SIMPLE ALGEBRAS AND DERIVATIONS(1)

BY
KLAUS HOECHSMANN

Introduction. In the theory of crossed products, a central simple algebra is constructed from a given normal splitting field by extending the multiplicative group of that field by its Galois group and embedding the result into a ring. An analogue of this theory for purely inseparable fields of exponent 1 was worked out by Hochschild [2]: Given an extension E of the ground field K of characteristic $p > 0$ such that $E^p \subset K$, one considers certain "regular" extensions of E—regarded as an abelian restricted Lie algebra—by the restricted Lie algebra of its K-derivations; an appropriate associative embedding of the resulting Lie-algebras yields central simple K-algebras of dimension $(E:K)^2$ split by E. This procedure is generalized in [3], where instead of E some central simple E-algebra A is extended by the derivation algebra of E/K. The present paper concerns itself with a simpler, more explicit version of this construction, a version which, for the case $A = E$, was already given by Jacobson [5] in 1937. Its transparency is due to the use of only one derivation instead of a whole algebra of them. Thus it is essentially "cyclic" and independent of the Lie structure of the set of K-derivations of E. On the other hand, it necessarily has the disadvantage of not being canonical.

The use of derivations in the study of algebras goes back to Teichmüller [7]. There, however, only the simplest case ($E = K(z)$, $z^p \in K$) is treated, and the derivations are mainly used to deduce the existence of normal fields in an algebra from the existence of purely inseparable ones, just as in §6 below.

In Jacobson's short paper [5], derivations play a role more obviously analogous to that of automorphisms in the theory of cyclic algebras. After Hochschild's work [2; 3], the subject is again touched by Amitsur [1], who studied in detail the ring of "differential polynomials" from which the algebras considered here are obtained as residue-class rings. Our aim is to provide a short direct approach to results similar to but more explicit than those of [2; 3]. The tools used are well-known results of Jacobson [4] and Ore [8].

The author wishes to acknowledge his indebtedness to the referee for useful comments and references. He especially wishes to thank Professor H. Zassenhaus with whose guidance and encouragement this work was done.

Received by the editors January 1, 1962.

[1] From the author's Ph. D. thesis at the University of Notre Dame. This work was financially supported by the National Research Council of Canada.

1. **On derivations.** Throughout §§1 to 6, K will be a certain field of characteristic $p > 0$, and Z an extension field such that $Z^p \subset K$ and $(Z:K) = p^m$. Unless otherwise stated, all derivations considered will be K-derivations, that is, they will be linear over K.

The Z-dimension of the vector space $D_{Z/K}$ of derivations of Z into itself is m, and, as Jacobson [4] pointed out, there always exist derivations d such that $\{d, d^p, \cdots, d^{p^{m-1}}\}$ is a basis of $D_{Z/K}$ over Z. Such derivations are called *generators* of $D_{Z/K}$ and characterized by the property that their null-field is precisely K. (Clearly, then, any derivation is a generator of D_{Z/K_1}, where K_1 is its null-field.) The characteristic polynomial $f(x)$ (over K) of a generator is a p-polynomial of degree p^m and is at the same time its minimal polynomial. These facts follow quickly from the paragraph after Lemma 3 in [4].

Associated with each generator d of $D_{Z/K}$ is an additive homomorphism T_d from Z into K. If the minimal polynomial of d is $f(x) = \sum_{k=0}^{m} \lambda_k x^{p^k}$, then $T_d(\zeta) = \sum_{k=0}^{m} \lambda_k \sum_{i=0}^{k} (d^{p^i-1}\zeta)^{p^{k-i}}$ for $\zeta \in Z$. In §12 of [4], Jacobson introduces such a map and calls it V although it does depend on the choice of d[2]. It is implicit in his calculations that $T_d(\zeta) = f(u+z) - f(u)$ whenever Z is contained in a ring R, and $u \in R$ is such that $uz - zu = dz$ for all $z \in Z$. This is a most important property of T_d, making it an additive analogue of the norm function on a cyclic extension field. In this context, let the cyclic extension C of K be contained in a ring R with identity, and let $u \in R$ be such that the transformation $\xi \to u\xi u^{-1}$ ($\xi \in C$) generates the Galois group of C; then the norm of $c \in C$ equals $(uc)^n u^{-n}$, where n is the degree of C.

A generator d of $D_{Z/K}$ will be called *separable*, if its minimal polynomial $f(x)$ is separable.

PROPOSITION 1.1. *d is separable, if and only if d^p is a generator.*

Proof. If d^p is not a generator, it satisfies an equation

$$(d^p)^{p^n} + \mu_{n-1}(d^p)^{p^{n-1}} + \cdots + \mu_0 d^p = 0 \qquad (\mu_i \in Z)$$

with $n < m$. This is possible only if $n + 1 = m$, but then the elements μ_i coincide with the coefficients of the minimal polynomial of d. Evidently the latter could not be separable. Conversely, if d is not separable, its minimal polynomial can be written as a polynomial of degree p^{m-1} in x^p, and $d^p, (d^p)^p, \cdots, (d^p)^{p^{m-1}}$ are linearly dependent.

Suppose now that d is a separable generator and let E be a separable splitting field of its polynomial. We set $\mathbf{Z} = E \otimes_K Z$ and extend d to $\mathbf{Z}$ by prescribing $d(e \otimes z) = e \otimes dz$. In this situation, we have

[2] Let $m = 1$, $Z = K(z)$. Then $d: z \to 1$ and $D: z \to z$ are both generators of $D_{Z/K}$. Putting $\zeta = z^{p-1}$, we have $T_d(\zeta) = \zeta^p - 1$, whereas $T_D(\zeta) = \zeta^p$. It is unknown whether or not the module $T_d(Z)$ is independent of d.

PROPOSITION 1.2. *There exist $\alpha_1 \cdots \alpha_m \in E$, linearly independent over the prime field, and $z_1 \cdots z_m \in Z$, such that*

$$Z = E(z_1 \cdots z_m) \qquad \textit{and} \qquad dz_i = \alpha_i z_i.$$

Proof. The proper values of d form an additive group of order p^m because of the separability of d. Let $\{\alpha_1 \cdots \alpha_m\}$ be a basis of this group over the prime field, with corresponding proper vectors $z_1 \cdots z_m$. Since the products $z_1^{v_1} \cdots z_m^{v_m}$ $(0 \leqq v_i < p)$ correspond to the p^m different proper values of d, they span Z over E. Hence $Z = E(z_1 \cdots z_m)$.

If a separable generator has all its proper values in K, it will be called *regular.* A kind of converse of Proposition 1.2 is

PROPOSITION 1.3. *Let $Z = K(z_1 \cdots z_m)$. Given $\alpha_1 \cdots \alpha_m \in K$, linearly independent over the prime field, there exists a unique regular generator d, such that $dz_i = \alpha_i z_i$.*

This statement guarantees the existence of regular generators of $D_{Z/K}$. Its proof is elementary and need not be given here.

For use in §4, we shall finally establish the following property of derivations.

PROPOSITION 1.4. *Let S be a separable commutative algebra over Z. For $d \in D_{Z/K}$, let $\bar{d}$ denote the unique extension of d to S. Then $\bar{d}(S) \cap Z = d(Z)$.*

Proof. Obviously, $d(Z) \subseteq \bar{d}(S) \cap Z$. Let K_1 be the null field of d; $(Z : K_1) = p^u$, Since $(d(Z) : K_1) = p^n - 1$, it suffices to show that $\bar{d}(S) \cap Z \neq Z$.

The minimal polynomial $f(x)$ of d over K_1 is a p-polynomial of degree p^n. Let $g(x) = (1/x) \cdot f(x)$. For $\zeta \in \bar{d}(S) \cap Z$, there exists $\eta \in S$ such that $\bar{d}\eta = \zeta$. Hence $g(d)(\zeta) = f(\bar{d})(\eta) = 0$. If Z were equal to $\bar{d}(S) \cap Z$, we would have $g(d) = 0$.

2. **The ring $R[\![u;D]\!]$.** Let R be a ring with a given derivation $D: R \rightarrow R$. We define the ring $R[\![u;D]\!]$ of "differential polynomials" to be the set of formal polynomials

$$a_0 + a_1 u + \cdots + a_n u^n, \qquad a_i \in R,$$

on which addition is defined as usual and multiplication with the aid of the basic rule

$$ua = au + Da, \qquad a \in R; \tag{1}$$

that .si strictly speaking, by the distributive law and the rule

$$(au^k)(bu^l) = \sum_{i+j=k} \binom{k}{i} a(D^j b) u^{i+l}. \tag{2}$$

is formally obtained by a k-fold application of (1) to the product $u^k b$, associativity of multiplication being assumed. Associativity of the multiplication given by (2) is most easily verified by starting with the well-established additive group M of these polynomials and showing that $R\llbracket u;D\rrbracket$, as defined, is isomorphic to the ring of endomorphisms of M generated by the maps

$$\bar{r} : au^k \to (r\,a)u^k, \qquad r \in R,$$

and

$$\bar{u} : au^k \to au^{k+1} + (D\,a)u^k,$$

provided, of course, that the ring $\bar{R} = \{\bar{r} \mid r \in R\}$ is isomorphic to R (this can be achieved by adjoining an auxiliary identity element to R, if it does not already have one).

We note that $R\llbracket u;D\rrbracket$ is universal in the following sense. If ϕ is a homomorphism of R into a ring R' which contains an element $\bar{u}$ such that $\bar{u}\phi(r) - \phi(r)\,\bar{u} = \phi(D\,r)$ $(r \in R)$, then ϕ can be extended to a homomorphism $\phi' : R\llbracket u;D\rrbracket \to R'$ by setting $\phi'(u) = \bar{u}$.

The ring defined in this section has been studied by Ore [9] and, more recently, Amitsur [1]. In [9], it appears as a special case of a ring of "noncommutative" polynomials. In [1], with R simple, the main emphasis is on the ideals of $R\llbracket u;D\rrbracket$.

3. **Differential extensions.** A construction will be described in this section, by which a central simple Z-algebra A can be embedded as the centralizer of Z in a central simple K-algebra. The following assumptions must be made about A:

(1) There is a derivation $\bar{d}$ on A whose restriction d to Z is a generator of $D_{Z/K}$, and

(2) A contains an element c, such that $\bar{d}c = 0$ and $\operatorname{ad} c = f(\bar{d})$[3].

Let $f(x)$ again denote the minimal polynomial of d. We denote by $(A, \bar{d}, c)$ the K-algebra obtained by imposing the relation $f(u) = c$ on the ring $A\llbracket u;\bar{d}\rrbracket$. A K-algebra so constructed will be called a *differential extension of A to K*. The basic theorem of this paper is

THEOREM 3.1. *Let B a K-algebra. $B \simeq (A, \bar{d}, c + \gamma)$ with $\gamma \in K$, if and only if B is central simple and contains A as the centralizer of Z.*

It should be noted that $c + \gamma$ satisfies the same condition as c. To prove that $(A, \bar{d}, c)$ is central simple, we first establish two lemmas.

LEMMA 3.1. *The elements u^k $(0 \leqq k < p^m)$ form a left A-basis of $(A, \bar{d}, c)$.*

Proof. According to the preceding section, $A\llbracket u;\bar{d}\rrbracket$ has the left A-basis $\{u^k \mid k \geqq 0\}$. Let J be the ideal in $A\llbracket u;\bar{d}\rrbracket$ generated by $f(u) - c$. Since $f(u)$ is a K-linear combination of p-powers of u, we have $\operatorname{ad} f(u) = f(\operatorname{ad} u)$. Restricted to A, this means $\operatorname{ad} f(u) = f(\bar{d}) = \operatorname{ad} c$. Hence $f(u) - c$ commutes with A. It also commutes with u, since $\bar{d}c = 0$. Therefore $f(u) - c$ is in the center of $A\llbracket u;\bar{d}\rrbracket$,

[3] For every r in a ring R, $\operatorname{ad} r$ is the inner derivation by r, mapping x to $r \circ x = rx - xr$.

so that $J = A[\![u;d]\!] \cdot (f(u) - c)$. Since $f(u) - c$ has "degree" $p^m$and the coefficients of the powers u^k $(k > 0)$ are in K, no nontrivial element of J can have degree less than p^m. Thus $\{u^k \,|\, 0 \leqq k < p^m\}$ are linearly independent over A modulo J. On the other hand, it is obvious that they span $A[\![u;\bar{d}]\!]$ modulo J.

As a result of this lemma, every element of $(A, \bar{d}, c)$ can be uniquely written as $a_n u + \cdots + a_1 u + a_0$ $(0 \leqq n < p^m$: $a_i \in A)$. Thus we can speak of the *degree* of such an element (in the above case n, if $a_n \neq 0$).

Lemma 3.2. *Given $b = a_n u^n + \cdots + a_0$, there exists $z \in Z$ such that $b \circ z \neq 0$. The degree of $b \circ z$ is less than that of b.*

Proof. For arbitrary $z \in Z$, it is easy to calculate that

$$u^k z = \sum_{i=0}^{k} \binom{k}{i} (d^i z) u^{k-i}.$$

Hence

$$b \circ z = \sum_{k=0}^{n} a_k (u^k z - z u^k) = \sum_{k=0}^{n} a_k \sum_{i=1}^{k} \binom{k}{i} (d^i z) u^{k-i}.$$

The last expression contains no term in u^n; thus the second part of the lemma is verified. The coefficient of u^0 is $a_n d^n z + \cdots + a_0 z$. It suffices to show that it does not vanish for all z; for by the previous lemma this term cannot be cancelled by the others.

$(Z : K) = p^m$. On the other hand, the solutions of $a_n d^n z + \cdots + a_0 = 0$ form a space of dimension at most n over K. In fact, if $z_0 \cdots z_n$ are linearly independent over K, the Wronskian $\det(d^j z_i)$ $(i, j = 0, \cdots, n)$ does not vanish. In the vector space Z^{n+1} of $(n+1)$-tuples in Z, the vectors $V_k = (d^k z_0 \cdots d^k z_n)$ $(k = 0, \cdots, n)$ form a basis. Hence the equation $a_n V_n + \cdots + a_0 V_0 = 0$ is impossible in $A \otimes_K Z^{n+1}$.

The first part of Theorem 3.1 can now be proved.

K is in the center of $(A, \bar{d}, c)$, since it commutes with u. Conversely, Lemma 3.2 implies that a central element of $(A, \bar{d}, c)$ must be in A, and therefore in Z; in order to commute with u it must finally be in K. Thus $(A, \bar{d}, c)$ is central over K.

Let I be a proper ideal of $(A, \bar{d}, c)$. Since A is simple, $I \cap A = \{0\}$, i.e., the degree of every element of I is positive. Let $b \in I$ have minimal positive degree. Since $b \circ z \in I$ with smaller degree, we must have $b \circ z = 0$ for all $z \in Z$. This contradicts Lemma 3.2.

Finally, let A_1 be the centralizer of Z in $(A, \bar{d}, c)$. It is well known that $((A, \bar{d}, c) : K) = (A_1 : K)(Z : K)$, so that $(A_1 : K) = ((A, \bar{d}, c) : Z)$[4]. On the other hand, $A \subseteq A_1$ and $((A, \bar{d}, c) : Z) = p^m (A : Z) = (A : K)$. Hence $A_1 = A$.

[4] The equation used here follows from a general theorem of representation theory, which will be used more fully later: let R be a simple algebra, M a representation module of R, and S the algebra of R-endomorphisms of M; then $S \sim R'$ ($\sim$ denoting similarity in the sense of Brauer and $'$ denoting anti-isomorphic copy) and $(\dim R)(\dim S) = (\dim M)^2$.

For the second half of Theorem 3.1, we recall that every derivation from a semi-simple subalgebra of a central simple K-algebra B into B is extendable to an inner derivation of B [4, Theorem 7]; this result will in the sequel be referred to as Jacobson's theorem. In the situation of our theorem, it follows that there exists $u \in B$, such that $ua - au = \bar{d}a$ for all $a \in A$. Set $f(u) = c'$. Obviously c' satisfies condition (2). Thus $0 = \operatorname{ad} c - \operatorname{ad} c' = \operatorname{ad}(c - c')$, and $c - c' \in Z$; furthermore $\bar{d}(c - c') = 0$, so that $c' = c + \gamma$, with $\gamma \in K$. We have shown that the subalgebra of B generated by A and u is a homomorphic image of $(A, \bar{d}, c + \gamma)$. By simplicity of the latter and a look at the dimension $((B:K) = (Z:K)(A:K))$ the theorem is established.

THEOREM 3.2. $(A, \bar{d}, c + \gamma_1) \simeq (A, \bar{d}, c + \gamma_2)$ *if and only if* $\gamma_1 - \gamma_2 \in T_d(Z)$.

Proof. Let the indeterminates used in the construction of the two differential extensions be u_1 and u_2 respectively. Suppose an isomorphism $\sigma : (A, \bar{d}, c + \gamma_1) \rightarrow (A, \bar{d}, c + \gamma_2)$ to be given. It is well known that the isomorphism between σA and A in $(A, \bar{d}, c + \gamma_2)$ may be extended to an (inner) automorphism of the latter. Hence we may assume right away that σ leaves A fixed.

Now, $(\sigma u_1) \circ a = \sigma u_1 \circ \sigma a = \sigma(u_1 \circ a) = \bar{d}a$ for all $a \in A$; in other words, $\operatorname{ad}(\sigma u_1) = \operatorname{ad} u_2$ or $\sigma u_1 = u_2 + \zeta$ $(\zeta \in Z)$. $T_d(\zeta) = f(u_2 + \zeta) - f(u_2) = \sigma f(u_1) - f(u_2) = \gamma_1 - \gamma_2$.

Conversely, it is now clear that the correspondence $u_1 \rightarrow u_2 + \zeta$ where $\zeta \in T_d^{-1}(\gamma_1 - \gamma_2)$, induces an isomorphism between the two given algebras.

Theorem 3.2 classifies differential extensions involving a fixed derivation $\bar{d}$. It may be added that, if d is separable, $(A, \bar{d}, c) \simeq (A, \bar{d}^p, c^p)$; the proof of this is almost obvious. In this connection, it may also be asked, if by proper choice of $\bar{d}$, c can be chosen in K. This can only be done if A is obtained by extending the ground field of a K-algebra. We have the following

PROPOSITION. $f(\bar{d}) = 0$ *if and only if* $A = B \otimes_K Z$, *where* B *is central simple over* K, *and* $\bar{d}$ *is the derivation mapping* $b \otimes z$ *to* $b \otimes dz$ $(b \in B,\ z \in Z)$.

Proof. Putting $A = Z$, $\bar{d} = d$ and $c = 0$ in Theorem 3.1, one obtains a central simple K-algebra $(Z, d, 0)$, in which Z is a maximal commutative subring.

If $f(\bar{d}) = 0$, the differential extension $(A, \bar{d}, 0)$ can be constructed and contains an isomorphic image C of $(Z, d, 0)$. The centralizer B of C is another central simple K-algebra contained in $(A, \bar{d}, 0)$. This is possible only if $(A, \bar{d}, 0) \simeq B \otimes_K C$. In this form, A corresponds to the centralizer of $Z \subset C$, namely $B \otimes_K Z$. Finally, since the indeterminate u is in the centralizer C of B, we have $\bar{d}b = 0$ for $b \in B$ and hence $\bar{d}(b \otimes z) = b \otimes dz$.

The converse is trivial.

This section will close with a theorem on Kronecker products of differential extensions. For Kronecker products over K, the symbol $\otimes$ will be used without subscript; further, the convention of denoting the anti-isomorphic copy of a ring R by R' will be adopted. Given central simple Z-algebras A_1 and A_2 with extension $\bar{d}_1$ and $\bar{d}_2$ of a fixed generator d of $D_{Z/K}$, it is easily seen that d is extended to $A_1 \otimes_Z A_2$ by $\bar{d}_1 \oplus_Z \bar{d}_2$: $a_1 \otimes_Z a_2 \rightarrow \bar{d}_1 a_1 \otimes_Z a_2 + a_1 \otimes_Z \bar{d}_2 a_2$. We have

Theorem 3.3. *If* $B_i = (A_i, d_i, c_i)$ $(i = 1,2)$, *then*

$$B_1 \otimes B_2 \sim \left(A_1 \underset{Z}{\otimes} A_2,\ \bar{d}_1 \underset{Z}{\oplus} \bar{d}_2,\ c_1 \underset{Z}{\otimes} 1 + 1 \underset{Z}{\otimes} c_2 \right)$$ [5].

Proof. Consider the Z-space $M = B_1 \otimes_Z B_2$. $M = (B_1 \otimes B_2)/R$, where R is the subspace of $B_1 \otimes B_2$ spanned by the differences $(zb_1 \otimes b_2 - b_1 \otimes zb_2)$ $(z \in Z)$. Obviously, R is a right ideal and the right regular representation of $B_1 \otimes B_2$ induces a nontrivial representation of $B_1' \otimes B_2'$ on M. Hence $B_1 \otimes B_2 \sim B$, where B is the algebra of $B_1' \otimes B_2'$-endomorphisms of M. The previously cited relation between the dimensions of a simple algebra, its representation module, and the endomorphism algebra of this module shows that $(B : K) = ((A_1 \otimes_Z A_2) : K)p^{2m}$. Since $(A_1 \otimes_Z A_2,\ \bar{d}_1 \oplus_Z \bar{d}_2,\ c_1 \otimes_Z 1 + 1 \otimes_Z c_2)$ has exactly that dimension, the theorem will be established, if a homomorphic image of it is found in B.

Let u_i be the indeterminate in the construction of (A_i, d_i, c_i) $(i = 1,2)$ and consider the subalgebra B^* of $B_1 \otimes B_2$ generated by $w = u_1 \otimes 1 + 1 \otimes u_2$ and the elements $a_1 \otimes a_2$ $(a_i \in A_i)$. It is easily seen that R is a natural left B^*-module and hence that there is a representation ϕ of B^* on M. Furthermore, $\phi(B^*) \subseteq B$. Since $(za_1 \otimes a_2 - a_1 \otimes za_2) B_1 \otimes B_2 \subseteq R$, $\phi(za_1 \otimes a_2) = \phi(a_1 \otimes za_2)$ and $A_1 \otimes_Z A_2$ can be identified with the algebra generated by $\{\phi(a_1 \otimes a_2)\}$.

Let $v = \phi(w)$.

$$\begin{aligned} v \circ (a_1 \otimes_Z a_2) &= \phi(w \circ (a_1 \otimes a_2)) \\ &= \phi(\bar{d}_1 a_1 \otimes a_2 + a_1 \otimes \bar{d}_2 a_2) \\ &= \bar{d}_1 \oplus_Z \bar{d}_2 (a_1 \otimes_Z a_2). \end{aligned}$$

Finally,

$$\begin{aligned} f(v) &= \phi f(w) = \phi f([u_1 \otimes 1] + [1 \otimes u_2]) \\ &= c_1 \otimes_Z 1 + 1 \otimes_Z c_2. \end{aligned}$$

4. **Existence of differential extensions.** It is well known [3, Theorem 6;4, §10] that any K-derivation of Z is extendable to A. Of the conditions (1) and (2) introduced in §3, the first is therefore always satisfied, and the existence of differential extensions of A to K is equivalent to condition (2). It, too, is always fulfilled. In fact, Hochschild [3, §3] has shown that A can be embedded as the centralizer of Z in a suitable central simple K-algebra B. Even more generally, if R is any simple ring with a derivation D, it is proved by Amitsur in [1, Corollary 2] that R can be embedded in a simple ring in which D is induced by an

[5] For the proof, the reader is reminded of the result stated in footnote (4).

inner derivation (although this second ring is not unique up to isomorphism, as claimed in [1], cf. Theorem 3.2). Both these results immediately imply the existence of differential extensions for arbitrary A. Our object is to take a more direct route by simply verifying (2).

THEOREM. *Given a generator d of $D_{Z/K}$, there exists an extension $\bar{d}$ to A and an element $c \in A$, separable over K, satisfying* (2).

Proof. Let S be a separable, maximal commutative subalgebra of A. d has a unique extension d' to S. If $\tilde{d}$ is an arbitrary extension of d to A, its restriction to S differs from d' by an inner derivation i of A, by Jacobson's theorem. Thus $\bar{d} = \tilde{d} + i$ coincides with d' on S. $f(\bar{d}) = 0$ on S. Jacobson's theorem now implies the existence of $b \in A$, such that ad $b = f(\bar{d})$. Since S is maximal commutative, $b \in S$.

Clearly, $\bar{d}f(\bar{d}) = f(\bar{d})\bar{d}$, or $\bar{d}(\mathrm{ad}\, b) = (\mathrm{ad}\, b)\bar{d}$. Thus for all $a \in A$, $\bar{d}(b \circ a) = (\bar{d}b) \circ a + b \circ (\bar{d}a) = b \circ \bar{d}a$. Hence $(\bar{d}b) \circ a = 0$; i.e., $\bar{d}b \in Z$. By Proposition 1.4, $\bar{d}b = dz$ for some $z \in Z$. Set $c = b - z$. We still have ad c = ad $b = f(\bar{d})$; moreover, $\bar{d}c = 0$.

As pointed out in [3, §3], an interesting consequence of this theorem is the fact that the Brauer group B_K of similarity classes of central simple K-algebras is an extension of the subgroup B_K^Z of classes split by Z by the group B_Z[6]. Denoting a similarity class by square brackets, one easily sees that B_K breaks up into sets of the form $\{[(A,\bar{d},c + \gamma)] \mid A,\bar{d},c \text{ fixed}; \gamma \in K\}$; these, however, are cosets of B_K^Z, since $(A,\bar{d},c + \gamma) \sim (A,\bar{d},c) \otimes_K (Z,d,\gamma)$, and since $B_K^Z = \{[(Z,d,\gamma)]\}$, as will be seen in the next section; finally, the map $[(A,\bar{d},c + \gamma)] \to [A]$ is a homomorphism from B_K onto B_Z.

The original purpose of introducing differential extensions is the systematic construction of p-algebras. Let E be a maximal subfield of a p-algebra over K, such that $E = Z_0 \supset Z_1 \supset \cdots \supset Z_n = K$ and $Z_{i-1}^p \subset Z_i$ (it is a well-known peculiarity of p-algebras that they have purely inseparable splitting fields). We fix generators d_i of D_{Z_{i-1}/Z_i} $(i = 1, \cdots, n)$ and extensions $\bar{d}_i$ of d_i to the centralizers A_{i-1} of Z_{i-1} in B. Then $A_i = (A_{i-1}, \bar{d}_i, c_{i-1})$ for suitable $c_{i-1} \in A_{i-1}$ and $B = (A_{n-1}, \bar{d}_n, c_{n-1})$ is obtained from E by n successive differential extensions. Conversely, if n differential extensions are carried out formally, starting with E, the result is a p-algebra over K with E as maximal subfield. To make this construction explicit would be to provide an analogue of the crossed product construction for p-algebras. A paper on this problem is in preparation.

5. **The algebras** (Z, d, γ). We now specialize the considerations of § 3 to the case, where $A = Z$ and $c = 0$, and obtain the algebras already constructed, in the

[6] By an easy induction, this actually holds for any purely inseparable Z, not only for those of exponent 1.

same way, by Jacobson [5]. Corresponding to Theorems 3.1 to 3.3, we then have:

THEOREM 5.1. *A K-algebra B is of the form (Z,d,γ), if and only if B is central simple and contains Z as a maximal subfield.*

THEOREM 5.2. $(Z,d,\gamma_1) \simeq (Z,d,\gamma_2)$, *if and only if* $\gamma_1 - \gamma_2 \in T_d(Z)$.

In [5] Theorem 5.1 and the criterion, given below, for the splitting of (Z,d,γ) are proved.

THEOREM 5.3. $(Z,d,\gamma_1) \otimes_K (Z,d,\gamma_2) \sim (Z,d,\gamma_1 + \gamma_2)$[7].

Furthermore, it is easily seen that $(Z,d,0)$ is the algebra of matrices of degree p^m over K, so that (Z,d,γ) splits over K, if and only if $\gamma \in T_d(Z)$. These results yield an additive description of the Brauer group B_K^Z, namely

THEOREM 5.4. $B_K^Z \simeq K^+/T_d(Z)$, *K^+ denoting the additive group of K.*

Proof. Consider the map $\sigma : K^+ \to B_K$ defined by $\sigma(\gamma) = [(Z,d,\gamma)]$. By Theorem 5.3, σ is a homomorphism; its kernel is $T_d(Z)$ by the remark preceding this theorem. Finally, since every class of B_K^Z contains an algebra with Z as maximal subfield, σ is surjective by Theorem 5.1.

It is apparent now that the theory of differential extensions of Z bears a strong formal resemblance to that of cyclic crossed products. The role of the norm in the latter is played here by the additive map T_d. As Jacobson proved [4, Theorem 15], $T_d(z) = 0$ if and only if $z = d\zeta/\zeta$ for some $\zeta \in Z$. The map $\delta : \zeta \to d\zeta/\zeta$ is a homomorphism from $Z^\times$ (multiplicative group) into Z^+. Thus, the exact sequence

$$0 \to K^\times \to Z^\times \xrightarrow{\delta} Z^+ \xrightarrow{T_d} K^+ \to B_K^Z \to 0$$

is the analogue of

$$0 \to K^\times \to C^\times \xrightarrow{\varepsilon} C^\times \xrightarrow{\nu} K^\times \to B_K^C \to 0$$

in the case of crossed products of a cyclic extension C of K, where $\varepsilon(c) = c/c^\sigma$ (σ being a generating automorphism) and ν is the norm function. The flaw in this analogy is the dependence mentioned in §1 of T_d on d.

6. Connection with crossed products.

Unfortunately the method of differential extension of a field does not allow one to construct algebras that cannot be obtained by more classical means: the algebras discussed in the preceding paragraph are constructible as crossed products. In fact, provided d is *regular*, every description of an algebra as a differential extension (Z,d,γ) canonically yields a description of it as a crossed product. In this section, we shall discuss this duality of possible descriptions. Throughout it; d will denote a fixed regular generator

[7] For $m = 1$, Theorems 5.2 and 5.3 are contained in [7] as Theorems 3 and 8.

of $D_{Z/K}$. Further fixed objects: V, the additive group of proper values of d; P, the multiplicative group of proper vectors of d; and $f(x)$, the minimal polynomial of d. We note that V is a submodule of order p^m of K^+, P is a subgroup ot Z . Mapping a proper vector onto the corresponding proper value yields an isomorphism of $P/K^\times$ and V. $f(x) = \prod_{\lambda\in V} (x-\lambda)$ is separable, and so is $f(x)-\gamma$ for any $\gamma \in K$.

The term "crossed product" will be used in a slightly wider than normal sense. Let S be a finite dimensional, commutative, separable K-algebra with a group G of K-automorphisms (not necessarily all). Given a factor set $a: G \times G \to S^\times$ (multiplicative group) satisfying the usual associativity relations, one obtains a K-algebra (S,G,a), a *crossed product* of S by G, in the usual way. Of course, we are interested in the case where (S,G,a) is central simple and of dimension $(S:K)^2$. For this, Teichmüller [6] gave the following necessary and sufficient conditions:

Let $S = N_0 \oplus \cdots \oplus N_n$, a direct sum of fields N_i.

I. If $\sigma \in G$ and $\sigma \mid N_0 = 1$, then $\sigma = 1$.

II. G is transitive on the set of fields $\{N_0 \cdots N_n\}$.

III. If $s \in S$ and $s^G = s$, then $s \in K$.

A group satisfying I, II, III, will be called a T-group on S.

Given an algebra in the form (Z,d,γ), consider the subring S generated by K and the standard element u. Evidently, $S \simeq K[x]/(f(x)-\gamma)$ is a separable commutative K-algebra. The substitution $u \to u-\lambda$ $(\lambda \in V)$ defines a K-automorphism σ_λ on S, because $f(u-\lambda)=\gamma=f(u)$. Let $G=\{\sigma_\lambda \mid \lambda \in V\}$. It is easy to find elements of (Z,d,γ) which "produce" these automorphisms: $zuz^{-1} = u-\lambda$, if z is chosen in the coset P_λ of P modulo $K^\times$ for which $uz-zu=\lambda z$ $(\lambda \in V)$. Selecting representatives $z_\lambda \in P_\lambda$ and putting $a(\sigma_\lambda,\sigma_\mu) = z_\lambda z_\mu z_{\lambda+\mu}^{-1}$, for λ, $\mu \in V$, it is obvious that $(Z,d,\gamma)=(S,G,a)$. Since (Z,d,γ) is central simple with Z maximally commutative in it, G must be a T-group on S (a direct verification of this fact is easy). We have shown

Theorem 6.1. *In (Z,d,γ), let $S=K[u]$, and G be the group of automorphisms of S defined by $u \to u-\lambda$ $(\lambda \in V)$. G is a T-group on S, and $(Z,d,\gamma)=(S,G,a)$, where a is any factor-set corresponding to the extension P of $K^\times$ by G.*

We remark that the generating element u of S generates (in another sense) the derivation algebra of Z, while reciprocally, the generating elements $\{z_\lambda\}$ of Z generate "the" automorphism group of S.

In [6] it is proved that $(S,G,a) \sim (N_0,H,a^{(0)})$, where H is the subgroup $\{\sigma \in G \mid N_0^\sigma = N_0\}$ (isomorphic to the Galois group of N_0/K), and $a^{(0)}$ is obtained from a by restricting the domain to $H \times H$ and projecting the image into N_0. In our situation, the algebra $(N_0,H,a^{(0)})$ clearly would be a differential extension of the field Z_0 generated by those z_λ for which $\sigma_\lambda \in H$. Z_0 is also a splitting field of (Z, d, γ); its dimension is equal to that of N_0. Hence

THEOREM 6.2. *If Z is a minimal splitting field of (Z, d, γ), then S is a normal extension field of K, G its Galois group, and (Z, d, γ) a crossed product in the usual sense.*

7. **An application.** Let L be a Lie algebra over a field F of characteristic $p > 0$ with basis $B = \{u_0, u_1, \cdots, u_m\}$. For $v \in L$, the minimal polynomial of the linear transformation $\operatorname{ad} v : u_i \to v \circ u_i$ divides a certain p-polynomial $\psi(x)$. $\psi(v)$ lies in the center of the universal embedding algebra $\mathcal{U}$ of L. The idea of these polynomials is due to Jacobson; accordingly we shall call $\psi(x)$ the Jacobson polynomial of v. Let $\psi_i(x)$ be the Jacobson polynomial of u_i and denote by y_i the central element $\psi_i(u_i)$ of $\mathcal{U}$. $J(B)$ will stand for the subalgebra of $\mathcal{U}$ generated by $y_0 \cdots y_m$. The ring D of quotients with denominators from $J(B)$ is an algebra of p-power dimension over the quotient field $K(B)$ of $J(B)$. Since D has no zero-divisors, it is a division p-algebra over its center, which must be some finite extension of $K(B)$. It remains to mention, that $K(B) = F(y_0 \cdots y_m)$ is purely transcendental. Details are found in [10].

In [10], Zassenhaus also shows that an F-homomorphism θ of the center of $\mathcal{U}$ onto an extension field C of F induces an F-homomorphism of $\mathcal{U}$ onto an algebra containing C in its center (the latter will be called the *specialization* of $\mathcal{U}$ induced by θ). It was his question as to the nature of these p-algebras D and the specializations of $\mathcal{U}$ which initiated the present investigations. Here, now, is a fragment of an answer.

Let $\alpha_1 \cdots \alpha_m \in F$ be linearly independent over the primefield and consider the Lie algebra L with basis $B = \{u_0, u_1, \cdots, u_m\}$ and multiplication $u_i \circ u_j = 0 \; (i, j \neq 0)$ and $u_0 \circ u_i = \alpha_i u_i$. Such a Lie algebra can be described as one whose root spaces (including the Cartan-subalgebra) are 1-dimensional and whose roots are linearly independent over the prime field. In the notation introduced above, we have

LEMMA. *The center of D is $K(B)$. $(D : K(B)) = p^{2m}$.*

Proof. For $i \neq 0$, it is clear that $\psi_i(x) = x^P$. Hence $u_i^P = y_i \in K$. The minimal polynomial of $\operatorname{ad} u_0$ is of degree $\leqq m$, and therefore $\psi_0(x)$ has degree at most p^m. Hence $(D : K(B)) \leqq p^{2m}$.

Let K_1 be the center of D. $\operatorname{ad} u_0$ defines a K_1-derivation d on the field $E_1 = K_1(u_1 \cdots u_m)$; $d(u_1^{\nu_1} \cdots u_m^{\nu_m}) = (\sum_{i=1}^{m} \nu_i \alpha_i) u_1^{\nu_1} \cdots u_m^{\nu_m}$. Since d evidently has p^m distinct proper vectors, $(E_1 : K_1) \geqq p^m$. The dimension of D over K_1 is at least $(E_1 : K_1)^2 = p^{2m}$. The lemma is established, as we have $p^{2m} \leqq (D : K_1) \leqq (D : K(B)) \leqq p^{2m}$.

As a result of this lemma, we can write K instead of $K(B)$.

THEOREM 7.1. *$D \simeq (E, d, y_0)$, where $E = K(u_1 \cdots u_m)$ and d is the derivation induced by* ad u_0. *d is regular.*

Proof. Since $(E:K) = p^m$, E is a maximal subfield of D. d clearly is a regular generator of $D_{E/K}$ and u_0 is exactly such that $d\lambda = u_0 \circ \lambda$, for $\lambda \in E$. Finally $\psi_0(x)$ is the minimal polynomial of d, because it is of degree p^m; and $\psi_0(u_0) = y_0$.

We make two observations:

(1) Since D is a division algebra, it is a crossed product of $K(u_0)$ by its abelian Galois group.

(2) Every algebra of the type (Z, d, γ) and of dimension p^{2m} depends on (among other things) $m + 1$ parameters from its center K, namely, γ and the pth powers of the generators of Z. If K is a field of rational functions in these parameters, (Z, d, γ) is a division algebra.

The following theorem can now be stated without proof.

THEOREM 7.2. *Let $Z = F(z_1 \cdots z_m)$, where $z_i^p = \beta_i \in F$ and $\beta_1 \cdots \beta_m$ form a p-independent set. Let d be the derivation of Z defined by $dz_i = \alpha_i z_i$. Then (Z, d, β_0) is the specialization of $\mathcal{U}$ induced by the map θ of $F[y_0, \cdots, y_m]$*[8] *onto F for which $\theta y_i = \beta_i$.*

Theorem 7.2 states that any central simple F-algebra of dimension p^{2m}, containing a purely inseparable maximal subfield of exponent 1, can be obtained from $\mathcal{U}$ by a suitable specialization of the center of $\mathcal{U}$ onto F. Conversely, every such specialization θ maps $\mathcal{U}$ onto such an algebra, provided that $\{\theta(y_i) \mid i \neq 0\}$ is a p-independent set.

REFERENCES

1. S. A. Amitsur, *Derivations in simple rings*, Proc. London Math. Soc. **7** (1957), 87–112.

2. G. Hochschild, *Simple algebras with purely inseparable splitting fields of exponent* 1, Trans. Amer. Math. Soc. **79** (1955), 477–489.

3. ———, *Lie algebras and simple associative algebras*, Trans. Amer. Math. Soc. **80** (1955), 135–147.

4. N. Jacobson, *Abstract derivation and Lie algebras*, Trans. Amer. Math. Soc. **42** (1937), 206–224.

5. ———, *p-algebras of exponent p*, Bull. Amer. Math. Soc. **43** (1937), 667–670.

6. O. Teichmüller, *Verschränkte Produkte mit Normalringen*, Deutsch. Math. **1** (1936)› 92–102.

7. ———, *p-Algebren*, Deutsch. Math. **1** (1936), 362–388.

8. O. Ore, *On a special class of polynomials*, Trans. Amer. Math. Soc. **35** (1933), 559–584.

9. ———, *Theory of non-commutative polynomials*, Ann. of Math. **34** (1933), 480–508.

10. H. Zassenhaus, *Representations of Lie algebras of prime characteristic*. I, Proc. Glasgow Math. Assoc. **2** (1954), 1–36.

UNIVERSITY OF NOTRE DAME,
NOTRE DAME, INDIANA
UNIVERSITÄT HAMBURG,
HAMBURG, GERMANY

[8] Obviously, $F[y_0, \cdots, y_m]$ is the center of $\mathcal{U}$.