# ABSTRACT DERIVATION AND LIE ALGEBRAS*

BY

NATHAN JACOBSON†

The purpose of this paper is the investigation of the algebraic properties of the set of operations mapping an algebra on itself and having the formal character of derivation in the field of analytic functions. Some of the results obtained are analogous to well-known theorems on automorphisms of algebras.‡ The considerations in I are general and quite elementary. In II and III we restrict ourselves to the derivations of an associative algebra having a finite basis and in the main to semi-simple algebras. A number of results of the theory of algebras are presupposed. These may be found in Deuring's *Algebren*, Springer, 1935.

## I. Derivations in an arbitrary algebra

1. Let $\mathfrak{R}$ be an arbitrary algebra (hypercomplex system not necessarily commutative or associative, or of finite order) over a commutative field $\mathfrak{F}$. Then $\mathfrak{R}$ is a vector space (with elements $x, y, \cdots$) over $\mathfrak{F}$ (with elements $\alpha, \beta, \cdots$) in which a composition $xy\epsilon\mathfrak{R}$ is defined such that

$$(1)\quad (x + y)z = xz + yz,\quad z(x + y) = zx + zy,\quad (xy)\alpha = (x\alpha)y = x(y\alpha).$$

A *derivation* $D$ of $\mathfrak{R}$ is a single valued mapping of $\mathfrak{R}$ on itself such that

$$(2)\ \text{(a)}\ (x + y)D = xD + yD,\ \text{(b)}\ (x\alpha)D = (xD)\alpha,\ \text{(c)}\ (xy)D = (xD)y + x(yD).$$

Thus $D$ is a linear transformation in the vector space $\mathfrak{R}$ satisfying the special condition (2c). It is well known that the sum $D_1+D_2$, difference $D_1-D_2$, scalar product $D\alpha$ and product $D_1D_2$ (defined respectively by $x(D_1\pm D_2)\equiv xD_1\pm xD_2$, $x(D\alpha)\equiv(xD)\alpha$, $x(D_1D_2)\equiv((xD_1)D_2)$ of linear transformations are linear transformations. If $D$, $D_1$, $D_2$ are derivations we have besides

$$(3)\quad \begin{aligned}(xy)(D_1 \pm D_2) &= (xy)D_1 \pm (xy)D_2 = (xD_1)y + x(yD_1) \pm (xD_2)y \pm x(yD_2)\\ &= (x(D_1 \pm D_2))y + x(y(D_1 \pm D_2)),\end{aligned}$$

$$(4)\quad (xy)D\alpha = ((xy)D)\alpha = ((xD)y + x(yD))\alpha = (xD\alpha)y + x(yD\alpha),$$

---

* Presented to the Society, December 31, 1936; received by the editors November 6, 1936.

† National Research Fellow.

‡ A direct connection between derivations and automorphisms may sometimes be established. For example if $\mathfrak{R}$ is the ring of polynomials $\mathfrak{F}[x]$ where $\mathfrak{F}$ is a field of characiterstic 0, and $D$ is defined by $f(x)D=f'(x)$ the usual derivative then exp $D=1+D+D^2/2!+\cdots$ is an automorphism since $f(x)$ exp $D=f(x+1)$.

$$(5)\qquad \begin{aligned}(xy)D_1D_2 &= ((xy)D_1)D_2 = ((xD_1)y + x(yD_1))D_2\\ &= (xD_1D_2)y + x(yD_1D_2) + (xD_1)(yD_2) + (xD_2)(yD_1).\end{aligned}$$

Thus $D_1 \pm D_2$, $D\alpha$ are derivations, but not in general $D_1D_2$. However (5) shows that the commutator $[D_1, D_2] = D_1D_2 - D_2D_1$ does satisfy (2c) and so is a derivation. We recall the relations

$$(6)\quad [D_1, D_2] = -[D_2, D_1],\ [[D_1, D_2], D_3] + [[D_2, D_3], D_1] + [[D_3, D_1], D_2] = 0.$$

As a consequence of (2) we have Leibniz's formula:

$$(7)\quad (xy)D^k = (xD^k)y + C_{k,1}(xD^{k-1})(yD) + C_{k,2}(xD^{k-2})(yD^2) + \cdots + x(yD^k).$$

Hence if $\mathfrak{F}$ has characteristic $p \neq 0$ we have

$$(8)\qquad (xy)D^p = (xD^p)y + x(yD^p);$$

i.e., $D^p$ is a derivation.

By *a restricted Lie algebra of linear transformations* we shall mean a system of linear transformations closed relative to the operations of addition, subtraction, scalar multiplication, commutation, and taking $p$th powers, if $p$ ($=0$ or a prime) is the characteristic of the field over which the vector space is defined.* With this definition we have

THEOREM 1. *The derivations of an algebra $\mathfrak{R}$ over $\mathfrak{F}$ constitute a restricted Lie algebra $\mathfrak{D}$ of linear transformations in $\mathfrak{R}$.*

We call $\mathfrak{D}$ the *derivation algebra* or, more briefly, the *d-algebra* of $\mathfrak{R}$ over $\mathfrak{F}$. It should be noted that we are regarding $\mathfrak{D}$ as an algebra over $\mathfrak{F}$.

2. Suppose $D, E, D_1, D_2, \cdots$ are elements of any associative algebra $\mathfrak{A}$. As a generalization of the multinomial theorem in a commutative algebra we have

$$(9)\qquad (D_1 + D_2 + \cdots + D_r)^k = \sum \begin{Bmatrix} D_1 & D_2 & \cdots & D_r \\ j_1 & j_2 & \cdots & j_r \end{Bmatrix},$$

where the summation is extended over $j_1, \cdots, j_r$ such that $j_\alpha \geqq 0$ and $j_1 + \cdots + j_r = k$ and where $\{D_1 \cdots D_r / j_1 \cdots j_r\}$ denotes the sum of the $(j_1 + \cdots + j_r)!/(j_1! \cdots j_r!)$ terms obtained by multiplying $j_1$ of the $D_1$'s, $j_2$ of the $D_2$'s, $\cdots$, $j_r$ of the $D_r$'s together in every possible order. Let $D_{i_1} + D_{i_2} + \cdots + D_{i_s} = D_{i_1 i_2 \cdots i_s}$ where $i_1, i_2, \cdots, i_s$ are distinct and have values in the range $1, 2, \cdots, k$. Consider

$$D^k_{i_1 \cdots i_k} - \sum_C D^k_{i_1 \cdots i_{k-1}} + \cdots + (-1)^{k-1} \sum_C D^k_{i_1} = Q,$$

* We use the convention $D^0 = 0$.

where $\sum_C D^k_{i_1\cdots i_s}$ denotes the sum of the $C_{k,s}$ terms obtained by letting $i_1, \cdots, i_s$ run through all the combinations of $1, 2, \cdots, k$ taken $s$ at a time. By (9), $Q$ is a sum of terms of the form $\{D_{m_1}\cdots D_{m_t}/j_1\cdots j_t\}$ where $j_\alpha>0$ and $j_1+j_2+\cdots+j_t=k$. Since

$$\begin{Bmatrix} D_{m_1} & \cdots & D_{m_t} \\ j_1 & \cdots & j_t \end{Bmatrix} = \begin{Bmatrix} D_{m_1} & \cdots & D_{m_t} & D_{n_1} & \cdots & D_{n_r} \\ j_1 & \cdots & j_t & 0 & \cdots & 0 \end{Bmatrix},$$

where $n_1, n_2, \cdots, n_r$ are distinct indices different from $m_1, m_2, \cdots, m_r$, the term $\{D_{m_1}\cdots D_{m_t}/j_1\cdots j_t\}$ has the coefficient $C_{k-t,r}$ in $\sum_C D^k_{i_1\cdots i_{t+r}}$ and hence the coefficient of this term in $Q$ is

$$C_{k-t,k-t} - C_{k-t,k-t-1} + \cdots + (-1)^{k-t}C_{k-t,0} = \delta_{kt},$$

i.e., $=0$ or $1$ according as $k\neq t$ or $k=t$. Hence

$$(10)\qquad D^k_{i_1\cdots i_k} - \sum_C D^k_{i_1\cdots i_{k-1}} + \cdots + (-1)^k \sum_C D^k_{i_1} = \begin{Bmatrix} D_1 & \cdots & D_k \\ 1 & \cdots & 1 \end{Bmatrix}.^*$$

Since

$$\begin{Bmatrix} D_1+\cdots+D_r & D \\ k & 1 \end{Bmatrix} = \sum \begin{Bmatrix} D_1 & \cdots & D_r & D \\ j_1 & \cdots & j_r & 1 \end{Bmatrix},$$

where $j_\alpha \geqq 0$ and $j_1+\cdots+j_r=k$, we may derive the following formula similar to (10):

$$(11)\qquad \begin{Bmatrix} D_{i_1\cdots i_k} & D \\ k & 1 \end{Bmatrix} - \cdots + (-1)^{k-1}\sum_C \begin{Bmatrix} D_{i_1} & D \\ k & 1 \end{Bmatrix} = \begin{Bmatrix} D_1 & \cdots & D_k & D \\ 1 & \cdots & 1 & 1 \end{Bmatrix}.$$

If in (10) and (11) we set $j_1$ of the $D$'s equal to $D_1$, $j_2$ equal to $D_2, \cdots, j_l$ equal to $D_l$ then $\{D_1\cdots D_k/1\cdots 1\}$ and $\{D_1\cdots D_kD/1\cdots 11\}$ become respectively $(j_1!\cdots j_l!)\{D_1\cdots D_l/j_1\cdots j_l\}$ and $(j_1!\cdots j_l!)\{D_1\cdots D_lD/j_1\cdots j_l1\}$ and we obtain expressions for these as sums of $k$th powers and as sums of terms of the type $\{ED/k1\}$.

An analogue of (7) is

$$(12)\qquad DE^k = E^kD + C_{k,1}E^{k-1}D' + \cdots + D^{(k)}$$

where $D'=[D, E], \cdots, D^{(j)}=[D^{(j-1)}, E]$. Hence

$$E^lDE^{k-l} = E^kD + C_{k-l,1}E^{k-1}D' + \cdots + C_{k-l,j}E^{k-j}D^{(j)} + \cdots + E^lD^{(k-l)},$$

and summing on $l=0, 1, \cdots, k$ we have

---

* If we set $D_1=D_2=\cdots=D_k=1$ in (10) we obtain the identity
$$k^k - C_{k,1}(k-1)^k + C_{k,2}(k-2)^k - \cdots + (-1)^{k-1}C_{k,k-1}1^k = k!.$$

(13) $$\begin{Bmatrix} E & D \\ k & 1 \end{Bmatrix} = C_{k+1,1}E^kD + \cdots + C_{k+1,j+1}E^{k-j}D^{(j)} + \cdots + D^{(k)},$$

since

$$C_{k,j} + C_{k-1,j} + \cdots + C_{j,j} = C_{k+1,j+1}.$$

If the characteristic of $\mathfrak{A}$ is $p \neq 0$ special cases of (12) and (13) are

(14) $$\text{(a)}\quad [D, E^p] = D^{(p)}, \qquad \text{(b)}\quad \begin{Bmatrix} E & D \\ p-1 & 1 \end{Bmatrix} = D^{(p-1)}.$$

Equations (11) and (14b) show that $\{D_1 \cdots D_p/1 \cdots 1\}$ is expressible as a linear combination of $(p-1)$-fold commutators, i.e., of the type $D^{(p-1)}$ where $D = D_p$ and $E$ is a sum of the other $D_i$'s. Hence we see also that $(j_1! \cdots j_l!)\ \{D_1 \cdots D_l/j_1 \cdots j_l\}$ where $j_1 + \cdots + j_l = p$ is a linear sum of $(p-1)$-fold commutators. If no $j_i = p$, $(j_1! \cdots j_l!) \not\equiv 0 \pmod p$ and so $\{D_1D_2 \cdots D_l/j_1j_2 \cdots j_l\}$ is a linear sum of $(p-1)$-fold commutators and (9) becomes

(15) $$(D_1 + D_2 + \cdots + D_r)^p = D_1^p + D_2^p + \cdots + D_r^p + S,$$

where $S$ is a linear sum of $(p-1)$-fold commutators.

3. If $\mathfrak{D}$ is any system of linear transformations we define the *enveloping algebra* $\mathfrak{A}$ of $\mathfrak{D}$ to be the totality of linear combinations of products of a finite number of elements of $\mathfrak{D}$. We call $k$ the degree of the monomial $D_1D_2 \cdots D_k$, $D_i \epsilon \mathfrak{D}$. Suppose $\mathfrak{D}$ is a Lie algebra of linear transformations and consider $D_1D_2 \cdots D_k$ where $k < p$ if $p \neq 0$ and arbitrary if $p = 0$. We have

$$D_1 \cdots D_{i-1}D_{i+1}D_iD_{i+2} \cdots D_k = D_1D_2 \cdots D_k + D_1 \cdots D_{i-1}D'D_{i+2} \cdots D_k,$$

where $D' = [D_{i+1}, D_i] \epsilon \mathfrak{D}$. Since any arrangement $i_1i_2 \cdots i_k$ of $1, 2, \cdots, k$ may be obtained from $1, 2, \cdots, k$ by a sequence of transpositions of adjacent indices

$$D_{i_1}D_{i_2} \cdots D_{i_k} = D_1D_2 \cdots D_k + R,$$

where $R$ is a sum of terms of degree $< k$. Hence

$$\begin{Bmatrix} D_1 & D_2 & \cdots & D_k \\ 1 & 1 & \cdots & 1 \end{Bmatrix} = (k!)D_1D_2 \cdots D_k + S,$$

where degree of $S < k$. Since the left-hand side of this equation is expressible by (10) as a sum of $k$th powers of elements in $\mathfrak{D}$ and $k! \not\equiv 0 \pmod p$, we have by induction that $D_1D_2 \cdots D_k$ is a linear combination of $l$th powers of elements of $\mathfrak{D}$ where $l \leq k$.

THEOREM 2. *If $\mathfrak{D}$ is a Lie algebra of linear transformations the elements in the enveloping algebra $\mathfrak{A}$ of degree $k<p$ if $p\neq 0$ and of arbitrary degree if $p=0$ are expressible as linear combinations of lth powers $l\leqq k$, of elements of $\mathfrak{D}$.**

If $\mathfrak{D}$ is restricted (10) shows that $\{D_1D_2\cdots D_r/j_1j_2\cdots j_r\}\in\mathfrak{D}$ if $j_1+j_2+\cdots+j_r=p$ and $D_i\in\mathfrak{D}$. This transformation is also expressible as a sum of $(p-1)$-fold commutators of elements of $\mathfrak{D}$. Since $(D_1+D_2+\cdots+D_r)^{p^k}$ $=((D_1+D_2+\cdots+D_r)^{p^{k-1}})^p$ for $j_1, j_2, \cdots, j_r$ such that $j_1+j_2+\cdots+j_r=p^k$, we have

$$\begin{Bmatrix} D_1 & D_2 & \cdots & D_r \\ j_1 & j_2 & \cdots & j_r \end{Bmatrix} = \sum \left\{ \begin{matrix} \begin{Bmatrix} D_1 & D_2 & \cdots & D_r \\ k_{11} & k_{12} & \cdots & k_{1r} \end{Bmatrix} & \begin{Bmatrix} D_1 & D_2 & \cdots & D_r \\ k_{21} & k_{22} & \cdots & k_{2r} \end{Bmatrix} & \cdots \\ m_1 & m_2 & \cdots \end{matrix} \right\},$$

where the summation is extended over the non-negative integers such that the ordered set $(k_{l1}, k_{l2}, \cdots, k_{lr})\neq(k_{m1}, k_{m2}, \cdots, k_{mr})$ for $l\neq m$ and

$$k_{l1}+k_{l2}+\cdots+k_{lr}=p^{k-1} \qquad (l=1, 2, \cdots),$$

$$m_1+m_2+\cdots=p,$$

$$k_{1i}m_1+k_{2i}m_2+\cdots=j_i \qquad (i=1, 2, \cdots, r).$$

Hence we see by induction on $k$ that $\{D_1D_2\cdots D_r/j_1j_2\cdots j_r\}\in\mathfrak{D}$ *for all* $j_1, j_2, \cdots$ *such that* $j_1+j_2+\cdots+j_r=p^k$.

4. Because of (14a) we are led to the definition: A *restricted Lie Algebra* $\mathfrak{R}$ *of characteristic* $p$ $(=0$ or not) is an algebra (i.e., satisfies (1)) in which the composition $[x, y]$ (in place of $xy$) satisfies

(16) $$[x, y] = -[y, x],$$

(17) $$[[x, y], z]+[[y, z], x]+[[z, x], y]=0,$$

for every $y$ there exists an element denoted as $y^p$ such that

(18) $$[\cdots[[x, \overbrace{y]y]\cdots y}^{p}] = [x, y^p]$$

for all $x$. A *restricted subalgebra* $\mathfrak{S}$ of $\mathfrak{R}$ is a subalgebra containing $y^p$ for every $y$ in $\mathfrak{S}$. Similarly we define restricted ideal, etc.†

Suppose $\mathfrak{R}$ is an associative algebra. We may define a new composition $[x, y]=xy-yx$ in terms of $xy$ defined in $\mathfrak{R}$. It is readily verified that $\mathfrak{R}$ is a

* This is a slight extension of a result announced recently by M. Zorn (Bulletin of the American Mathematical Society, vol. 42 (1936), p. 485). Cf. H. Poincaré, *Sur les groupes continus*, Cambridge Philosophical Transactions, vol. 18 (1899), pp. 220–255.

† For definitions of the important concepts in the theory of Lie algebras the reader is referred to Jacobson, *Rational methods in the theory of Lie algebras*, Annals of Mathematics, vol. 36 (1935), pp. 875–881.

restricted Lie algebra if $y^p$ is defined as the $p$th power of $y$ in $\mathfrak{R}$. We shall call this Lie algebra *the restricted Lie algebra determined by the associative* $\mathfrak{R}$.

5. If $\mathfrak{R}$ is any algebra the mapping $a_r$: $x \to xa$ is a linear transformation and will be called the *right multiplication* determined by $a$. Suppose $D$ is a derivation in $\mathfrak{R}$. Equation (2c) gives the commutation relation

$$[a_r, D] = (aD)_r. \tag{19}$$

Similarly we define $a_l$ as $x \to ax$ and call this mapping the *left multiplication* determined by $a$. In place of (19) we have $[a_l, D] = (aD)_l$. If $\mathfrak{R}$ is a Lie algebra $a_r = -a_l$ and, by (16) and (17),

$$[x, y]a_r = [xa_r, y] + [x, ya_r].$$

Thus $a_r$ is a derivation which we call *inner*.

THEOREM 3. *The totality of inner derivations of a (restricted) Lie algebra* $\mathfrak{R}$ *is a (restricted) ideal* $\mathfrak{J}$ *in the d-algebra* $\mathfrak{D}$ *of* $\mathfrak{R}$. $\mathfrak{J} \cong \mathfrak{R}/\mathfrak{C}$ *where* $\mathfrak{C}$ *is the centrum of* $\mathfrak{R}$.*

If $a_r$ and $b_r$ are multiplications associated with $a$ and $b$ it follows directly from the definition of $\mathfrak{R}$ that $a_r \pm b_r = (a \pm b)_r$, $a_r\alpha = (a\alpha)_r$, $[a_r, b_r] = [a, b]_r$ and if $\mathfrak{R}$ is restricted $(a_r)^p = (a^p)_r$. Hence $\mathfrak{J}$ is a subalgebra of $\mathfrak{D}$ and is restricted if $\mathfrak{R}$ is. Furthermore the correspondence $a \to a_r$ is a homomorphism between $\mathfrak{R}$ and $\mathfrak{J}$. Since the elements of $\mathfrak{C}$ are the ones corresponding to 0 in this homomorphism $\mathfrak{R}/\mathfrak{C} \cong \mathfrak{J}$. Equation (19) shows that $\mathfrak{J}$ is an ideal.

Suppose $\mathfrak{R}$ is associative and $D$ a derivation. $D$ is also a derivation in the restricted Lie algebra determined by $\mathfrak{R}$. Hence the $d$-algebra of $\mathfrak{R}$ as an associative algebra is a restricted subalgebra of the $d$-algebra of $\mathfrak{R}$ as a Lie algebra. Moreover the inner derivations $x \to [x, a]$ are derivations of the associative $\mathfrak{R}$ since

$$[xy, a] = [x, a]y + x[y, a].$$

Thus $\mathfrak{J}$ is a restricted ideal in the $d$-algebra of the associative $\mathfrak{R}$.

If $\mathfrak{R}$ is associative, $\mathfrak{D}$ its $d$-algebra, $D \epsilon \mathfrak{D}$ and $c \epsilon \mathfrak{C}$ the centrum of $\mathfrak{R}$ then $c_r = c_l \equiv c$ and it is easily verified that $Dc \epsilon \mathfrak{D}$ also. Hence $\mathfrak{D}$ has $\mathfrak{C}$ as well as $\mathfrak{F}$ as a set of multipliers under which it is invariant. A subalgebra $\mathfrak{E}$ of $\mathfrak{D}$ which contains with every element $E$ also $Ec$ for every $c$ in $\mathfrak{C}$ will be called a $\mathfrak{C}$-*subalgebra* of $\mathfrak{D}$.

If $\mathfrak{R}$ is arbitrary, $D \epsilon \mathfrak{D}$ the elements $k \epsilon \mathfrak{R}$ such that $kD = 0$ are called *D-constants*. Their totality is a subalgebra. If $kD = 0$ for all $D$ then $k$ is a *constant*. If $\mathfrak{R}$ has an identity 1 we have $1^2 = 1$ and hence $1(1D) + (1D)1 = 1D$ or $1D = 0$

* The *centrum* is the set of elements $c$ such that $[c, x] = 0$ for all $x$ in $\mathfrak{R}$.

so that 1 is a constant. More generally if $\mathfrak{D}_1$ is a subalgebra of $\mathfrak{D}$ we denote the set of elements $k$ in $\mathfrak{R}$ such that $kD_1=0$ for all $D_1 \epsilon \mathfrak{D}_1$ by $\mathfrak{R}(\mathfrak{D}_1)$. $\mathfrak{R}(\mathfrak{D}_1)$ is a subalgebra. On the other hand if $\mathfrak{R}_1$ is a subalgebra of $\mathfrak{R}$ we define $\mathfrak{D}(\mathfrak{R}_1)$ to be the set of derivations $E$ such that $x_1E=0$ for all $x_1 \epsilon \mathfrak{R}_1$. $\mathfrak{D}(\mathfrak{R}_1)$ is a restricted subalgebra of $\mathfrak{D}$. Evidently $\mathfrak{D}(\mathfrak{R}(\mathfrak{D}_1)) \supset \mathfrak{D}_1$ and $\mathfrak{R}(\mathfrak{D}(\mathfrak{R}_1)) \supset \mathfrak{R}_1$. If $\mathfrak{R}$ is associative with centrum $\mathfrak{C}$, $\mathfrak{D}(\mathfrak{R}_1)$ is a restricted $\mathfrak{C}$-subalgebra of $\mathfrak{D}$.

$\mathfrak{S}$ is a *characteristic subalgebra* of $\mathfrak{R}$ if it is mapped on itself by every element of $\mathfrak{D}$. The subalgebra of constants $\mathfrak{R}_0$, the centrum $\mathfrak{C}$ and the powers of $\mathfrak{R}$ are characteristic. If $\mathfrak{S}$ is characteristic, $\mathfrak{D}(\mathfrak{S})$ is an ideal. In particular $\mathfrak{D}(\mathfrak{C})$ is an ideal containing $\mathfrak{J}$ if $\mathfrak{R}$ is associative or a Lie algebra. The derivations mapping $\mathfrak{R}$ on the characteristic subalgebra $\mathfrak{S}$ also form a restricted ideal $\mathfrak{G}$. In the case of a Lie algebra or an associative algebra the ideal associated in this way with $\mathfrak{C}$ is the *annihilator* of $\mathfrak{J}$, i.e., the set of elements $G$ such that $[a_r, G]=0$ for all $a_r$. This is an immediate consequence of (19).

## II. Derivations in an associative algebra with a finite basis

6. In the remainder of the paper $\mathfrak{R}$ will denote an associative algebra with a finite basis over $\mathfrak{F}$. We propose to study the $d$-algebra $\mathfrak{D}$ of $\mathfrak{R}$.

THEOREM 4. *If* $\mathfrak{R}=\mathfrak{R}_1 \oplus \mathfrak{R}_2$ *and* $\mathfrak{R}_1^2=\mathfrak{R}_1$, $\mathfrak{R}_2^2=\mathfrak{R}_2$ *then* $\mathfrak{D}=\mathfrak{D}_1 \oplus \mathfrak{D}_2$ *where* $\mathfrak{D}_i$ *is isomorphic to the d-algebra of* $\mathfrak{R}_i$.

$\mathfrak{R}_1$ is characteristic; for $\mathfrak{R}_1^2=\mathfrak{R}_1$ and so the arbitrary element $x_1$ of $\mathfrak{R}_1$ has the form $\sum y_1z_1$, $y_1, z_1 \epsilon \mathfrak{R}_1$. Hence $x_1D=\sum(y_1z_1)D=\sum(y_1D)z_1+\sum y_1(z_1D) \epsilon \mathfrak{R}_1$ since this is an ideal. Similarly $\mathfrak{R}_2$ is characteristic. Let $\mathfrak{D}_i$ be the ideals mapping $\mathfrak{R}$ onto $\mathfrak{R}_i$. Since $\mathfrak{R}_1 \cap \mathfrak{R}_2=0$, $\mathfrak{D}_1 \cap \mathfrak{D}_2=0$ and hence $[\mathfrak{D}_1, \mathfrak{D}_2] \subset \mathfrak{D}_1 \cap \mathfrak{D}_2 =0$.† If $x=x_1+x_2$, $x_i \epsilon \mathfrak{R}_i$ and $D$ any derivation, the mappings $x \rightarrow x_1D \equiv xD_1$ and $x \rightarrow x_2D \equiv xD_2$ are derivations in $\mathfrak{D}_1$ and $\mathfrak{D}_2$ respectively. Since $D=D_1+D_2$, $\mathfrak{D}=\mathfrak{D}_1 \oplus \mathfrak{D}_2$. The isomorphism between $\mathfrak{D}_1$ and the $d$-algebra of $\mathfrak{R}_1$ follows directly from the fact that the transformations of $\mathfrak{D}_1$ induce all the derivations in $\mathfrak{R}_1$ and map $\mathfrak{R}_2$ into 0. Similarly $\mathfrak{D}_2$ is isomorphic to the $d$-algebra of $\mathfrak{R}_2$.

Let $x_1, x_2, \cdots, x_r$ be a basis for $\mathfrak{R}$ over $\mathfrak{F}$ ($\mathfrak{R}=x_1\mathfrak{F}+x_2\mathfrak{F}+\cdots+x_r\mathfrak{F}$) and suppose $x_ix_j=\sum x_\rho \gamma_{\rho ij}$, $\gamma_{\rho ij} \epsilon \mathfrak{F}$. If $D$ is a derivation in $\mathfrak{R}$ and

$$(x_1D, x_2D, \cdots, x_rD) = (x_1, x_2, \cdots, x_r)\Delta, \ \Delta = (\alpha_{ij}), \ \alpha_{ij} \epsilon \mathfrak{F},$$

then the condition $(x_ix_j)D=(x_iD)x_j=x_i(x_jD)$ gives

$$\sum_\rho \alpha_{k\rho}\gamma_{\rho ij} = \sum_\rho \gamma_{k\rho j}\alpha_{\rho i} + \sum_\rho \gamma_{ki\rho}\alpha_{\rho j} \qquad (i, j, k = 1, 2, \cdots, r), \tag{20}$$

a set of $n^3$ linear homogeneous equations for the coordinates $\alpha_{ij}$ of $\Delta$. Con-

† $[\mathfrak{A}, \mathfrak{B}]$ denotes the smallest subspace of $\mathfrak{D}$ containing all the elements $[A, B]$, where $A \epsilon \mathfrak{A}$, $B \epsilon \mathfrak{B}$.

versely if $\Delta$ is any matrix whose coordinates satisfy (20) the linear transforma tion $D$ determined by $\Delta$ satisfies $(x_ix_j)D=(x_iD)x_j+x_i(x_jD)$ for all $i$, $j$ and hence $(xy)D=(xD)y+x(yD)$ for all $x$, $y$, i.e., $D$ is a derivation. Now suppose $\mathfrak{K}$ is a field containing $\mathfrak{F}$ and let $\mathfrak{R}_{\mathfrak{K}}=x_1\mathfrak{K}+x_2\mathfrak{K}+\cdots+x_r\mathfrak{K}$ and $\mathfrak{D}^*$ be the $d$-algebra of $\mathfrak{R}_{\mathfrak{K}}$ (over $\mathfrak{K}$). Evidently the matrix $\Delta$ also determines a derivation $D^*$ in $\mathfrak{R}_{\mathfrak{K}}$. Furthermore since the maximum number of linearly independent solutions of (20) in $\mathfrak{K}$ is the same as in $\mathfrak{F}$ it follows that if $D_1, D_2, \cdots, D_s$ is a basis for $\mathfrak{D}$ then $D_1^*, D_2^*, \cdots, D_s^*$ is a basis for $\mathfrak{D}^*$, and if $[D_i, D_j]=\sum D_\rho\mu_{\rho ij}$, $D_i^p=\sum D_\rho\nu_{\rho i}$ $(\mu_{\rho ij}, \nu_{\rho i}\epsilon\mathfrak{F})$, then $[\Delta_j, \Delta_i]=\sum\Delta_\rho\mu_{\rho ij}$, $\Delta_i^p=\sum\Delta_\rho\nu_{\rho i}$ and hence $[D_i^*, D_j^*]=\sum D_\rho^*\mu_{\rho ij}$, $(D_i^*)^p=\sum D_\rho^*\nu_{\rho i}$. Thus we have proved

THEOREM 5. *If $\mathfrak{D}$ is the d-algebra of $\mathfrak{R}$ then $\mathfrak{D}_{\mathfrak{K}}$ is the d-algebra of $\mathfrak{R}_{\mathfrak{K}}$.*

7. We now consider the $d$-algebra of a semi-simple algebra $\mathfrak{R}$. Since $\mathfrak{R}=\mathfrak{R}_1\oplus\mathfrak{R}_2\oplus\cdots\oplus\mathfrak{R}_t$ where $\mathfrak{R}_i$ are simple and $\mathfrak{R}_i^2=\mathfrak{R}_i$ we have as a consequence of Theorem 4

THEOREM 6. *The d-algebra of a semi-simple algebra is a direct sum of algebras isomorphic to the d-algebras of its simple components.*

We suppose therefore that $\mathfrak{R}$ is simple and let $\mathfrak{C}$ denote its centrum. $\mathfrak{C}$ is an algebraic field over $\mathfrak{F}$ and is characteristic. Let $\mathfrak{C}_0$ be the subfield of constants of $\mathfrak{C}$. Because of (19),

$$[D_1, D_2]c_0 = [D_1c_0, D_2] = [D_1, D_2c_0],$$

where $c_0$ here denotes the multiplication determined by the element $c_0$ of $\mathfrak{C}_0$. Thus $\mathfrak{D}$ as well as $\mathfrak{R}$ may be regarded as an algebra over $\mathfrak{C}_0$. We may therefore suppose that $\mathfrak{C}_0=\mathfrak{F}$, i.e., the only constants in $\mathfrak{C}$ are the multiples of 1 by elements of $\mathfrak{F}$. In this case we shall show that $\mathfrak{C}$ is an inseparable field of a simple type over $\mathfrak{F}$.

Let $c$ be any element of $\mathfrak{C}$ not in $\mathfrak{F}$. Since $cD\epsilon\mathfrak{C}$, we have

$$\begin{aligned} \phi(c)D &\equiv (c^r + c^{r-1}\gamma_1 + \cdots + \gamma_r)D \\ &= (rc^{r-1} + (r-1)c^{r-2}\gamma_1 + \cdots + \gamma_{r-1})(cD) \qquad (21) \\ &= \phi'(c)(cD), \end{aligned}$$

where $\phi'(\lambda)$ is the formal derivative of the polynomial $\phi(\lambda)$ in the polynomial ring $\mathfrak{F}[\lambda]$. If $\phi(c)=0$ is the minimum equation of $c$ and $D$ is chosen so that $cD\neq 0$, (21) gives $\phi'(c)=0$ and hence $\phi'(\lambda)=0$. Thus $c$ is inseparable. In particular if the characteristic $p=0$, $\mathfrak{C}=\mathfrak{F}$ and $\mathfrak{R}$ is a normal simple algebra. If $p\neq 0$, $c^p=\gamma\epsilon\mathfrak{F}$ since $c^pD=pc^{p-1}(cD)=0$ for all $D$.

LEMMA 1. *If $\mathfrak{F}$ is a field of characteristic $p\neq 0$, the polynomial $\lambda^p-\alpha$ is either irreducible or a pth power of a linear factor in $\mathfrak{F}[\lambda]$.*

Suppose $\lambda^p-\alpha$ is reducible and $\phi(\lambda)$ of degree $<p$ is an irreducible factor, say

$$\lambda^p - \alpha = \phi(\lambda)^r\psi(\lambda), \qquad (\phi(\lambda), \psi(\lambda)) = 1.$$

Differentiating we obtain

$$0 = r\phi(\lambda)^{r-1}\phi'(\lambda)\psi(\lambda) + \phi(\lambda)^r\psi'(\lambda).$$

$\psi'(\lambda)\neq 0$ implies that $\phi(\lambda)^r$ divides $r\phi(\lambda)^{r-1}\phi'(\lambda)\psi(\lambda)$ and $\phi(\lambda)$ divides $r\phi'(\lambda)\psi(\lambda)$. Since $\phi'(\lambda)\neq 0$ and $(\phi(\lambda), \psi(\lambda))=1$, it follows that $r=p$ and hence $\psi(\lambda)$ has degree 0 contrary to the assumption $\psi'(\lambda)\neq 0$. Hence $\psi'(\lambda)=0$ or $\psi(\lambda)$ has degree 0 and may be taken to be 1. Then $r\phi(\lambda)^{r-1}\phi'(\lambda)=0$ and so $r=p, \lambda^p-\alpha=\phi(\lambda)^p$.

We return to the consideration of the structure of $\mathfrak{C}$ in the case $p\neq 0$. If $\mathfrak{C}\neq\mathfrak{F}$ choose $c_1\epsilon\mathfrak{C}, \notin\mathfrak{F}$. $c_1^p=\gamma_1\epsilon\mathfrak{F}$. The polynomial $\lambda^p-\gamma_1$ is irreducible in $\mathfrak{F}[\lambda]$. For otherwise $\lambda^p-\gamma_1=(\lambda-\delta)^p$, $\delta\epsilon\mathfrak{F}$ and $\lambda^p-\gamma_1=(\lambda-c_1)^p=(\lambda-\delta)^p$, $c_1=\delta\epsilon\mathfrak{F}$ contrary to the choice of $c_1$. The order of $\mathfrak{F}^1=\mathfrak{F}(c_1)$ over $\mathfrak{F}$ is therefore $p$. If $\mathfrak{C}\neq\mathfrak{F}^1$ choose $c_2\epsilon\mathfrak{C}, \notin\mathfrak{F}^1$. $c_2^p=\gamma_2\epsilon\mathfrak{F}$ and the polynomial $\lambda^p-\gamma_2$ is irreducible in $\mathfrak{F}^1$. Hence $\mathfrak{F}^2=\mathfrak{F}^1(c_2)=\mathfrak{F}(c_1, c_2)$ has order $p$ over $\mathfrak{F}^1$ and consequently $p^2$ over $\mathfrak{F}$. Continuing in this way we prove that $\mathfrak{C}=\mathfrak{F}(c_1, c_2, \cdots, c_m)$, $c_i^p=\gamma_i$ and $\mathfrak{C}$ has order $p^m$ over $\mathfrak{F}$.

8. We determine first the structure of the $d$-algebra $\mathfrak{D}$ of a normal simple algebra $\mathfrak{R}$, i.e., $\mathfrak{C}=\mathfrak{F}$. The following theorem is fundamental.

THEOREM 7. *If $\mathfrak{S}$ is a semi-simple subalgebra of $\mathfrak{R}$, any derivation in $\mathfrak{S}$ may be extended to an inner derivation in $\mathfrak{R}$.*†

By Wedderburn's theorem $\mathfrak{R}$ is the totality of $t\times t$ matrices with coordinates in a normal division algebra $\mathfrak{G}$. In particular the elements $z$ of $\mathfrak{S}$ are such matrices and we have a representation $z\rightarrow z$ of $\mathfrak{S}$ by matrices in $\mathfrak{G}$. We suppose first that this representation is irreducible. If $D$ is any derivation in $\mathfrak{S}$ it is readily verified that

$$z\rightarrow\begin{pmatrix} z & 0\\ 0 & z\end{pmatrix}, \qquad z\rightarrow\begin{pmatrix} z & 0\\ zD & z\end{pmatrix} \tag{22}$$

are also representations of $\mathfrak{S}$ by matrices $(2t\times 2t)$ in $\mathfrak{G}$. Since, as E. Noether‡ has shown, every representation of a semi-simple algebra by matrices in a normal division algebra is completely reducible, any two representations with

† This proof is an extension of an argument communicated to me by R. Brauer.

‡ E. Noether, *Nichtkommutative Algebra*, Mathematische Zeitschrift, vol. 37 (1933), pp. 514–541. The theorem is stated here only for simple algebras but the proof given is also valid for semi-simple algebras.

the same irreducible parts are similar. Thus the two representations in (22) are similar, i.e., there exists a fixed non-singular matrix

$$A = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix}, \qquad a_{ij} \epsilon \mathfrak{R}$$

such that

$$\begin{pmatrix} z & 0 \\ zD & z \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}$$

for all $z \epsilon \mathfrak{S}$. Hence

$$za_{11} = a_{11}z, \qquad za_{12} = a_{12}z, \qquad (zD)a_{11} + za_{21} = a_{21}z,$$
$$(zD)a_{12} + za_{22} = a_{22}z.$$

By Schur's lemma, $a_{11}$ and $a_{12}$ are either 0 or non-singular and both cannot be 0 since $A$ is non-singular. If $a_{11} \neq 0$, we set $a = -a_{21}a_{11}^{-1}$ and if $a_{11} = 0$, we set $a = -a_{22}a_{12}^{-1}$. Then $a \epsilon \mathfrak{R}$ and $zD = [z, a]$ as was to be shown.

If $z \rightarrow z$ is not irreducible it is completely reducible and so there exists a fixed matrix $b$ in $\mathfrak{R}$ such that

$$b^{-1}zb = \begin{pmatrix} z_1 & & & \\ & z_2 & & \\ & & \ddots & \\ & & & z_l \end{pmatrix}$$

and $z \rightarrow z_i$ are irreducible representations of $\mathfrak{S}$. As before

$$z \rightarrow \begin{pmatrix} z_i & 0 \\ (zD)_i & z_i \end{pmatrix}, \qquad z \rightarrow \begin{pmatrix} z_i & 0 \\ 0 & z_i \end{pmatrix}$$

are similar representations of $\mathfrak{S}$ and there exists a matrix $a_i$ such that $(zD)_i = [z_i, a_i]$. Then if

$$a = \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_l \end{pmatrix},$$

$b^{-1}(zD)b = [b^{-1}zb, a]$ and $zD = [z, bab^{-1}]$, $bab^{-1} \epsilon \mathfrak{R}$.

As a special case we have

Theorem 8. *The d-algebra of a normal simple algebra contains only inner derivations.*

Corollary. *If* $\mathfrak{R}$ *is simple,* $\mathfrak{D}(\mathfrak{C}) = \mathfrak{J}$.

If $D \epsilon \mathfrak{D}(\mathfrak{C})$, $(xc)D = (xD)c$ for all $x$ and all $c \epsilon \mathfrak{C}$. Thus $D$ is a derivation of $\mathfrak{N}$ considered as an algebra over $\mathfrak{C}$. By Theorem 8, $D$ is inner and so $\mathfrak{D}(\mathfrak{C}) \subset \mathfrak{J}$. Since $\mathfrak{J} \supset \mathfrak{D}(\mathfrak{C})$ we have equality.

Suppose again that $\mathfrak{N}$ is normal simple. Theorem 8 implies that $\mathfrak{D} = \mathfrak{J} \cong \mathfrak{N}/\mathfrak{F}$ where $\mathfrak{N}$ is the restricted Lie algebra determined by the associative $\mathfrak{N}$ and $\mathfrak{F}$ is the centrum consisting of the multiples of 1. We may extend $\mathfrak{F}$ to the field $\mathfrak{K}$ such that $\mathfrak{N}_{\mathfrak{K}} = \mathfrak{K}_n$ is the complete matrix algebra of order $n^2$ over $\mathfrak{K}$, i.e., $\mathfrak{K}_n$ has a basis $e_{ij}$ $(i, j = 1, 2, \cdots, n)$ such that $e_{ij}e_{kl} = \delta_{jk}e_{il}$. We consider the structure of the Lie algebra $\mathfrak{K}_n$ having basis $e_{ij}$ also and multiplication table

$$[e_{ij}, e_{kl}] = \delta_{jk}e_{il} - \delta_{il}e_{kj}. \tag{23}$$

The centrum of $\mathfrak{K}_n$ is $\mathfrak{K}$ the totality of multiples of $1 = e_{11} + e_{22} + \cdots + e_{nn}$. This is an ideal as is $\mathfrak{K}_n' = [\mathfrak{K}_n, \mathfrak{K}_n]$. From (23) follows that $e_{ts}$, $e_{tt} - e_{ss} \epsilon \mathfrak{K}_n'$ if $t \neq s$. Evidently every element of $\mathfrak{K}_n'$ has trace 0. Conversely if $a = \sum e_{ij}\alpha_{ij}$ and $\mathrm{tr}(a) = \alpha_{11} + \alpha_{22} + \cdots + \alpha_{nn} = 0$,

$$a = (e_{11} - e_{nn})\alpha_{11} + (e_{22} - e_{nn})\alpha_{22} + \cdots + (e_{n-1,n-1} - e_{nn})\alpha_{n-1,n-1} + \sum_{t \neq s} e_{ts}\alpha_{ts} \epsilon \mathfrak{K}_n'$$

and so $\mathfrak{K}_n'$ is the set of matrices of trace 0 and is generated by $e_{11} - e_{nn}$, $e_{22} - e_{nn}, \cdots, e_{n-1,n-1} - e_{nn}$, $e_{ts}$ $(t \neq s)$. These $n^2 - 1$ elements are evidently linearly independent and hence form a basis for $\mathfrak{K}_n'$. Since $(e_{ss} - e_{tt})^p = e_{ss} - e_{tt}$, $e_{st}^p = 0$ if $p \neq 0$ is the characteristic of $\mathfrak{K}$, $\mathfrak{K}_n'$ by (15) contains the $p$th power of every element belonging to it, i.e., $\mathfrak{K}_n'$ is a restricted ideal. $\mathfrak{K}_n'$ contains 1 if and only if $\mathrm{tr}(1) = n \equiv 0 \pmod p$.

Suppose $\mathfrak{B}$ is an ideal $\neq \mathfrak{K}$ in $\mathfrak{K}_n$ and $b = \sum e_{ij}\beta_{ij} \epsilon \mathfrak{B}$, $\notin \mathfrak{K}$. Suppose first $\beta_{uv} \neq 0$ for some pair $u, v, u \neq v$. If $n > 2$, choose $t \neq v, \neq u$ and then $[[[b, e_{vu}], e_{tu}], e_{tt}]\beta_{uv}^{-1} = e_{tu} \epsilon \mathfrak{B}$. If $p \neq 2$, $[[b, e_{vu}], e_{vu}]\ (-2\beta_{uv})^{-1} = e_{vu} \epsilon \mathfrak{B}$. If all $\beta_{uv} = 0$ then $b = e_{11}\beta_{11} + e_{22}\beta_{22} + \cdots + e_{nn}\beta_{nn}$ and since $b \notin \mathfrak{K}$, $\beta_{uu} \neq \beta_{vv}$ for some pair $u \neq v$ and hence $[b, e_{uv}]\ (\beta_{uu} - \beta_{vv})^{-1} = e_{uv} \epsilon \mathfrak{B}$. Thus in any case unless $n = p = 2$ $\mathfrak{B}$ contains an $e_{st}$, $s \neq t$ and since by (23), $[e_{st}, \mathfrak{K}_n] = \mathfrak{K}_n'$, $\mathfrak{B} \supset \mathfrak{K}_n'$. If $\mathfrak{B} \neq \mathfrak{K}_n$, $\mathfrak{B} = \mathfrak{K}_n'$.

Any ideal of $\mathfrak{K}_n/\mathfrak{K}$ the derivation ring of the associative algebra $\mathfrak{K}_n$ has the form $\mathfrak{B}/\mathfrak{K}$ where $\mathfrak{B}$ is an ideal in the Lie algebra $\mathfrak{K}_n$ containing $\mathfrak{K}$. If $p \nmid n$ the only such ideals are $\mathfrak{K}$ and $\mathfrak{K}_n$. Hence $\mathfrak{K}_n/\mathfrak{K}$ is a simple Lie algebra, i.e., has no proper ideals.

If $p \mid n$ and either $p \neq 2$ or $n > 2$, $\mathfrak{K}_n/\mathfrak{K}$ has one proper ideal $\mathfrak{K}_n'/\mathfrak{K}$ and this is restricted. It may be shown by a direct argument similar to the above that $\mathfrak{K}_n'/\mathfrak{K}$ is simple except when $p = n = 2$ and hence the Lie algebra $\mathfrak{K}_n/\mathfrak{K}$ is semi-simple. Since $\mathfrak{K}_n'/\mathfrak{K}$ is the only proper ideal in $\mathfrak{K}_n/\mathfrak{K}$ the latter is not a direct sum of simple ideals.†

THEOREM 9. *If $\mathfrak{N}$ is a normal simple algebra of order $n^2$ and $p \nmid n^2$ then the d-algebra $\mathfrak{D}$ of $\mathfrak{N}$ is simple.*

THEOREM 10. *If $\mathfrak{N}$ is normal simple and $p \mid n^2$ but either $p \neq 2$ or $n > 2$ $\mathfrak{D}$ is semi-simple though not simple.*

To prove these theorems we note that a proper ideal $\mathfrak{B}$ of $\mathfrak{D}$ becomes a proper ideal $\mathfrak{B}_{\mathfrak{K}}$ of $\mathfrak{D}_{\mathfrak{K}}$ the $d$-algebra of $\mathfrak{N}_{\mathfrak{K}}$ when $\mathfrak{F}$ is extended to $\mathfrak{K}$. By choosing $\mathfrak{K}$ so that $\mathfrak{N}_{\mathfrak{K}} = \mathfrak{K}_n$, $\mathfrak{D}_{\mathfrak{K}} \cong \mathfrak{K}_n/\mathfrak{K}$ it follows that $\mathfrak{D}$ has no such ideals if $p \nmid n^2$. If $p \mid n^2$ and either $p \neq 2$ or $n > 2$, $[\mathfrak{D}, \mathfrak{D}]_{\mathfrak{K}} \cong \mathfrak{K}_n'/\mathfrak{K}$ is a proper restricted ideal of $\mathfrak{D}_{\mathfrak{K}}$ and hence $\mathfrak{D}' = [\mathfrak{D}, \mathfrak{D}]$ is a proper restricted ideal in $\mathfrak{D}$. $\mathfrak{D}'$ is simple since $\mathfrak{D}_{\mathfrak{K}}'$ is.

If $n = p = 2$ it is easily seen that $\mathfrak{K}_2/\mathfrak{K}$ and hence $\mathfrak{D}$ is solvable.

9. We consider next the $d$-algebra $\mathfrak{D}$ of the other extreme case, namely, $\mathfrak{N} = \mathfrak{C} = \mathfrak{F}(c_1, c_2, \cdots, c_m)$ where $c_i^p = \gamma_i$ and the order of $\mathfrak{N}$ over $\mathfrak{F}$ is $p^m$, $p \neq 0$. Let $D$ be any element of $\mathfrak{D}$ and consider the correspondence $D \rightarrow (c_1D, c_2D, \cdots, c_mD)$ mapping $\mathfrak{D}$ on the space $\mathfrak{N}^{(m)}$ of ordered $m$-tuples of elements of $\mathfrak{N}$. This correspondence is linear relative to $\mathfrak{F}$ and since $c_1D = c_2D = \cdots = c_mD = 0$ implies that $D = 0$ it is $(1-1)$. Moreover if $(d_1, d_2, \cdots, d_m)$ is an arbitrary element of $\mathfrak{N}^{(m)}$ there is a $D \epsilon \mathfrak{D}$ such that $c_iD = d_i$. For $\mathfrak{N} \cong \mathfrak{F}[\lambda_1, \lambda_2, \cdots, \lambda_m]/\mathfrak{P}$ where $\mathfrak{P}$ is the ideal having the basis $\lambda_1^p - \gamma_1$, $\lambda_2^p - \gamma_2, \cdots, \lambda_m^p - \gamma_m$. If $d_1(\lambda_1, \cdots, \lambda_m)$, $d_2(\lambda_1, \cdots, \lambda_m), \cdots$, $d_m(\lambda_1, \cdots, \lambda_m)$ are arbitrary polynomials, then the transformation $D$ defined by

$$c(\lambda_1, \lambda_2, \cdots, \lambda_m)D = \sum_i \frac{\partial c(\lambda_1, \lambda_2, \cdots, \lambda_m)}{\partial \lambda_i} d_i(\lambda_1, \lambda_2, \cdots, \lambda_m)$$

is easily verified to be a derivation in $\mathfrak{F}[\lambda_1, \lambda_2, \cdots, \lambda_m]$. If $z(\lambda_1, \lambda_2, \cdots, \lambda_m) \epsilon \mathfrak{P}$ then $zD \epsilon \mathfrak{P}$ also. It follows that $D$ induces a derivation in $\mathfrak{F}[\lambda_1, \lambda_2, \cdots, \lambda_m]/\mathfrak{P}$, i.e., in $\mathfrak{N}$ and since $d_i(\lambda_1, \cdots, \lambda_m)$ were arbitrary, $D$ may be chosen so that $c_iD = d_i$. We have therefore established an isomorphism between $\mathfrak{D}$ and $\mathfrak{N}^{(m)}$ considered as vector spaces over $\mathfrak{F}$. The order of $\mathfrak{N}^{(m)}$ is $mp^m$ and hence the order of $\mathfrak{D}$ is $mp^m$ also.

LEMMA 2. *If $\mathfrak{N}$ is any commutative field, $D$ a derivation in it, and $\mathfrak{F}$ the subfield of D-constants, a necessary and sufficient condition that the elements $y_1, y_2, \cdots, y_r$ be linearly dependent over $\mathfrak{F}$ is that the Wronskian*

† If $p=0$ a fundamental theorem due to E. Cartan, *Thèse*, Paris, 1894, states that a semi-simple Lie algebra is a direct sum of simple algebras. The algebras $\mathfrak{K}_n/\mathfrak{K}$ for $p \mid n$ show that this does not hold for $p \neq 0$. A second example of this type will be given below.

$$\begin{vmatrix} y_1 & y_2 & \cdots & y_r \\ y_1D & y_2D & \cdots & y_rD \\ \cdot & \cdot & \cdots & \cdot \\ y_1D^{r-1} & y_2D^{r-1} & \cdots & y_rD^{r-1} \end{vmatrix} = 0.$$

The usual proof of this result for analytic functions is valid here.† As a consequence we have

LEMMA 3. *The differential equation* $y(D^r+D^{r-1}a_1+\cdots+a_r)=0$, $a_i\epsilon\mathfrak{R}$, *has at most r solutions* $y_1, y_2, \cdots, y_r$ *in* $\mathfrak{R}$ *linearly independent over* $\mathfrak{F}$.

It has been shown by R. Baer‡ that if $\mathfrak{R}$ is a field of the type $\mathfrak{F}(c_1,c_2,\cdots,c_m)$, $c_i^p=\gamma_i\epsilon\mathfrak{F}$, there exists a derivation $D$ such that the $D$-constants are precisely the elements of $\mathfrak{F}$. Let $D$ denote a fixed derivation of this type and set $cD=c'$ for any $c\epsilon\mathfrak{R}$. $D^p$, $D^{p^2}, \cdots$ are derivations and since $\mathfrak{R}$ is commutative the transformation $Da_0+D^pa_1+\cdots+D^{p^{m-1}}a_{m-1}$ is a derivation for arbitrary right multiplication $a_i$ $(=a_{ir})$ in $\mathfrak{R}$. If $Da_0+D^pa_1+\cdots+D^{p^{m-1}}a_{m-1}=0$, i.e., $y(Da_0+D^pa_1+\cdots+D^{p^{m-1}}a_{m-1})=0$ for all $y$ in $\mathfrak{R}$, it follows by Lemma 3 and the fact that $\mathfrak{F}$ is the set of $D$-constants that all $a_i=0$. Thus as the $a_i$ vary in $\mathfrak{R}$ we obtain in this way $mp^m$ linearly independent (over $\mathfrak{F}$) derivations and hence the complete algebra $\mathfrak{D}$. We shall therefore call $D$ a *generator* of $\mathfrak{D}$. Since $D^{p^m}$ is a derivation we have

$$D^{p^m} = D^{p^{m-1}}b_{m-1} + D^{p^{m-2}}b_{m-2} + \cdots + Db_0.$$

Taking commutators with $D$ we have by (19),

$$0 = D^{p^{m-1}}b'_{m-1} + D^{p^{m-2}}b'_{m-2} + \cdots + Db'_0,$$

and hence $b_i'=0$, i.e., $b_i=\beta_i\epsilon\mathfrak{F}$, and

$$D^{p^m} = D^{p^{m-1}}\beta_{m-1} + D^{p^{m-2}}\beta_{m-2} + \cdots + D\beta_0. \tag{24}$$

As a consequence of (19), we note also

$$[D^{p^k}a, D^{p^j}b] = D^{p^k}a^{(p^j)}b - D^{p^j}b^{(p^k)}a, \tag{25}$$

where $a^{(p^j)}=aD^{p^j}$. If $E=Da\neq 0$ then the $E$-constants are the same as the $D$-constants since the multiplication $a$ is non-singular and hence $E$ is a generator of $\mathfrak{D}$ also.

THEOREM 11. *The d-algebra of the field* $\mathfrak{R}=\mathfrak{F}(c_1, c_2, \cdots, c_m)$, $c_i^p=\gamma_i$ *is simple except when* $p=2$, $m=1$.

---

† See, for example, T. Chaundy, *Differential Calculus*, Oxford, 1935, p. 106.

‡ R. Baer, *Algebraische Theorie der differentiierbaren Funktionenkörper*. I, Sitzungsberichte, Heidelberger Akademie, 1927, pp. 15–32.

Let $\mathfrak{B}\neq 0$ be an ideal in $\mathfrak{D}$ and $E=Db_0+D^pb_1+\cdots+D^{p^j}b_j$, $b_j\neq 0, j<m$, belong to $\mathfrak{B}$. We call $j$ the *length* of $E$ and suppose $E$ chosen in $\mathfrak{B}$ so that $j$ is minimal. We assert that $j=0$. For if $j>0$ we may suppose $b_j=1$. This is evident if $b_j'=0$ or $b_j=\beta_j\epsilon\mathfrak{F}$ and if $b_j'\neq 0$, $[E, D(b_j')^{-1}]=Db_0^*+D^pb_1^*+\cdots+D^{p^j}\epsilon\mathfrak{B}$. But if $E=Db_0+D^pb_1+\cdots+D^{p^{j-1}}b_{j-1}+D^{p^j}$ then

$$[E, Da] = D(ab_0' - a'b_0 - \cdots - a^{(p^{j-1})}b_{j-1} - a^{(p^j)}) + D^pab_1' + \cdots + D^{p^{j-1}}ab_{j-1}'.$$

$[E, Da]$ has length $<j$ and may be chosen $\neq 0$ since by Lemma 3 $a$ may be chosen so that $ab_0'-a'b_0-\cdots-a^{(p^{j-1})}b_{j-1}-a^{(p^j)}\neq 0$. This contradicts the minimality of $j$ in $\mathfrak{B}$ and shows that $E=Db_0$, $b_0\neq 0$. Since $E$ as well as $D$ is a generator of $\mathfrak{D}$, by changing the notation we may suppose that $\mathfrak{B}\supset D$. Then $\mathfrak{B}\supset[Da, D]=Da'$ also. Since the null space of the linear transformation $D$ in $\mathfrak{R}$ has order 1, the order of $\mathfrak{R}'$ the set of all $a'$ is $p^m-1$ over $\mathfrak{F}$. If $1\notin\mathfrak{R}'$ the smallest space containing all $a'$ and 1 is $\mathfrak{R}$. Since $\mathfrak{B}\supset D$ and $Da'$, $\mathfrak{B}$ will then contain $Da$ for all $a$ in $\mathfrak{R}$. Also if $p\neq 2$, $\mathfrak{B}\supset\frac{1}{2}[Da', Db]+\frac{1}{2}[Da'b, D]=Da''b$ and since $a''$ is not identically 0 and $b$ is arbitrary, $\mathfrak{B}\supset Da$ for all $a$. Suppose finally that $p=2$ and $\mathfrak{R}'\supset 1$, say $u'=1$. Here $\mathfrak{B}\supset[[D^2a, D], Db]=D^2a''b+Da'b''$. If $m>1$, $a''$ is not identically 0 and hence $b$ may be chosen so that $a''b=u$. Set $a'b''=v$. $\mathfrak{B}\supset[D^2u+Dv, Da]+D(va+ua'+a)'=D^2a$ and $[D^2a, Db]+D^2a'b=Dab''$. Thus in any case unless $p=2$, $m=1$, $\mathfrak{B}\supset Da$ for all $a$ and since $[D^{p^k}b, Da]+Da^{(p^k)}b=D^{p^k}b'a$, $\mathfrak{B}\supset$ all $D^{p^k}a$ so that $\mathfrak{B}=\mathfrak{D}$.

If $p=2$, $m=1$, $\mathfrak{D}$ has order 2 and hence is solvable. In all other cases the algebras $\mathfrak{D}$ are simple algebras which, like inseparable fields, have no counterparts for $p=0$.

If $E$ is any derivation, the totality of expressions $E^{p^k}a_0+E^{p^{k-1}}a_1+\cdots+Ea_{\mathfrak{K}}$, $a_i\epsilon\mathfrak{R}$ is, by virtue of (15) and (19), a restricted $\mathfrak{R}$-($=\mathfrak{E}$-)subalgebra $\mathfrak{E}$ of $\mathfrak{D}$. Conversely if $\mathfrak{E}$ is any restricted $\mathfrak{R}$-subalgebra of $\mathfrak{D}$, $\mathfrak{E}$ is generated in this fashion. To prove this let $E=D^{p^e}g_0+D^{p^{e-1}}g_1+\cdots+Dg_e$, $g_0\neq 0$, be an element of smallest length in $\mathfrak{E}$. Since $\mathfrak{E}$ is an $\mathfrak{R}$-algebra we may suppose that $g_0=1$ and then $E=D^{p^e}+D^{p^{e-1}}g_1+\cdots+Dg_e$ is unique. If $F=D^{p^f}h_0+D^{p^{f-1}}h_1+\cdots+Dh_f\epsilon\mathfrak{E}$, $f\geqq e$ and

$$F_1 = F - E^{p^{f-e}}h_0 = D^{p^{f-1}}k_0 + \cdots + Dk_{f-1}$$

by (15) and (25). $F_1$ has length $\leqq f-1$ and belongs to $\mathfrak{E}$. Repeating this process we obtain an expression for $F$ of the form $E^{p^{f-e}}a_0+\cdots+Ea_{f-e}$.

If as in I we denote the elements of $\mathfrak{R}$ which are constants for all the derivations in $\mathfrak{E}$ by $\mathfrak{R}(\mathfrak{E})$ it is clear that $\mathfrak{R}(\mathfrak{E})$ coincides with the subfield $\mathfrak{S}$ of $E$-constants. On the other hand if $E$ is any derivation, $\mathfrak{S}$ the set of $E$-constants, then the argument at the beginning of this section shows that $E$ generates the $d$-algebra $\mathfrak{D}(\mathfrak{S})$ of $\mathfrak{R}$ considered as a field over $\mathfrak{S}$. Hence $\mathfrak{D}(\mathfrak{S}) = \mathfrak{C}$, i.e.,

$$\mathfrak{D}(\mathfrak{R}(\mathfrak{C})) = \mathfrak{C}.$$

If $\mathfrak{S}$ is any subfield of $\mathfrak{R}$, $\mathfrak{D}(\mathfrak{S})$ contains an element $E$ such that the $E$-constants are precisely $\mathfrak{S}$. Hence $\mathfrak{R}(\mathfrak{D}(\mathfrak{S}))$ cannot be larger than $\mathfrak{S}$ and so

$$\mathfrak{R}(\mathfrak{D}(\mathfrak{S})) = \mathfrak{S}.$$

We have therefore proved

THEOREM 12. *There is a* (1–1) *correspondence between the subfields* $\mathfrak{S}$ *of* $\mathfrak{R}$ *containing* $\mathfrak{F}$ *and the restricted* $\mathfrak{R}$*-subalgebras* $\mathfrak{C}$ *of the d-algebra* $\mathfrak{D}$ *of* $\mathfrak{R}$ *over* $\mathfrak{F}$. *The correspondence is given by either* $\mathfrak{C} = \mathfrak{D}(\mathfrak{S})$ *or* $\mathfrak{S} = \mathfrak{R}(\mathfrak{C})$.

10. We now suppose that $\mathfrak{R}$ is simple and that $\mathfrak{R} \supset \mathfrak{C} \supset \mathfrak{F}$ where $\mathfrak{C} = \mathfrak{F}(c_1, c_2, \cdots, c_m)$, $c_i^p = \gamma_i$ and $p \neq 0$. Let $\mathfrak{D}$ denote the $d$-algebra of $\mathfrak{R}$ over $\mathfrak{F}$ and $\mathfrak{E}$ that of $\mathfrak{C}$ over $\mathfrak{F}$. If $D \epsilon \mathfrak{D}$, $D$ induces a derivation in $\mathfrak{C}$ and hence $\mathfrak{D}$ is homomorphic with a subalgebra $\mathfrak{E}_1$ of $\mathfrak{E}$. Since $\mathfrak{D}(\mathfrak{C})$ is the set of elements corresponding to 0 in this homomorphism, we have $\mathfrak{E}_1 \cong \mathfrak{D}/\mathfrak{D}(\mathfrak{C})$. But by the corollary to Theorem 8, $\mathfrak{D}(\mathfrak{C}) = \mathfrak{J}$ and hence $\mathfrak{E}_1 \cong \mathfrak{D}/\mathfrak{J}$. We wish to show that $\mathfrak{E}_1 = \mathfrak{E}$.

$\mathfrak{R}$ may be regarded as a normal simple algebra over $\mathfrak{C}$ and there exists a separable field $\mathfrak{C}(s)$ over $\mathfrak{C}$ such that $\mathfrak{R} \times \mathfrak{C}(s) = \mathfrak{C}(s)_n$ the matrix algebra of order $n^2$ with elements in $\mathfrak{C}(s)$. As has been shown by Albert† the separable extension $\mathfrak{C}(s)$ of the inseparable field $\mathfrak{C}$ has the form $\mathfrak{K}(c_1, \cdots, c_m) = \mathfrak{C}_{\mathfrak{K}}$ where $\mathfrak{K}$ is a separable field over $\mathfrak{F}$. Now consider $\mathfrak{R}_{\mathfrak{K}}$. The centrum of this algebra is $\mathfrak{C}_{\mathfrak{K}} = \mathfrak{C}(s)$ and if $x_1, x_2, \cdots, x_{n^2}$ form a basis of $\mathfrak{R}$ over $\mathfrak{C}$ they are also a basis for $\mathfrak{R}_{\mathfrak{K}}$ over $\mathfrak{C}_{\mathfrak{K}} = \mathfrak{C}(s)$. It follows that $\mathfrak{R}_{\mathfrak{K}} = \mathfrak{R} \times \mathfrak{C}(s) = \mathfrak{C}(s)_n = (\mathfrak{C}_{\mathfrak{K}})_n$.

The $d$-algebra of $\mathfrak{R}_{\mathfrak{K}}$ is $\mathfrak{D}_{\mathfrak{K}}$ and the ideal of inner derivations of $\mathfrak{D}_{\mathfrak{K}}$ is $\mathfrak{J}_{\mathfrak{K}}$. If $E^*$ is any derivation in $\mathfrak{C}_{\mathfrak{K}}$ over $\mathfrak{K}$, the correspondence $\sum e_{ij} c_{ij}^* \rightarrow \sum e_{ij}(c_{ij}^* E^*)$, $c_{ij}^* \epsilon \mathfrak{C}_{\mathfrak{K}}$ is readily verified to be a derivation in $\mathfrak{R}_{\mathfrak{K}}$ inducing $E^*$ in $\mathfrak{C}_{\mathfrak{K}}$. Hence $\mathfrak{D}_{\mathfrak{K}}/\mathfrak{J}_{\mathfrak{K}}$ is isomorphic to the complete $d$-algebra of $\mathfrak{C}_{\mathfrak{K}}$ and so has order $mp^m$ over $\mathfrak{K}$. Since $\mathfrak{D}_{\mathfrak{K}}/\mathfrak{J}_{\mathfrak{K}} \cong (\mathfrak{D}/\mathfrak{J})_{\mathfrak{K}}$, $\mathfrak{D}/\mathfrak{J}$ has order $mp^m$ over $\mathfrak{F}$. Comparing orders we have $\mathfrak{E} \cong \mathfrak{D}/\mathfrak{J}$.

THEOREM 13. *Suppose* $\mathfrak{R}$ *is a simple algebra of order* $n^2$ *over its centrum* $\mathfrak{C} = \mathfrak{F}(c_1, c_2, \cdots, c_m)$, $c_i^p = \gamma_i$, $p \neq 0$. *Then the d-algebra of* $\mathfrak{D}$ *over* $\mathfrak{R}$ *is semi-simple unless* $p = 2$ *and either* $n \leqq 2$ *or* $m = 1$.

Let $\mathfrak{B}$ be a solvable ideal in $\mathfrak{D}$. $\mathfrak{B} + \mathfrak{J}$‡ is an ideal and $(\mathfrak{B} + \mathfrak{J})/\mathfrak{J}$ is a solva-

† A. A. Albert, *Simple algebras of degree $p^e$ over a centrum of characteristic $p$*, these Transactions, vol. 40 (1936), p. 113.

‡ $\mathfrak{B} + \mathfrak{J}$ denotes the smallest space containing $\mathfrak{B}$ and $\mathfrak{J}$.

ble ideal in $\mathfrak{D}/\mathfrak{I}\cong\mathfrak{C}$. But by Theorem 11, $\mathfrak{C}$ is simple. Hence $(\mathfrak{B}+\mathfrak{I})/\mathfrak{I}=0$ or $\mathfrak{B}+\mathfrak{I}=\mathfrak{I}$ and $\mathfrak{B}\subset\mathfrak{I}$. However, by Theorem 10, $\mathfrak{I}$ is semi-simple and so $\mathfrak{B}=0$.

$\mathfrak{D}$ is not a direct sum of $\mathfrak{I}$ and a second ideal. For we have seen (§5) that the elements commutative with all elements in $\mathfrak{I}$ are those mapping $\mathfrak{R}$ into $\mathfrak{C}$. If $F$ is such an element, then $F^*$ the extension of $F$ maps $\mathfrak{R}_{\mathfrak{K}}$ into $\mathfrak{C}_{\mathfrak{K}}$ (cf. Theorem 5). If $e_{ij}F^*=c_{ij}^*\epsilon\mathfrak{C}_{\mathfrak{K}}$, it follows from $e_{ij}e_{kl}=\delta_{jk}e_{il}$ that $c_{ij}^*=0$. Hence $(e_{ij}c^*)F^*=e_{ij}(c^*F^*)$ for $c^*\epsilon\mathfrak{C}_{\mathfrak{K}}$. If this belongs to $\mathfrak{C}_{\mathfrak{K}}$ we must have $c^*F^*=0$. Thus $F^*=0$, $F=0$, and $\mathfrak{D}$ is not a direct sum.

## III. Theory of $D$-fields

11. In this part we propose to study $\mathfrak{R}=\mathfrak{F}(c_1, c_2, \cdots, c_m)$, $c_i^p=\gamma_i$, $p\neq 0$ relative to the fixed derivation $D$ and shall obtain several analogues of theorems on automorphisms of cyclic fields. Without loss of generality we may assume that $\mathfrak{F}$ is the field of $D$-constants and hence $D$ is a generator of the $d$-algebra of $\mathfrak{R}$. We have seen that $D$ satisfies (24),

$$D^{p^m} = D^{p^{m-1}}\beta_1 + D^{p^{m-2}}\beta_2 + \cdots + D\beta_m,$$

and no equation of lower degree of the form $D^r+D^{r-1}a_1+\cdots+a_r$, $a_i\epsilon\mathfrak{R}$.

Suppose $y_1, y_2, \cdots, y_{p^m}$ is a basis for $\mathfrak{R}$ and

$$(y_1D, y_2D, \cdots, y_{p^m}D) = (y_1, y_2, \cdots, y_{p^m})\Delta \qquad \Delta = (\alpha_{ij}).$$

If $f(\lambda)$ is the characteristic function $|\lambda 1-\Delta|$, then by the Hamilton-Cayley theorem, $f(D)=0$. Since the degree of $f(\lambda)$ is $p^m$ we have

$$f(\lambda) = |\lambda 1 - \Delta| = \lambda^{p^m} - \lambda^{p^{m-1}}\beta_1 - \cdots - \lambda\beta_m. \tag{26}$$

Since the characteristic and minimum equations of $A$ are identical, $A$ is similar to

$$B = \begin{pmatrix} 0 & & & & & & & 0 \\ 1 & & & & & & & \beta_m \\ & 1 & & & & & & 0 \\ & & \ddots & & & & & \vdots \\ & & & & & & & \beta_1 \\ & & & & \ddots & & & 0 \\ & & & & & & & \vdots \\ & & & & & & 1 & 0 \end{pmatrix}.$$

It follows that $\mathfrak{R}$ has a basis of the form $z, zD, zD^2, \cdots, zD^{p^m-1}$, i.e., $\mathfrak{R}$ is a cyclic space relative to the linear transformation $D$.†

A polynomial of the form $\lambda^{p^e}+\lambda^{p^{e-1}}\rho_1+\cdots+\lambda\rho_e$ will be called a *p-polynomial*.‡ A subfield $\mathfrak{S}$ of $\mathfrak{R}$ containing $\mathfrak{F}$ and $vD$ for every $v$ in $\mathfrak{S}$ will be called a *D-subfield* of $\mathfrak{R}$. Thus $\mathfrak{S}$ is a space invariant under the transformation $D$.

THEOREM 14. *There is a* (1–1) *correspondence between the D-subfields of* $\mathfrak{R}$ *and the p-polynomial factors of* $f(\lambda)$.

Any subspace $\mathfrak{S}$ of $\mathfrak{R}$ is cyclic with generator $w$. If $g(\lambda)$ is a polynomial of least degree such that $wg(D)=0$ then $g(\lambda)$ is the minimum function of $D$ acting in $\mathfrak{S}$ and the order of $\mathfrak{S}=$degree of $g(\lambda)$. $g(\lambda)$ is therefore uniquely determined by $\mathfrak{S}$ and is a factor of $f(\lambda)$. For if $h(\lambda)=f(\lambda)q(\lambda)+g(\lambda)r(\lambda)=(g(\lambda), f(\lambda))$ then $wh(D)=0$ and since $g(\lambda)$ is minimal, $g(\lambda)=h(\lambda)$. Conversely if $g(\lambda)$ is a factor of $f(\lambda)$, $f(\lambda)=g(\lambda)k(\lambda)$, the vectors $v$ such that $vg(D)=0$ form an invariant subspace $\mathfrak{S}$. $\mathfrak{S}\supset zk(D)$, $zd(D)D,\cdots$ if $z$ is a generator of $\mathfrak{R}$, and if the degree of $g(\lambda)$ is $r$, $zk(D), zk(D)D,\cdots, zk(D)D^{r-1}$ are linearly independent. Hence the order of $\mathfrak{S}$ is $\geqq r$. On the other hand the minimum function of $D$ in $\mathfrak{S}$ is $g(\lambda)$ so that order of $\mathfrak{S}$ is $r$, $\mathfrak{S}=(zk(D), zk(D)D,\cdots)$. Thus we have a (1–1) correspondence between the invariant subspaces $\mathfrak{S}$ of $\mathfrak{R}$ and the factors $g(\lambda)$ of $f(\lambda)$. If $\mathfrak{S}$ is a field, $D$ is a generator of the $d$-algebra of $\mathfrak{S}$ over $\mathfrak{F}$ and hence $g(\lambda)$ is a $p$-polynomial. Conversely if $g(\lambda)$ is a $p$-polynomial and $v_1, v_2\epsilon\mathfrak{S}$, i.e., $v_1g(D)=v_2g(D)=0$, then since $g(D)$ is a derivation, $v_1v_2g(D)=(v_1g(D))v_2+v_1(v_2g(D))=0$ so that $\mathfrak{S}$ is closed under multiplication and hence is a $D$-subfield of $\mathfrak{R}$.

Suppose $g(\lambda)=\lambda^{p^e}+\lambda^{p^{e-1}}\rho_1+\cdots+\lambda\rho_e$, $h(\lambda)=\lambda^{p^f}+\lambda^{p^{f-1}}\sigma_1+\cdots+\lambda\sigma_f$ and $e\leqq f$. Then $g(\lambda)-h(\lambda)^{p^{e-f}}=\lambda^{p^{e-1}}\tau_1+\cdots+\lambda\tau_{e-1}$. By repeating this process we may express $g(\lambda)$ in the form

$$g(\lambda) = h(\lambda)^{p^{e-f}} + h(\lambda)^{p^{e-f-1}}\omega_1 + \cdots + h(\lambda)\omega_{e-f} + r(\lambda) \qquad (\omega_1 = \tau_1),$$

where $r(\lambda)$ is a $p$-polynomial of degree $<p^f$. Since $r(\lambda)$ is the remainder obtained by dividing $g(\lambda)$ by $h(\lambda)$, by continuing the euclid algorithm we find that $(g(\lambda), h(\lambda))$ *is a p-polynomial.*

If $k(\lambda)$ is any polynomial (coefficients in $\mathfrak{F}$), then

$$\lambda^{p^j} = k(\lambda)q_j(\lambda) + s_j(\lambda) \qquad (j = 0, 1, 2, \cdots),$$

where degree $s_j(\lambda)<$degree $k(\lambda)=r$. Since there are at most $r$ independent polynomials of degree $<r$ there exist elements, $\alpha_0, \alpha_1, \cdots, \alpha_r$ not all 0 such that $s_r(\lambda)\alpha_0+s_{r-1}(\lambda)\alpha_1+\cdots+s_0(\lambda)\alpha_r=0$ and hence

† For a discussion of cyclic spaces see Jacobson, *Pseudo-linear transformations*, Annals of Mathematics, vol. 38 (1937), p. 496.

‡ This term is due to O. Ore, *On a special class of polynomials*, these Transactions, vol. 35 (1933), p. 560.

$$h(\lambda) = \lambda^{p^r}\alpha_0 + \lambda^{p^{r-1}}\alpha_1 + \cdots + \lambda\alpha_r = k(\lambda)\sum q_j(\lambda)\alpha_j,$$

i.e., *any polynomial is a factor of some $p$-polynomial.*† Since the h.c.f. of $p$-polynomials is a $p$-polynomial, the $p$-polynomial of least degree divisible by $k(\lambda)$ is unique. We denote it by $\{k(\lambda)\}$.

Now suppose $\mathfrak{S}$ is a subspace of $\mathfrak{R}$ invariant under $D$ and $k(\lambda)$ is the minimum function of $D$ in $\mathfrak{S}$. Let $\{\mathfrak{S}\}$ denote the enveloping field of $\mathfrak{S}$. $\{\mathfrak{S}\}$ is a $D$-field and $D$ has minimum function $\{k(\lambda)\}$ in $\{\mathfrak{S}\}$. If $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are invariant subspaces, $k_1(\lambda)$, $k_2(\lambda)$ the corresponding minimum functions, then $\mathfrak{S}_1+\mathfrak{S}_2$ and $\mathfrak{S}_1 \cap \mathfrak{S}_2$ are invariant and the associated functions are respectively $[k_1(\lambda), k_2(\lambda)]$ and $(k_1(\lambda), k_2(\lambda))$.

12. Let $\mathfrak{M}$ denote the algebra of linear transformations generated by $D$ and the multiplications of $\mathfrak{R}$. Since $D^{p^m-1}a_1+D^{p^m-2}a_2+\cdots+a_{p^m}=0$ implies all $a_i=0$, $\mathfrak{M}$ has order $p^{2m}$ over $\mathfrak{F}$ and hence is isomorphic to $\mathfrak{F}_{p^m}$ the algebra of all $p^m\times p^m$ matrices in $\mathfrak{F}$. The multiplication of the elements of $\mathfrak{M}$ may be ascertained from the multiplications of the elements of $\mathfrak{R}$ and the rules

$$(27) \qquad \text{(a) } aD = Da + a', \qquad \text{(b) } f(D) = D^{p^m} - D^{p^{m-1}}\beta_1 - \cdots - D\beta_m = 0.$$

Let $c$ be an arbitrary element of $\mathfrak{R}$ and consider the powers of $D_1=D+c$. From (27a) we obtain by induction

$$(28) \qquad D_1^k = (D+c)^k = D^k + C_{k,1}D^{k-1}V_1(c) + C_{k,2}D^{k-2}V_2(c) + \cdots + V_k(c),$$

where

$$(29) \qquad V_1(c) = c, \qquad V_j(c) = V_{j-1}(c)' + V_{j-1}(c)c.$$

For $k=p^i$, (28) specializes to

$$(30) \qquad D_1^{p^i} = (D+c)^{p^i} = D^{p^i} + V_{p^i}(c).$$

$D_1$ evidently satisfies (27a), and from (30) and (27b) we have as the condition that $D_1$ also satisfies (27b),

$$(31) \qquad V(c) = V_{p^m}(c) - V_{p^{m-1}}(c)\beta_1 - \cdots - V_1(c)\beta_m = 0.$$

On the other hand if $D_1$ satisfies (27) the correspondence $D\to D_1$, $a\to a$ defines an automorphism of $\mathfrak{M}$ and conversely. Since every automorphism of $\mathfrak{M}\cong\mathfrak{F}_{p^m}$ is inner there exists an element $B\in\mathfrak{M}$ such that

$$B^{-1}aB = a, \qquad B^{-1}D_1B = D$$

for all $a$ in $\mathfrak{R}$. Since $\mathfrak{R}$ has maximum order for a commutative subfield of $\mathfrak{M}$, $B=b\in\mathfrak{R}$ and hence the second condition gives

† This result is due to Ore, loc. cit., p. 581.

$$c = b^{-1}b', \tag{32}$$

i.e., $c$ is a *logarithmic derivative*. We have therefore proved

THEOREM 15. *A necessary and sufficient condition that $c \epsilon \mathfrak{R}$ be a logarithmic derivative is that* (31) *hold.*

This is an analogue of Hilbert's theorem on the elements of norm 1 in a cyclic field. $V(c)$ takes the part of the norm and derivation that of the generating automorphism of the cyclic field.

We denote the set of logarithmic derivatives by $\mathfrak{L}$. Since $-b'/b = (b^{-1})'/(b^{-1})$ and $b'/b + c'/c = (bc)'/bc$, $\mathfrak{L}$ is a group under addition and the correspondence $b \rightarrow b'/b$ establishes a homomorphism between the multiplicative group of $\mathfrak{R}$ and $\mathfrak{L}$. The elements corresponding to 0 here are those of $\mathfrak{F}$. Hence $\mathfrak{L} \cong \mathfrak{R}/\mathfrak{F}$.

By means of the recursion formula (29) we may prove by induction

$$V_j(c) = \sum_{i=1}^{j} P_{ij}, \qquad P_{ij} = \sum \frac{j!}{\alpha!\beta!\cdots}\left(\frac{c}{1!}\right)^{\alpha}\left(\frac{c'}{2!}\right)^{\beta}\cdots, \tag{33}$$

where the summation in $P_{ij}$ is extended over all non-negative integers such that

$$\alpha + \beta + \gamma + \cdots = i, \qquad \alpha + 2\beta + 3\gamma + \cdots = j.$$

(The coefficients in $P_{ij}$ are understood to be the integers obtained by cancelling the common factors in $j!/(\alpha!\beta!\cdots)(1!)^{\alpha}(2!)^{\beta}\cdots$.) By (33) it is easily seen that $V_p(c) = c^p + c^{(p-1)}$. Since

$$D_1^{p^j} = (D_1^{p^{j-1}})^p = (D^{p^{j-1}} + V_{p^{j-1}}(c))^p = D^{p^j} + V_{p^j}(c),$$

we have

$$V_{p^j}(c) = (V_{p^{j-1}}(c))^p + (V_{p^{j-1}}(c))^{(p^j - p^{j-1})}, \tag{34}$$

and hence

$$V_{p^j}(c) = c^{p^j} + (c^{(p-1)})^{p^{j-1}} + (c^{(p^2-1)})^{p^{j-2}} + \cdots + c^{(p^j-1)}. \tag{35}$$

Then $V_{p^j}(c)' = c^{(p^j)}$ and so by (27b), $(V(c))' = 0$, i.e., $V(c) \epsilon \mathfrak{F}$ *for any $c$ in* $\mathfrak{R}$. Also by (35), or more directly by (30),

$$V(b + c) = V(b) + V(c). \tag{36}$$

UNIVERSITY OF CHICAGO,
CHICAGO, ILL.