, a), \quad f(ab, c) = f(a, bc),$$

and, for characteristic $p > 0$,

$$f(a^p, b^p) = \{f(a, b)\}^p.$$

Furthermore

$$\mathfrak{D}_{A(L)/\mathfrak{Z}} = \mathfrak{D}_{p^{2m}, f, \mathfrak{Z}},$$
$$0 = \mathfrak{D}_{p^{2m+1}, f, \mathfrak{Z}}.$$

By application of θ it follows that

$$\mathfrak{D}_{p^{2m}, \theta f, \theta\mathfrak{Z}} = \theta\mathfrak{D}_{p^{2m}, f, \mathfrak{Z}} = \theta\mathfrak{D}_{A(L)/\mathfrak{Z}} \neq 0,$$
$$\mathfrak{D}_{p^{2m+1}, \theta f, \theta\mathfrak{Z}} = \theta\mathfrak{D}_{p^{2m+1}, f, \mathfrak{Z}} = 0.$$
$$\theta f(u, v) = \theta f(v, u),$$
$$\theta f(u, vw) = \theta f(uv, w),$$
$$\theta f(u^p, v^p) = \{\theta f(u, v)\}^p,$$

for u, v, w contained in

$$\mathfrak{S} = \theta^{(A(L))}A(L).$$

It follows that the set of all the elements u of $\mathfrak{S}$ which satisfy the condition

$$f(u, v) = 0 \text{ for all } v \in \mathfrak{S}$$

forms a two-sided ideal $\mathfrak{A}$ of $\mathfrak{S}$ such that $\dim_{\theta\mathfrak{Z}}(\mathfrak{S}/\mathfrak{A}) = p^{2m}$, and θf induces a non-degenerate symmetric bilinear form g on $\mathfrak{S}/\mathfrak{A}$ over $\theta\mathfrak{Z}$ satisfying $g(\hat{u}^p, \hat{v}^p) = \{g(\hat{u}, \hat{v})\}^p$ and hence $g(\hat{u}^{p^j}, \hat{v}^{p^j}) = \{g(\hat{u}, \hat{v})\}^{p^j}$, for all $\hat{u}, \hat{v}$ contained in $\mathfrak{S}/\mathfrak{A}$. Now for any element $\hat{x}$ of the radical of $\mathfrak{S}/\mathfrak{A}$, $\hat{x}^{p^j} = 0$ for some j. Hence $\{g(\hat{x}, \hat{v})\}^{p^j} = g(\hat{x}^{p^j}, \hat{v}^{p^j}) = 0$ and therefore $g(\hat{x}, \hat{v}) = 0$ for all $\hat{v}$ in $\mathfrak{S}/\mathfrak{A}$; hence $\hat{x} = 0$. Since this argument still holds after any extension of the ground field $\theta\mathfrak{Z}$ of $\mathfrak{S}/\mathfrak{A}$, it follows that $\mathfrak{S}/\mathfrak{A}$ is separable over $\theta\mathfrak{Z}$. From theorem 4 it follows that the degree of a minimal polynomial of $\mathfrak{S}$ over $\theta\mathfrak{Z}$ is not greater than p^m. This holds *a fortiori* for $\mathfrak{S}/\mathfrak{A}$. Since $\mathfrak{S}/\mathfrak{A}$ is separable and of dimension p^{2m} over $\theta\mathfrak{Z}$, it follows that $\mathfrak{S}/\mathfrak{A}$ is centrally simple over $\theta\mathfrak{Z}$ and hence that the degree of $\mathfrak{S}/\mathfrak{A}$ over $\theta\mathfrak{Z}$ is equal to p^m. But the degree of

* For a simplification of this proof and for other valuable advice, I am indebted to W. E. Jenner.

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

the minimal polynomial of an algebra $\mathfrak{S}$ with a unit element over the ground field is at least equal to the sum of the degrees of the minimal polynomials of the simple components of $\mathfrak{S}$ modulo its radical, and is certainly greater than this sum if the radical of $\mathfrak{S}$ is not zero. Since we have already proved that there is a simple component of $\mathfrak{S}$ over its radical with minimal polynomial over $\theta\mathfrak{Z}$ of degree p^m, it follows that the degree of the minimal polynomial of $\mathfrak{S}$ over $\theta\mathfrak{Z}$ is at least p^m and is equal to p^m only if $\mathfrak{S}$ is simple. But, according to theorem 4, the degree of the minimal polynomial of $\mathfrak{S}$ over $\theta\mathfrak{Z}$ is not greater than p^m. Hence the degree is p^m and $\mathfrak{S}$ is simple; *i.e.*, $\mathfrak{S} \simeq \mathfrak{S}/\mathfrak{A}$, *i.e.*, $\mathfrak{A} = 0$. Hence $\theta^{(\Delta(L))}A(L)$ is centrally simple of dimension p^{2m} over $\theta\mathfrak{Z}$; q.e.d.

Theorems 4 and 5 find convenient expression in

THEOREM 6. *The degree of any absolutely irreducible representation Δ of the Lie-algebra L over F is at most p^m. It is equal to p^m if and only if Δ does not map the discriminant ideal of $A(L)$ over $\mathfrak{Z}$ onto zero.*

The representation Δ is given as the representation of the Lie-algebra $(L \times \Phi)_F = L_\Phi$ over a suitable extension Φ of F, such that the proper representation of $A(L_\Phi) = (A(L) \times \Phi)_F$ over Φ induced by Δ, which may also be denoted by Δ, maps $A(L_\Phi)$ onto the full ring of matrices of degree f over Φ. The representation Δ induces a specialisation θ of $\mathfrak{Z}_\Phi = (\mathfrak{Z} \times \Phi)_F$ onto a set of matrices which commute with Δ. According to Schur's Lemma, Δ maps $\mathfrak{Z}_\Phi$ onto ΦI_f. We consider the specialisation θ of $\mathfrak{Z}_\phi$ over Φ defined by

$$\theta(\zeta) I_f = \Delta(\zeta) \qquad (\zeta \in \mathfrak{Z}_\Phi).$$

There is an operator-homomorphism

$$\theta^{(\Delta(L_\Phi))} u \to \Delta u$$

of $\theta^{(\Delta(L_\Phi))}A(L_\Phi)$ over $\theta\mathfrak{Z}_\Phi$ onto $\Delta A(L_\Phi)$. In other words, Δ induces an absolutely irreducible representation of degree f of $\theta^{(\Delta(L_\Phi))}A(L_\Phi)$ over $\theta\mathfrak{Z}_\Phi$; *i.e.*, there is a difference algebra of the algebra $\theta^{(\Delta(L_\Phi))}A(L_\Phi)$ over $\theta\mathfrak{Z}_\Phi$ isomorphic to the full matrix algebra of degree f over $\theta\mathfrak{Z}_\Phi$. According to theorem 4, the degree of a minimal polynomial is not greater than p^m, and hence $f \leqslant p^m$. If the degree is equal to p^m, then the argument given in the proof of theorem 5 shows that the algebra $\theta^{(\Delta(L_\Phi))}A(L_\Phi)$ is itself isomorphic to the full matrix algebra of degree p^m over $\mathfrak{Z}_\Phi$. Furthermore it follows from theorem 5 that $f = p^m$ if and only if

$$\theta \mathfrak{D}_{A(L_\Phi)/\mathfrak{Z}_\Phi} \neq 0.$$

Since $\mathfrak{D}_{A(L_\Phi)/\mathfrak{Z}_\Phi} = \Phi \mathfrak{D}_{\mathfrak{Z}(L)/A}$, the previous inequality is equivalent to the inequality $\mathfrak{D}_{A(L)/\mathfrak{Z}} \neq 0$; q.e.d.

Though it is probably not true that the image of the minimal polynomial P belonging to the general element a of $A(L)$ over $\mathfrak{Z}$ under any specialisation θ of $\mathfrak{Z}$ over F onto an extension of F will be a minimal polynomial again, it can be proved that θP is the characteristic polynomial of θa for a suitable representation of $\theta^{(\Delta(L))}A(L)$ over $\theta\mathfrak{Z}$.

From theorem 2 and the general theory developed in § 4, we derive

THEOREM 7. *The specialisation θ of $\mathfrak{Z}$ onto a semiprimary ring over F is extendable to a specialisation $\theta^{(\Delta(L))}$ of $A(L)$ onto a $\theta\mathfrak{Z}$-ring with exactly p^{2m} basis elements over $\theta\mathfrak{Z}$ if and only if*

$$\theta \mathfrak{E}_{p^{2m},\, A(L)/\mathfrak{Z}} = \theta\mathfrak{Z},$$

in other words, if and only if

$$\mathfrak{Z} = \mathfrak{E}_{p^{2m},\, A(L)/\mathfrak{Z}} + \mathfrak{Z}_\theta,$$

where $\mathfrak{Z}_\theta$ denotes the kernel of θ.

We have seen that for any indecomposable representation Δ of L over F, the algebra $\Delta\mathfrak{Z}$ is primary. Consequently all irreducible constituents of Δ will lead to specialisations of $\mathfrak{Z}$ with the same kernel, *i.e.*, to (*weakly*) *equivalent specialisations*. On the other hand, corresponding to any specialisation θ of $\mathfrak{Z}$ by a finite extension of F, there are indecomposable representations of L which are not irreducible, such that all the irreducible components lead to specialisations of $\mathfrak{Z}$ which are weakly equivalent to θ. In order to prove this we use a method of W. Krull.

Assume that there is an ideal $\mathfrak{a} \neq 0$ of $\mathfrak{Z}$ such that $\mathfrak{a}A(L) = \mathfrak{a}^2 A(L)$. We shall show that $\mathfrak{a} = \mathfrak{Z}$

In fact, since $\mathfrak{Z}$ satisfies the maximal condition and $A(L)$ is finitely-generated over $\mathfrak{Z}$, it follows that $\mathfrak{a}A(L)$ is finitely-generated over $\mathfrak{Z}$, say

$$\mathfrak{a}A(L) = \sum_{i=1}^{q} b_i \mathfrak{Z}.$$

Since $\mathfrak{a}^2 A(L) = \mathfrak{a}A(L)$, there must be equations

$$b_k = \sum_{i=1}^{q} \alpha_{ik} b_i \quad (k = 1, 2, \ldots, q),$$

with α_{ik} in $\mathfrak{a}$; hence

$$\sum_{i=1}^{q} (\delta_{ik} - \alpha_{ik}) b_i = 0 \quad (k = 1, 2, \ldots, q),$$

from which it follows that

$$\text{Det}\,(I_q - (\alpha_{ik})) = 0,$$

since not all the b_k vanish and $A(L)$ has no divisors of zero. Hence

$$1 = \text{Det}\, I_q \equiv 0 \pmod{\mathfrak{a}},$$

i.e., $1 \in \mathfrak{a}$ and so $\mathfrak{a} = \mathfrak{Z}$.

If, for an ideal $\mathfrak{a}$ of $\mathfrak{Z}$, $\mathfrak{a}A(L) = A(L)$, then $\mathfrak{a} \neq 0$ and $\mathfrak{a}^2 A(L) = \mathfrak{a}A(L)$; hence $\mathfrak{a} = \mathfrak{Z}$.

It follows that any proper ideal of $\mathfrak{Z}$ also generates a proper ideal of $A(L)$; *e.g.*, the kernel $\mathfrak{Z}_\theta$ of θ generates a proper ideal of $A(L)$.

Since the image $\theta\mathfrak{Z}$ is of finite dimension over F but $\mathfrak{Z}$ is not, it follows that

$$0 \subset \mathfrak{Z}_\theta \subset \mathfrak{Z}.$$

Hence the two-sided ideal $\mathfrak{U} = \mathfrak{Z}_\theta A(L)$ satisfies

$$0 \subset \mathfrak{U} \subset A(L).$$

Now for $j = 1, 2, \ldots, \mathfrak{Z}_\theta^j \neq 0$ and $\mathfrak{U}^j = (\mathfrak{Z}_\theta A(L))^j = \mathfrak{Z}_\theta^j (A(L))^j = \mathfrak{Z}_\theta^j A(L)$. Since $A(L)$ has no divisors of zero it follows that $(0) \subset \mathfrak{U}^j \subseteq \mathfrak{U} \subset A(L)$ and hence, as we have already seen, that $(\mathfrak{U}^j)^2 \subset \mathfrak{U}^j$. If $\mathfrak{U}^j$ were equal to $\mathfrak{U}^{j+1}$, it would follow that $\mathfrak{U}\mathfrak{U}^j = \mathfrak{U}\mathfrak{U}^{j+1}$, *i.e.*, that $\mathfrak{U}^{j+1} = \mathfrak{U}^{j+2}$, and therefore that $\mathfrak{U}^j = \mathfrak{U}^{j+2}$ and, by induction, that

$$\mathfrak{U}^j = \mathfrak{U}^{j+1} = \mathfrak{U}^{j+2} = \ldots ;$$

and hence that $\mathfrak{U}^j = \mathfrak{U}^{j+j} = \mathfrak{U}^{2j} = (\mathfrak{U}^j)^2$, contrary to our previous result. Hence

$$\mathfrak{U}^{j+1} \subset \mathfrak{U}^j.$$

Hence we have the infinite chain

$$A(L) \supset \mathfrak{U} \supset \mathfrak{U}^2 \supset \mathfrak{U}^3 \supset \ldots .$$

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

For $j>1$, the algebra* $\mathfrak{S}=A(L)-\mathfrak{Z}_\theta^j A(L)$ over F contains in its radical the two-sided ideal $\mathfrak{B}=\mathfrak{Z}_\theta A(L)-\mathfrak{Z}_\theta^j A(L)\neq 0$, for which $\mathfrak{S}-\mathfrak{B}\simeq \theta^{(A(L))}A(L)$. It follows that $\mathfrak{S}$ admits only proper representations such that all their irreducible constituents induce specialisations of $\mathfrak{Z}$ over F which are weakly equivalent to θ. But the regular representation of $\mathfrak{S}$ over F induces a representation which is not fully reducible. This is because the radical of $\mathfrak{S}$ does not vanish. Hence we have

THEOREM 8. *Every representation of finite degree over F of the Lie-algebra L decomposes into a sum of representations leading to specialisations of $\mathfrak{Z}$ by primary algebras over F. For any specialisation of $\mathfrak{Z}$ by a finite extension of F there are indecomposable representations of L of finite degree over F which are not fully reducible and such that each irreducible constituent leads to specialisations of $\mathfrak{Z}$ which are weakly equivalent to θ.*

Example 1. Let L be a nilpotent Lie-algebra. We know from [6] that for every absolutely irreducible representation Δ of L each matrix Δa has only one characteristic root $\lambda(a)$ and that any two absolutely irreducible representations with the same distribution of characteristic roots are equivalent. Furthermore, for any element a of L, $a^{p^j}=0$ if p^j is a power of p greater than the class of L. Hence a^{p^j} belongs to the ring $\mathfrak{o}$ previously constructed. It follows that for every specialisation ϕ over F of $\mathfrak{o}$ onto F the algebra $\phi^{(A(L))}A(L)$ over $\phi\mathfrak{o}$ has only one absolutely irreducible representation, up to equivalence. Since $\dim_F \phi^{(A(L))}A(L)=p^{(A(L);\,\mathfrak{o})}=p^l$, we find, by reduction of the regular representation of $\phi^{(A(L))}A(L)$ over F, which is of degree p^l, that every absolutely irreducible representation has a power of p for its degree.

This is one of the results proved in another way in [3] and in [4].

We may consider $Q(\mathfrak{o})L$ as a nilpotent Lie-algebra over $Q(\mathfrak{o})$. In the regular representation R of $Q(A(L))$ over $Q(\mathfrak{o})$, every element

$$a=\sum \xi_i a_i$$

of $Q(\mathfrak{o})L$ has only one characteristic root $\Lambda(a)$, namely the one defined by the equation

$$\Lambda(a)^{p^j}=\left(\sum \xi_i a_i\right)^{p^j}\in Q(\mathfrak{o}).$$

Since $Q(\mathfrak{o})L$ generates $Q(A(L))$ over $Q(\mathfrak{o})$ it follows that all absolutely irreducible constituents of R are equivalent. We find

THEOREM 9. *If L is a nilpotent Lie-algebra over F, then $Q(\mathfrak{Z})$ is a pure inseparable extension of $Q(\mathfrak{o})$.*

It is not always true for nilpotent Lie-algebras that $Q(\mathfrak{Z})=Q(\mathfrak{o})$, or what amounts to the same thing, that $\mathfrak{Z}=\mathfrak{o}$.

* We observe that $\mathfrak{Z}_\theta^j A(L)=\mathfrak{U}^j$, where $\mathfrak{U}=\mathfrak{Z}_\theta A(L)$, is a two-sided ideal of $A(L)$ for which

$$\dim_F[A(L)-\mathfrak{U}]<\infty.$$

We have to prove that $\dim_F[A(L)-\mathfrak{U}^j]<\infty$. This follows from the general result that if for two ideals $\mathfrak{X}$, $\mathfrak{Y}$ of an F-ring $\mathfrak{P}$ there are equations

$$\mathfrak{X}=\sum_{i=1}^q x_i\mathfrak{P},\quad \mathfrak{Y}=\sum_{j=1}^r \mathfrak{P}y_j,\quad \mathfrak{P}=\mathfrak{X}+\sum_{k=1}^s Fa_k=\mathfrak{Y}+\sum_{l=1}^t Fb_l,$$

then

$$\mathfrak{P}\mathfrak{P}=\mathfrak{X}\mathfrak{Y}+\sum_{k=1}^s\sum_{l=1}^t Fa_kb_l+\sum_{k=1}^s\sum_{j=1}^r Fa_ky_j+\sum_{i=1}^q\sum_{l=1}^t Fx_iy_l,$$

and from the fact that every ideal of $A(L)$ is finitely-generated over $\mathfrak{Z}$.

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

Example. Let L have four basis elements e_1, e_2, e_3, e_4 over a field of characteristic $p>2$, and multiplication table $e_i \circ e_1 = 0$, $e_4 \circ e_2 = e_3 \circ e_2 = e_1$, $e_4 \circ e_3 = e_2$. We see immediately that e_1 e_2^p, e_3^p, e_4^p belong to $\mathfrak{o} \cap L^*$, that e_1 is the basis of the center of L and that

$$L^* = Fe_2 \dotplus Fe_3 \dotplus Fe_4 \dotplus [\langle e_1, e_2^p, e_3^p, e_4^p \rangle_F \cap L^*].$$

Since no non-trivial linear combination of e_2, e_3, e_4 is in the center of L, it follows that

$$\mathfrak{o} \cap L^* = Fe_1 \dotplus \sum_{i=1}^{4} \sum_{j=1}^{\infty} Fe_i^{p^j},$$

$$\mathfrak{o} = \langle e_1, e_2^p, e_3^p, e_4^p \rangle_F,$$

$$l = \dim_F (L^* - \mathfrak{o} \cap L^*) = 3, \quad \dim_{\mathfrak{o}} A(L) = p^3, \quad 1 < \dim_{Q(\mathfrak{Z})} Q(A(L)) = p^{2m}/p^3,$$
$$\dim_{Q(\mathfrak{Z})} Q(A(L)) = p^2 < p^3, \quad m = 1, \quad \mathfrak{o} \subset \mathfrak{Z}.$$

It is an interesting problem to find out whether for all non-nilpotent Lie-algebras it is the case that $Q(\mathfrak{Z})$ is not pure inseparable over $Q(\mathfrak{o})$.

Example 2. The simple Lie-rings of Witt (*cf.* [2]) are obtained by taking a finite submodule $\mathfrak{M}$ of a field F of prime characteristic p and forming the Lie-algebra $L(\mathfrak{M}, F)$ with basis elements $e_\alpha, e_\beta, e_\gamma, \ldots$ over F, where $\alpha, \beta, \gamma, \ldots$ range over $\mathfrak{M}$ and the multiplication rule is

$$e_\alpha \circ e_\beta = (\beta - \alpha) e_{\alpha+\beta}.$$

We deal only with the case in which $\mathfrak{M}$ is the prime field of F and $p>2$. We note that for $\alpha \neq 0$, Lie-multiplication by e_α applied p times annihilates each element, and that Lie-multiplication by e_0 applied p times has the same effect as when applied once. It follows that the elements

$$\zeta_0 = e_0^p - e_0, \quad \zeta_\alpha = e_\alpha^p, \quad (\alpha \neq 0),$$

belong to $\mathfrak{o} \cap L^*$; and clearly they are linearly independent over F. They generate the p-invariant F-Lie-ring

$$\mathfrak{M} = \sum_{i=0}^{p-1} \sum_{j=0}^{\infty} \zeta_i^{p^j} F$$

contained in $\mathfrak{Z} \cap L^*$, and the F-subring $\mathfrak{o}_1 = \langle \zeta_0, \zeta_1, \ldots, \zeta_{p-1} \rangle_F$ of $\mathfrak{o}$. Since $\mathfrak{o}_1 \cap L^* \supseteq L^p + L$, it follows that $L^* = (L + \mathfrak{o}_1) \cap L^*$ and therefore that $\mathfrak{o} \cap L^* = (\mathfrak{o} \cap L) + (\mathfrak{o}_1 \cap L^*)$. Since L has center (0) it follows that $\mathfrak{o} \cap L = (0)$, $\mathfrak{o} \cap L^* = \mathfrak{o}_1 \cap L^*$, $\mathfrak{o} = \langle \mathfrak{o} \cap L^* \rangle_F = \langle \mathfrak{o}_1 \cap L^* \rangle_F = \mathfrak{o}_1$. We note that $\dim_F (L^* - \mathfrak{M}) = p$, and so $A(L)$ has p^p basis elements over $\mathfrak{o}$ namely, the p^p elements

$$e_0^{\alpha_0}, e_1^{\alpha_1}, \ldots, e_{p-1}^{\alpha_{p-1}} \quad (0 \leqslant \alpha_i < p).$$

It follows that $\dim_{\mathfrak{Z}} A(L)$ divides p^p. Since $\dim_{\mathfrak{Z}} A(L) = p^{2m}$ and $p>2$, it follows that $\dim_{\mathfrak{Z}} A(L) < p^p$; hence $\mathfrak{o} \subset \mathfrak{Z}$.

Choose the basis of L over F in the order $e_0, e_1, \ldots, e_{p-1}$. Let

$$\zeta = \sum \lambda_{\mu_0 \mu_1 \ldots \mu_{p-1}} e_0^{\mu_0} e_1^{\mu_1} \ldots e_{p-1}^{\mu_{p-1}} \tag{18}$$

be an element of $\mathfrak{Z}$ in canonical form. Denote by $\nu_0 = \nu_0(\zeta)$ the highest power of e_0 occurring among the terms of highest degree in (18), so that there is a term

$$\lambda_{\nu_0 \nu_1 \ldots \nu_{p-1}} e_0^{\nu_0} e_1^{\nu_1} \ldots e_{p-1}^{\nu_{p-1}} \neq 0, \quad \text{with} \quad \nu_0 + \nu_1 + \ldots + \nu_{p-1} = d(\zeta),$$

in (18).

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

Suppose, for some such term, that there is an exponent $i>0$ for which p does not divide ν_i. If we let $\lambda=\lambda_{\nu_0\nu_1\dots\nu_{p-1}}$, we have

$$0=e_{-i}\circ\zeta=\dots+e_{-i}\circ\lambda e_0^{\nu_0}e_1^{\nu_1}\dots e_{p-1}^{\nu_{p-1}}+\dots.$$

Computing the value of $e_{-i}\circ\lambda e_0^{\nu_0}e_1^{\nu_1}\dots e_{p-1}^{\nu_{p-1}}$ and straightening it out, we could find a term

$$2i\nu_i\lambda e_0^{\nu_0+1}\dots e_i^{\nu_i-1}\dots\neq 0$$

which, because of the maximum property of ν_0, could not be cancelled out by any other term. Hence

$$\nu_i\equiv 0 \pmod p, \text{ for } i=1, 2, \dots, p-1.$$

Substituting ζ_i for e_i^p if $i>0$ and substituting $\zeta_0^p+e_0$ for e_0^p and continuing in this way for as long as possible, we transform the canonical expression (18) for ζ, after a finite number of steps, into the form

$$\zeta=\sum_{0\leqq\eta_i<p,\text{ for } i=0,1,\dots,p-1}\kappa_{\eta_0\eta_1\dots\eta_{p-1}}e_0^{\eta_0}e_1^{\eta_1}\dots e_{p-1}^{\eta_{p-1}}, \tag{19}$$

which expresses ζ as a linear combination of the p^p basis elements of $A(L)$ over o. Writing for (19),

$$\zeta=\sum_{\substack{0\leqq\chi_i<p\\(i=0,1,\dots,p-1)}}\xi_{\alpha_0\alpha_1\dots\alpha_{p-1};\,\chi_0\chi_1\dots\chi_{p-1}}\zeta_0^{\alpha_0}\dots\zeta_{p-1}^{\alpha_{p-1}}e_0^{\chi_0}\dots e_{p-1}^{\chi_{p-1}} \tag{20}$$

with $\xi_{\alpha_0\dots\alpha_{p-1};\,\chi_0\dots\chi_{p-1}}\in F$, we may associate with each term on the right hand side of (20) a weight, the weight of the term shown being

$$\sum_{i=0}^{p-1}\alpha_i p+\chi_i.$$

In the process of transforming (18) into (20), we find that at each step a term of a certain weight is replaced by a term of the same weight, with the same coefficient,and perhaps an additional term of lower weight. At any rate the terms of highest weight in (20) are obtained from the terms of highest degree in (18) by replacing, as far as possible, pth powers of e_i by ζ_i, for $i=0$, $1, \dots, p-1$. After this has been done none of the terms of highest weight is cancelled out; there are highest terms, not equal to zero, of the form

$$\lambda_{\nu_0,p\beta_1\dots p\beta_{p-1}}e_0^{\nu_0}e_1^{p\beta_1}\dots e_{p-1}^{p\beta_{p-1}}$$

in (18). Writing $\nu_0=j+p\beta_0$, we find that there is a term of highest weight of the form

$$\lambda_{\nu_0,p\beta_1,\dots,p\beta_{p-1}}\zeta_0^{\beta_0}\zeta_1^{\beta_1}\dots\zeta_{p-1}^{\beta_{p-1}}e_0^j\neq 0$$

in (20). We thus find that, in (19),

$$\kappa_{j00\dots0}\neq 0.$$

It follows that the operator-homomorphism

$$\zeta\to\sum_{j=0}^{p-1}\kappa_{j00\dots0}e_0^j$$

of the o-module $\mathfrak{Z}$ onto the o-module with the p basis elements $1, e_0, \dots, e_0^{p-1}$ is an operator-isomorphism. The rank of $\mathfrak{Z}$ over o is therefore less than or equal to p.

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

It follows that

$$1 < \dim_{Q(\mathfrak{o})} Q(\mathfrak{Z}) \leqslant p,$$
$$\dim_{Q(\mathfrak{o})} Q(\mathfrak{Z}) / \dim_{Q(\mathfrak{o})} Q(A(L)) = p^p,$$
$$\dim_{Q(\mathfrak{o})} Q(\mathfrak{Z}) = p,$$
$$\dim_{Q(\mathfrak{Z})} (A(L)) = p^{p-1} = p^{2m},$$
$$m = \tfrac{1}{2}(p-1).$$

Our result may be stated thus :

The enveloping algebras of the Lie-algebras of Witt of dimension p over a field of charactercistic $p>2$ are maximal orders of a division algebra of dimension p^{p-1} over its center. Each absolutely irreducible representation is of degree $p^{\frac{1}{2}(p-1)}$ or less, and the upper bound is actually attained.

From [2] it follows now that $Q(\mathfrak{Z})$ is separable over $Q(\mathfrak{o})$.

For more detailed results, see [2].

§ 6. For certain purposes, in particular for the discussion of Kronecker-Lie-products (*cf.* [6]) it is of advantage to deal with $A(L)$ as a ring over $\mathfrak{o}$ instead of as a ring over $\mathfrak{Z}$.

We know that after a suitable extension of the ground field there is a basis of $A(L)$ over $\mathfrak{o}$ consisting of p^l elements, where $l = \dim_F (L^* - \mathfrak{Z} \frown L^*)$. It follows that

$$\mathfrak{E}_{A(L)/\mathfrak{o},\, i} = 0, \text{ for } i = 0, 1, \ldots, p^l - 1,$$
$$\mathfrak{E}_{A(L)/\mathfrak{o},\, p^l} = \mathfrak{o}.$$

Hence for any homomorphism θ of $\mathfrak{o}$ onto an algebra over F, it follows from theorem 2 that there will always be p^l basis elements of $\theta^{(A(L))} A(L)$ over $\theta\mathfrak{o}$. Hence all these homomorphisms are extendable.

Again, for the discussion of the irreducible representations of $A(L)$ of finite degree over F, we have to deal with the homomorphisms of $\mathfrak{o}$ over F onto finite extensions of F, and there will belong to any of them only a finite number of non-equivalent irreducible representations of L.

For the discussion of the indecomposable representations of $A(L)$ of finite degree over F, we have to deal with the homomorphisms of $\mathfrak{o}$ over F onto primary algebras over F.

Any homomorphism Θ over F of $A(L)$ into an F-ring $\mathfrak{R}^\Theta$, mapping 1 onto the unit element of $\mathfrak{R}^\Theta$, may be called a specialisation of $A(L)$ into this F-ring. Two specialisations Θ and Θ' of $A(L)$ into $\mathfrak{R}^\Theta$ and $\mathfrak{R}^{\Theta'}$, respectively, are called *equivalent* if there is an isomorphism between $\mathfrak{R}^\Theta$ and $\mathfrak{R}^{\Theta'}$ over F mapping Θx onto $\Theta' x$ for all $x \in A(L)$. This notion meets the usual three requirements for an equivalence relation. Two specialisations Θ and Θ' of $A(L)$ into the F-rings $\mathfrak{R}^\Theta$ and $\mathfrak{R}^{\Theta'}$, respectively, are added by the rule

$$(\Theta + \Theta')x = \Theta x + \Theta' x,$$

which defines a specialisation of $A(L)$ into the algebraic sum of $\mathfrak{R}^\Theta$ and $\mathfrak{R}^{\Theta'}$.

The Lie-Kronecker product of two specialisations Θ and Θ', denoted by $\Theta \otimes \Theta'$, is defined by the rules

$$\Theta \otimes \Theta'(a) = 1_{\mathfrak{R}^\Theta} \,.\, \Theta'(a) + \Theta(a) \,.\, 1_{\mathfrak{R}^{\Theta'}}, \quad \text{for } a \in L,$$
$$\Theta \otimes \Theta'(1) = 1_{\mathfrak{R}^\Theta} \,.\, 1_{\mathfrak{R}^{\Theta'}},$$
$$\Theta \otimes \Theta' \left(\sum \lambda_{\alpha_1 \alpha_2 \ldots \alpha_n} a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n} \right)$$
$$= \sum \lambda_{\alpha_1 \alpha_2 \ldots \alpha_n} \{\Theta \otimes \Theta'(a_1)\}^{\alpha_1} \ldots \{\Theta \otimes \Theta'(a_n)\}^{\alpha_n},$$

by which, in fact, a specialisation $\Theta \otimes \Theta'$ of $A(L)$ into the product ring of $\mathfrak{R}^\Theta$ and $\mathfrak{R}^{\Theta'}$ over F is defined, as can be easily verified. Furthermore, it is easy to verify that the substitution laws of addition and multiplication with respect to our equivalence notion hold, and that the classes of equivalent specialisations form a commutative semi-ring $S(A(L))$ with that specialisation Θ_1 of $A(L)$ onto F which is defined by the rules

$$\Theta_1(a) = 0 \quad \text{for } a \in L,$$
$$\Theta_1(1) = 1,$$
$$\Theta_1\left(\sum \lambda_{\alpha_1 \alpha_2 \dots \alpha_n} a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n}\right) = \lambda_{00 \dots 0}$$

acting as unit element. The semi-ring $S(A(L))$ contains as a subring the set $D(A(L))$ of all classes of equivalent specialisations containing all representations of $A(L)$ in the ring of all matrices of a certain finite degree, and the equivalence notion defined above coincides with the ordinary equivalence notion for representations.

From the theorem of Wedderburn–Remak–Krull–Schmidt–Fitting, it follows that

THEOREM 10. *The set of all classes of specialisations of $A(L)$ over F containing indecomposable representations of finite degree over F forms a basis of the commutative semi-ring $D(A(L))$ consisting of the set of all classes of equivalent specialisations containing representations of $A(L)$ of finite degree over F, relative to the natural numbers as multipliers.*

Any specialisation Θ of $A(L)$ into the ring $\mathfrak{R}^\Theta$ induces a specialisation Θ^L of L into $\mathfrak{R}^\Theta$, *i.e.*, a homomorphism over F of the Lie-algebra L over F into the F-Lie-ring attached to the associative F-ring $\mathfrak{R}^\Theta$. In this way there is defined a (1-1)-correspondence between the specialisations of $A(L)$ and those of L. Furthermore, the specialisations of L may be distributed into classes of equivalent ones, and added and multiplied as above, the Lie-Kronecker product this time being defined simply by the formula

$$\Theta \otimes \Theta'(a) = 1_{\mathfrak{R}^\Theta} \cdot \Theta' a + \Theta a \cdot 1_{\mathfrak{R}^\Theta}.$$

It follows that the correspondence

$$\Theta \to \Theta^L$$

induces an isomorphism between the semi-ring $S(A(L))$ and the semi-ring $S(L)$ of all classes of equivalent specialisations of L containing representations in the ring of all matrices of fixed finite degree over F.

All this can be stated with L^* in place of L, if the specialisations of L^* are defined as Lie-homomorphisms Θ of the F-Lie-ring L^* over F into arbitrary associative F-rings $\mathfrak{R}^\Theta$ with unit elements, satisfying the additional condition

$$\Theta(x^p) = (\Theta x)^p \quad \text{for all } x \text{ in } L^*.$$

We then have to use the rule

$$\Theta \otimes \Theta'(x^p) = \{\Theta \otimes \Theta'(x)\}^p,$$

which is easily verified, for the product definition.

Any specialisation Θ of $A(L)$ into $\mathfrak{R}^\Theta$ induces also a specialisation Θ^0 of o into $\mathfrak{R}^\Theta$, *i.e.*, a homomorphism over F of the F-ring o into the F-ring $\mathfrak{R}^\Theta$ which maps the unit element of o onto the unit element of $\mathfrak{R}^\Theta$. Equivalence, sum and product are defined as above, the Lie-

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

Kronecker product of two specialisations Θ, Θ' of $\mathfrak{o}$ into $\mathfrak{R}^{\Theta}$ and $\mathfrak{R}^{\Theta'}$, respectively, being defined by the formulas

$$\Theta \otimes \Theta'(u) = 1_{\mathfrak{R}^{\Theta}} \cdot \Theta' u + \Theta u \cdot 1_{\mathfrak{R}^{\Theta'}}, \quad \text{for } u \in \mathfrak{o} \frown L^*$$

and

$$\Theta \otimes \Theta' \left(\sum \lambda_{\alpha_1 \alpha_2 \dots \alpha_n} u_1^{\alpha_1} u_2^{\alpha_2} \dots u_n^{\alpha_n} \right)$$

$$= \sum \lambda_{\alpha_1 \alpha_2 \dots \alpha_n} \{\Theta \otimes \Theta'(u_1)\}^{\alpha_1} \dots \{\Theta \otimes \Theta'(u_n)\}^{\alpha_n},$$

for an arbitrary element of $\mathfrak{o}$ as represented according to lemma 4 of § 1.

But this time we find only a *homomorphism* of $S(A(L))$ onto the semi-ring $S(\mathfrak{o})$ of all classes of equivalent specialisations of $\mathfrak{o}$, and only a homomorphism of $D(A(L))$ onto the semi-ring $D(\mathfrak{o})$ of all classes of equivalent specialisations of $\mathfrak{o}$ containing representations by matrices of finite degree over F.

We call two specialisations Θ, Θ' of any one of the systems $A(L)$, L, L^* and $\mathfrak{o}$ weakly equivalent if

$$\Theta x = 0 \quad \text{if and only if} \quad \Theta' x = 0.$$

Weak equivalence again satisfies the necessary three requirements, and is implied by ordinary equivalence. It also satisfies the substitution laws of addition and multiplication; so the sets of all classes of weakly equivalent specialisations form subrings $W(A(L))$, $W(L)$, $W(L^*)$ and $W(\mathfrak{o})$. The sets of all classes of weakly equivalent specialisations containing representations by matrices of finite degree over F form semi-rings $WD(A(L))$, $WD(L)$, $WD(L^*)$ and $WD(\mathfrak{o})$.

The semi-rings $W(A(L))$, $W(L)$ and $W(L^*)$ are homomorphic to $S(A(L))$, $S(L)$ and $S(L^*)$, respectively; $WD(A(L))$, $WD(L)$ and $WD(L^*)$ are homomorphic to $D(A(L))$, $D(L)$ and $D(L^*)$, respectively; and $W(\mathfrak{o})$ is homomorphic to both $S(\mathfrak{o})$ and $W(A(L))$.

Instead of referring to classes of weakly equivalent specialisations containing representations by matrices of finite degree over f we might equally well refer to classes of weakly equivalent specialisations containing specialisations onto algebras over F. Instead of theorem 10 we have

THEOREM 11. *The sets of all classes of weakly equivalent specialisations of $A(L)$ and $\mathfrak{o}$, respectively, containing a specialisation onto a primary algebra over F, constitute bases of the commutative semi-rings $WD(A(L))$ and $WD(\mathfrak{o})$, respectively, of all classes of weakly equivalent specialisations of $A(L)$ and $\mathfrak{o}$, respectively, containing specialisations onto algebras over F, relative to the natural numbers as multipliers.*

Furthermore we have

THEOREM 12. *The units of the semi-ring $W(\mathfrak{o})$ of all classes of weakly equivalent specialisations of $\mathfrak{o}$ over F are represented by the specialisations of $\mathfrak{o}$ onto F, over F.*

Proof: If Θ represents a unit of $W(\mathfrak{o})$, then Θ may be chosen as a specialisation of $\mathfrak{o}$ onto an F-ring $\Theta\mathfrak{o}$. There will be another specialisation Θ' onto an F-ring $\Theta'\mathfrak{o}$, such that $\Theta \otimes \Theta'$ maps all elements of $L^* \frown \mathfrak{Z}$ onto zero:

$$1_{\Theta\mathfrak{o}} \cdot \Theta' u + \Theta u \cdot 1_{\Theta'\mathfrak{o}} = 0, \quad \text{for all } u \text{ in } L^* \frown \mathfrak{Z}.$$

https://doi.org/10.1017/S2040618500032974 Published online by Cambridge University Press

From the relation

$$1_{\Theta 0} \cdot \Theta' u = -\Theta u \cdot 1_{\Theta' 0} \quad (u \in L^* \cap \mathfrak{Z})$$

in the product ring $\Theta 0 \otimes \Theta' 0$ over F, we conclude that

$$\Theta u = \Lambda(u) 1_{\Theta 0}, \quad \Theta' u = -\Lambda(u) 1_{\Theta' 0}, \quad \text{where } \Lambda(u) \in F;$$

hence both $\Theta 0$ and $\Theta' 0$ coincide with F.

Conversely, if there is a specialisation Θ of $\mathfrak{o}$ onto F, then there is another one, Θ' say, defined by $\Theta' u = -\Theta u$. It follows that their product maps each element of $L^* \cap \mathfrak{Z}$ onto zero, which means that this product represents the unit element of $W(\mathfrak{o})$

If Θ and Θ' are two specialisations of $\mathfrak{o}$ onto F, say

$$\Theta u = \Lambda(u) \in F, \quad \Theta' u = \Lambda'(u) \in F, \quad \text{for } u \in L^* \cap \mathfrak{Z},$$

then it follows that

$$\Theta \otimes \Theta'(u) = \Lambda(u) + \Lambda'(u).$$

This proves the corollary to theorem 12.

The specialisations of $\mathfrak{o}$ onto F over F form an abelian group of characteristic p isomorphic to the group of units in $W(\mathfrak{o})$ and also to the group of units of $S(\mathfrak{o})$.

We define two specialisations Θ and Θ' of $A(L)$ to *belong to the same family* if they induce weakly equivalent specialisation of $\mathfrak{o}$. This relation satisfies the three necessary requirements for an equivalence relation.

Weak equivalence of two specialisations of $A(L)$ implies that they both belong to the same family. Again the substitution laws of addition and multiplication are satisfied. The set of all families forms a commutative semi-ring $F(A(L))$, and $F(A(L))$ is isomorphic to $W(\mathfrak{o})$. Each family contains among its members at most a finite number of non-equivalent irreducible representations of finite degree over F.

The set of all families containing an absolutely irreducible representation forms an abelian group of characteristic p which is isomorphic to the group of units of $S(\mathfrak{o})$.

This group may be recognised by making use of lemma 4 of § 1 as the additive group defined by the vector module of n dimensions over F.

REFERENCES

(1) Birkhoff, G., " Representability of Lie Algebras ", *Annals of Math.*, (2), **38** (1937), pp. 526–532.

(2) Chang, Ho-Jui, " Ueber Wittsche Lie-Ringe ", *Abh. Math. Sem. Univ. Hamburg*, **14** (1941), pp. 151–196.

(3) Jacobson, N., " Abstract derivation and Lie Algebras ", *Trans. Am. Math. Soc.*, **42** (1937), pp. 206–224.

(4) Jacobson, N., " A note on Lie algebras of characteristic p ", *Am. J. Math.*, **74** (1952), pp. 357–359.

(5) Witt, E., " Treue Darstellung Lie'scher Ringe ", *Crelles Journal f. Reine u. Angew. Math.*, **177** (1937), pp. 152–160.

(6) Zassenhaus, H., " Ueber Lie'sche Ringe mit Primzahl Characteristik ", *Abh. Math. Sem. Univ. Hamburg*, **13** (1939), pp. 1–100.

(7) Zassenhaus, H., " Ein Verfahren jeder endlichen p-Gruppe einen Lie-Ring der Characteristik p zuzuordnen ", *Abh. Math. Sem. Univ. Hamburg*, **13** (1939), pp. 200–207.

(8) Zassenhaus, H., " Darstellungstheorie nilpotenter Lie-Ringe bei Characteristik $p > 0$ " *Crelles Journal f. Reine u. Angew. Math.*, **185** (1940).

(9) Zassenhaus, H., *The Theory of Groups*, Chelsea, 1949.

McGill University,
Montreal, P.Q., Canada