SIMPLE ALGEBRAS WITH PURELY INSEPARABLE SPLITTING FIELDS OF EXPONENT 1

BY

G. HOCHSCHILD

Introduction. Let C be a field of characteristic $p \neq 0$, and let K be a finite algebraic extension field of C such that the pth power of every element of K lies in C. Then K/C is called a purely inseparable extension of exponent 1. It was shown by N. Jacobson that there is a Galois theory for such extensions in which the place of the Galois group is taken by the derivation algebra of K/C. In particular, if K is any field of characteristic p, the purely inseparable extensions K/C of exponent 1 are precisely those in which C is the field of constants of a restricted K-Lie ring of derivations of K which is of finite dimension over K. In the classical theory of simple algebras, it is shown that, if K/C is a Galois extension, the Brauer similarity classes of the simple algebras with center C and split by K constitute a group which is canonically isomorphic with the group of equivalence classes of the group extensions of the multiplicative group of K by the Galois group of K/C. The present paper provides the answer to a question put to me by J-P. Serre, of whether one could establish an analogous result, for K/C purely inseparable of exponent 1, in which restricted Lie algebra extensions [2] of K by the derivation algebra of K/C take the place of the group extensions. Not only is the answer to this question affirmative, but it provides an excellent illustration of the theory of restricted Lie algebra extensions. It turns out, in fact, that the Lie algebra extensions which arise from simple algebras are trivial extensions when regarded as *ordinary* extensions, so that the essential structural elements are here precisely those which differentiate the *restricted* extensions from the ordinary ones.

§1 contains the field theoretical background of our problem. In particular, it gives a simple proof of the main theorem of Jacobson's Galois theory [4] which we include here because it gives us the connection, on which many of our subsequent arguments are based, between the structure of the field extension K/C and that of the derivation algebra of K/C. Theorem 2, which is not needed in the sequel, is the analogue for the present situation of a well known result in the classical Galois theory and is significant for the cohomology theory of derivation algebras. In §2 we give a proof of a theorem of Jacobson's on derivations (in a slightly generalized form) which is fundamental for the crossed product theory that follows, in the same way as the analogous theorem for isomorphisms is the source of the classical theory of crossed products. In §3 we discuss the special type of restricted Lie algebra

Received by the editors October 6, 1954.

extensions which arise from simple algebras. §4 contains the main results.

A nonmeasurable, but very considerable, portion of this paper is the result of collaboration with J. T. Tate. Without making him in any way responsible for its content, I wish to thank him here for his various contributions.

1. Differential Galois theory.

THEOREM 1 (JACOBSON). *Let K be a field of characteristic p, and let T be a Lie ring of derivations of K such that*

(1) *if $\tau \in T$ then also $\tau^p \in T$, and*

(2) *if $u \in K$ and $\tau \in T$ then also $u\tau \in T$, where, for $v \in K$, $(u\tau)(v) = u\tau(v)$.*

Suppose furthermore that the dimension $[T:K]$ of T over K is finite. Let C be the field consisting of all elements of K which are annihilated by all $\tau \in T$. Then $[K:C] = p^{[T:K]}$, and every derivation of K which annihilates C is contained in T.

Proof. Put $[T:K] = k$. By an elementary lemma concerning spaces of maps of arbitrary sets into fields (Lemma 2.1 of [1]), we can find elements $u_1, \cdots, u_k$ in K and a basis $\tau_1, \cdots, \tau_k$ for T over K such that $\tau_i(u_j) = \delta_{ij}$ (Kronecker symbol). Writing $[\tau_i, \tau_j] = \sum_q v_{ijq}\tau_q$, with $v_{ijq} \in K$, we get $0 = [\tau_i, \tau_j](u_q) = v_{ijq}$, whence $[\tau_i, \tau_j] = 0$. In the same way we find that $\tau_i^p = 0$.

Since $\tau_q(u_q) = 1$ while $\tau_q(C[u_1, \cdots, u_{q-1}]) = (0)$, we have $u_q \notin C[u_1, \cdots, u_{q-1}]$. On the other hand, since pth powers are annihilated by every derivation, $u_q^p \in C$. Hence u_q is of degree p over $C[u_1, \cdots, u_{q-1}]$. It follows that $C[u_1, \cdots, u_k]$ is of degree p^k over C, and that the monomials $u_1^{e_1} \cdots u_k^{e_k}$, with $0 \leqq e_i < p$, constitute a basis for $C[u_1, \cdots, u_k]$ over C.

There remains only to prove that $C[u_1, \cdots, u_k] = K$. For then, if τ is any derivation of K which annihilates C, we have evidently $\tau = \sum_i \tau(u_i)\tau_i \in T$. Suppose that this is false, i.e., that there is an element v_1 in K which does not belong to $C[u_1, \cdots, u_k]$. Assume inductively that we have already found an element v_q of K which is not in $C[u_1, \cdots, u_k]$ and which is annihilated by every τ_i with $i < q$. Since $\tau_q^p = 0$, there is an exponent e $(0 \leqq e < p)$ such that τ_q^{e+1}, but not τ_q^e, maps v_q into $C[u_1, \cdots, u_k]$. We have $\tau_i\tau_q^e(v_q) = \tau_q^e\tau_i(v_q)$, which is 0 for $i < q$. Hence, replacing v_q by $\tau_q^e(v_q)$, we may suppose that $\tau_q(v_q) \in C[u_1, \cdots, u_k]$. Since $\tau_q(v_q)$ is annihilated by each τ_i with $i < q$, it follows then that $\tau_q(v_q) \in C[u_q, \cdots, u_k]$. Write $\tau_q(v_q)$ as a polynomial of degree $p-1$ in u_q, with coefficients in $C[u_{q+1}, \cdots, u_k]$. Since this polynomial is annihilated by τ_q^{p-1} (for $\tau_q^p(v_q) = 0$), the coefficient of u_q^{p-1} must be 0. Hence we can "integrate" this polynomial with respect to u_q, i.e., there is an element $w \in C[u_q, \cdots, u_k]$ such that $\tau_q(w) = \tau_q(v_q)$. Now put $v_{q+1} = v_q - w$. Then $v_{q+1} \notin C[u_1, \cdots, u_k]$ and $\tau_i(v_{q+1}) = 0$ for all $i < q+1$. We can repeat this construction until we obtain $v_{k+1} \notin C[u_1, \cdots, u_k]$ such that $\tau_i(v_{k+1}) = 0$ for all $i = 1, \cdots, k$. But then $v_{k+1} \in C$, and we have a contradiction. Hence $C[u_1, \cdots, u_k] = K$, and Theorem 1 is proved.

We can now introduce a device which will be very helpful in our later

dealings with T. Put $\sigma_i = u_i\tau_i$, where the u_i and the τ_i are chosen as in our proof of Theorem 1. Then $[\sigma_i, \sigma_j] = 0$, and $\sigma_i^p = \sigma_i$. Let T_0 denote the restricted subalgebra of the restricted Lie algebra T (over C) which is spanned, over C, by the σ_i's. Construct the restricted universal enveloping algebra U_{T_0} of T_0. (U_{T_0} is obtained from Jacobson's u-algebra of T_0 by adjoining an identity element; for the terminology and notation used here, see [2]). U_{T_0} is finite dimensional and commutative, and (because of $\sigma_i^p = \sigma_i$) has no nilpotent elements other than 0. Hence U_{T_0} is semisimple.

In [2] we have defined the restricted q-dimensional cohomology groups $H_*^q(L, M)$ for restricted Lie algebras L in restricted L-modules (i.e., unitary U_L-modules) M. We shall repeatedly use the elementary fact that if L and M are finite dimensional and U_L is semisimple then $H_*^q(L, M) = (0)$, for $q > 0$. This is seen by considering the U_L-module S of all linear maps of U_L into M, the operations being given by $(u \cdot s)(v) = s(vu)$, where u and v are in U_L and s in S. This module S contains M as a U_L-submodule. In fact, if, for $m \in M$, we define $s_m \in S$ by putting $s_m(v) = v \cdot m$, the map $m \to s_m$ is a U_L-isomorphism of M into S. It is not difficult to see from the definition of the restricted cohomology groups that $H_*^q(L, S) = (0)$, for $q > 0$. In our case, M is a direct module summand in S, because S is finite dimensional and U_L is semisimple. Hence we must also have $H_*^q(L, M) = (0)$. In particular, $H_*^q(T_0, M) = (0)$, for every finite dimensional restricted T_0-module M, and all $q > 0$.

It is well known that if G is a finite group of automorphisms of a field K then the 1-dimensional cohomology group of G in the multiplicative group of K is trivial. As a first application of our above remarks, we prove the following analogous result.

THEOREM 2. *If K, C, and T are as in Theorem* 1 *we have $H_*^1(T, K) = (0)$, where we regard T as a restricted Lie algebra over C, and K as a restricted T-module, in the natural fashion.*

Proof. Let $w \in H_*^1(T, K)$. This cohomology class w can be represented by a restricted Lie 1-cocycle (see Theorem 2.1 of [2]), i.e., by a C-linear map f of T into K such that

(1) $\rho_1(f(\rho_2)) - \rho_2(f(\rho_1)) = f([\rho_1, \rho_2])$, and

(2) $\rho^{p-1}(f(\rho)) = f(\rho^p)$, for all ρ, ρ_1, ρ_2 in T.

Since the restriction of w to T_0 is 0, by what we have seen above, we may choose f so that $f(\sigma_i) = 0$, for each i. Now write, with $u \in K$, $f(u\sigma_i) = g_i(u)$. Then g_i is a C-linear map of K into itself. If, in (1), we set $\rho_1 = \sigma_j$ and $\rho_2 = u\sigma_i$ we find that $\sigma_j g_i = g_i \sigma_j$. Hence each g_i is a T_0-endomorphism of K. If a is any monomial in $u_1, \cdots, u_k$ then Ca is evidently a simple T_0-submodule of K. Furthermore, K is the direct module sum of Ca and other such monomial submodules, and no two of these simple components of K are T_0-isomorphic. It follows that we must have $g_i(a) = (a)_i a$, where $(a)_i \in C$. Now apply (1) with $\rho_1 = a\sigma_i$ and $\rho_2 = b\sigma_j$, where a and b are monomials in $u_1, \cdots, u_k$. This gives

$a(b)_j\sigma_i(b)-b(a)_i\sigma_j(a)=f(a\sigma_i(b)\sigma_j-b\sigma_j(a)\sigma_i)$, and since $a\sigma_i(b)$ and $b\sigma_j(a)$ both lie in Cab the right side is equal to $(ab)_ja\sigma_i(b)-(ab)_ib\sigma_j(a)$. In particular, if a does not contain a factor u_j, so that $\sigma_j(a)=0$, this shows that $a(b)_j=(ab)_j$. Now write $h_j(e)=(u_j^e)_j$. Then it will suffice to show that $h_j=0$. For this, by what we have just seen, implies that $g_j=0$, and since $T=KT_0$ this implies that $f=0$. Now return to the last relation deduced from (1), putting $i=j$, $a=u_j^{e_1}$, and $b=u_j^{e_2}$. Then we obtain $e_2h_j(e_2)-e_1h_j(e_1)=(e_2-e_1)h_j(e_1+e_2)$. Write e for e_2 and put $e_1=p-1$. Noting that $h_j(e)$ depends only on the residue class of e mod p, we then find that $eh_j(e)+h_j(p-1)=(e+1)h_j(e-1)$. On the other hand, let us apply (2) with $\rho=u_j^{p-1}\sigma_j=u_j^p\tau_j$. Then $\rho^p=0$, and we find $h_j(p-1)\rho^{p-1}(u_j^{p-1})=0$, whence $h_j(p-1)=0$. Hence the last result becomes $eh_j(e)=(e+1)h_j(e-1)$. Since $h_j(0)=0$, this gives $h_j(e)=0$, for all e. This completes the proof of Theorem 2.

2. **Derivations of algebras.** The possibility of having a crossed product theory with derivations in the place of automorphisms hinges on the following result of Jacobson's [3].

THEOREM 3 (JACOBSON). *Let A be a simple ring with minimum condition, and let C denote the center of A. Let B be a semisimple finite dimensional algebra over C such that $C\subset B\subset A$, and let τ be a derivation of B into A which annihilates C. Then there is an element $t\in A$ such that $\tau(b)=tb-bt$, for all $b\in B$.*

Proof. Let A^* be an anti-isomorphic image of A, and construct the tensor product $B\otimes A^*$ with respect to C. Then $B\otimes A^*$ is still a semisimple ring with minimum condition, as follows from standard results. Let (A, A) be the direct sum of two copies $(A, 0)$ and $(0, A)$ of A, with its natural structure as a right A-module. We define a left B-module structure on (A, A) by setting $b\cdot(a_1, a_2)=(ba_1, \tau(b)a_1+ba_2)$. Correspondingly, (A, A) has now the structure of a $B\otimes A^*$-module. Since $B\otimes A^*$ is semisimple with minimum condition, $(0, A)$ is a direct module summand in (A, A), i.e., $(A, A)=U+(0, A)$, where U is a $B\otimes A^*$-submodule of (A, A), and $U\cap(0, A)=(0)$. Now U is $B\otimes A^*$-isomorphic with $(A, A)/(0, A)$, and therefore also with A, regarded as a $B\otimes A^*$-module in the canonical fashion. Let α be a $B\otimes A^*$-isomorphism of A onto U, and write $\alpha(1)=(u, v)$. Then we have, with $b\in B$, $(bu, \tau(b)u+bv)=b\cdot\alpha(1)=\alpha(b)=\alpha(1\cdot b)=\alpha(1)\cdot b=(ub, vb)$. Hence $bu=ub$ and $\tau(b)u=vb-bv$. Now there is an element of the form $(1, w)$ in U, and hence there is an element $a\in A$ such that $\alpha(a)=(1, w)$, i.e., $(ua, va)=(1, w)$, whence $ua=1$. Also, $\alpha(au)=(u, wu)$, and so $\alpha(au-1)=(0, wu-v)\in(0, A)$. Since $U\cap(0, A)=(0)$, this gives $au=1$. Since u commutes with the elements of B, so does its inverse a. From $\tau(b)u=vb-bv$, we obtain therefore $\tau(b)=(va)b-b(va)$, and Theorem 3 is proved.

3. **Regular extensions.** Let K/C be a purely inseparable extension of exponent 1, and put $[K:C]=p^k$. Let T be the restricted Lie algebra over C which consists of all derivations of K that annihilate C. We can find elements

$u_1, \cdots, u_k$ in K such that $K = C[u_1, \cdots, u_k]$ and the monomials $u_1^{e_1} \cdots u_k^{e_k}$ $(0 \leqq e_i < p)$ constitute a basis for K over C. Then T evidently contains derivations τ_i such that $\tau_i(u_j) = \delta_{ij}$, and it is easily seen that an element of K which is annihilated by each τ_i must lie in C. Hence C is the field of constants for T, and we are in the situation of Theorem 1.

Now let A be a simple finite dimensional algebra with center C which contains K as a maximal commutative subring. Let S denote the set of all elements s of A for which $D_s(K) \subset K$, where D_s denotes the derivation of A which is given by $D_s(a) = sa - as$, for all $a \in A$. Let $\phi(s)$ denote the restriction of D_s to K. S carries the structure of a restricted Lie algebra over C, with $[s_1, s_2] = s_1 s_2 - s_2 s_1$, and the p-map $s \to s^p$. By Theorem 3, the restricted Lie algebra homomorphism $s \to \phi(s)$ maps S onto all of T, and clearly the kernel of ϕ coincides with K. Thus the pair (S, ϕ) is a restricted Lie algebra extension of K by T.

Now we observe that both S and T carry also the structure of a vector space over K, and that this vector space structure is connected with the restricted Lie algebra structure in a certain way which we shall make explicit. Let R stand for S or T, and denote the elements of R by ρ, ρ_1, etc. Then, if v_1 and v_2 are in K, we have

(i) $[v_1\rho_1, v_2\rho_2] = v_1(\rho_1 \cdot v_2)\rho_2 - v_2(\rho_2 \cdot v_1)\rho_1 + v_1 v_2[\rho_1, \rho_2]$, where $\rho \cdot v$ denotes the ρ-transform of v in the appropriate R-module structure of K.

While this identity is evident, the connection of the K-space structure with the p-map is more difficult to find. The result is the following:

(ii) $(v\rho)^p = v^p \rho^p + t_{v_\rho}^{p-1}(v)\rho$, where t_σ, for any $\sigma \in R$, denotes the σ-operator $v \to \sigma \cdot v$ on K.

This result is an immediate consequence of the following general lemma.

LEMMA 1. *Let U be an associative algebra over the field P of the integers* mod p, *and let V be a commutative subalgebra of U. Let u be an element of U such that $D_u(V) \subset V$. Then, for every $v \in V$, $(vu)^p = v^p u^p + D_{vu}^{p-1}(v)u$.*

Proof. Let $y, x_0, x_1, \cdots$ be algebraically independent elements over P, and consider the polynomial ring $H = P[y, x_0, x_1, \cdots]$. There is evidently a derivation τ of H such that $\tau(y) = 1$ and $\tau(x_i) = x_{i+1}$, for each i. Let ζ_i denote the multiplication by x_i in H, and let E be the ring of additive endomorphisms of H which is generated by τ and all the ζ_i. Then, in E, we have $\tau\zeta_i = \zeta_i\tau + \zeta_{i+1}$ whence we see that there is a homomorphism f of E into U such that $f(\tau) = u$ and $f(\zeta_i) = D_u^i(v)$. There is an evident isomorphism $q \to q'$ of the subring of E which is generated by the ζ_i into H such that $\zeta_i' = x_i$. If q_1 and q_2 are in this subring Q, say, of E we have

$$(q_1\tau)(q_2') = q_1'(\tau q_2 - q_2\tau)' = (q_1\tau q_2 - q_1 q_2 \tau)' = (D_{q_1\tau}(q_2))'.$$

By rearranging the factors in the product $(\zeta_0\tau)^p$, using that $\tau\zeta_i = \zeta_i\tau + \zeta_{i+1}$, we clearly obtain (after applying a finite sequence of such straightenings) a

relation $(\zeta_0\tau)^p=\zeta_0^p\tau^p+\sum_{i=1}^{p-1} q_i\tau^i$, where the q_i are certain elements of Q which remain to be determined. Now we note that $(\zeta_0\tau)^p$ and τ^p are derivations and apply our map to the element y^{p-1}. We obtain $(p-1)(\zeta_0\tau)^p(y)y^{p-2}=\sum_{i=1}^{p-1}(p-1)\cdots(p-i)q_i' y^{p-1-i}$. By comparing coefficients, we conclude that $q_i'=0$ for $i>1$, whence $q_i=0$ for $i>1$, while $q_1'=(\zeta_0\tau)^p(y)=(\zeta_0\tau)^{p-1}(x_0)=(\zeta_0\tau)^{p-1}(\zeta_0')=(\zeta_0\tau)^{p-2}((D_{\zeta_0\tau}(\zeta_0))')=\cdots=(D_{\zeta_0\tau}^{p-1}(\zeta_0))'$. Hence $q_1=D_{\zeta_0\tau}^{p-1}(\zeta_0)$ and $(\zeta_0\tau)^p=\zeta_0^p\tau^p+D_{\zeta_0\tau}^{p-1}(\zeta_0)\tau$. Now if we apply the homomorphism f this yields the result of Lemma 1; and it is clear that Lemma 1 gives (ii) for $R=S$ when applied to A, and for $R=T$ when applied to the ring of all additive endomorphisms of K.

A restricted Lie algebra extension (S, ϕ) of K by T such that S can be given the structure of a K-space satisfying (i) and (ii) and for which ϕ is K-linear will be called a *regular* extension of K by T.

The following example shows that, in general, not every restricted extension of K by T is regular. Let $K=C[u]$, where $u^p\in C$, but $u\notin C$. Let S be the semidirect sum of the Lie algebras K and T, i.e., the underlying space of S is the direct sum (T, K) of the C-spaces T and K, and the commutation is given by $[(\rho_1, v_1), (\rho_2, v_2)]=([\rho_1, \rho_2], \rho_1(v_2)-\rho_2(v_1))$. Let $\rho\to\rho'$ be any p-semilinear map of T into C, i.e., an additive map such that, for $c\in C$, $(c\rho)'=c^p\rho'$. Define the p-map in S by $(\rho, v)^p=(\rho^p, \rho'+\rho^{p-1}(v)+v^p)$. This makes S into a restricted Lie algebra (see [2], §3). If we define $\phi(\rho, v)=\rho$ then ϕ is a restricted Lie algebra homomorphism of S onto T whose kernel coincides with $(0, K)$, which we identify with K. Now suppose that this extension (S, ϕ) of K by T is regular. Let τ be the element of T for which $\tau(u)=1$, and put $\sigma=u\tau$. Then, if $u(\tau, 0)$ denotes the u-multiple of $(\tau, 0)$ in an admissible K-space structure of S, we must have $(\sigma, 0)=u(\tau, 0)+v$, where v lies in K. Using (i), we obtain $(\tau, 0)=[(\tau, 0), (\sigma, 0)]=[(\tau, 0), u(\tau, 0)+v]=(\tau, 0)+\tau(v)$, whence $\tau(v)=0$, and so $v\in C$. Using this and (ii), we find that $(\sigma, \sigma')=(\sigma, 0)^p=(u(\tau, 0)+v)^p=(u(\tau,0))^p+v^p=u^p\tau'+(u\tau)^{p-1}(u)(\tau,0)+v^p=u^p\tau'+u(\tau,0)+v^p$, whence $\sigma'=u^p\tau'+v^p-v$. We may, for instance, take $C=P(x)$, with x transcendental over P, $\tau'=0$ and $\sigma'=x$. Then, since no element v of C satisfies $v^p-v=x$, it follows that our extension of K by T cannot be regular.

THEOREM 4. *Let (S, ϕ) and (S', ϕ') be regular extensions of K by T which are equivalent as restricted Lie algebra extensions. Then, for any admissible K-space structures of S and S', there is a K-linear equivalence isomorphism of S onto S'. Also, there is an ordinary Lie algebra isomorphism ψ of T into S which is K-linear and such that, for every $\tau\in T$, $\phi\psi(\tau)=\tau$, and $\psi(\tau)^p-\psi(\tau^p)\in C$.*

Proof. We shall first prove the second assertion of the theorem. Let T_0 be the restricted subalgebra of T which we introduced in §1, and put $S_0=\phi^{-1}(T_0)$. Let ϕ_0 denote the restriction of ϕ to S_0, so that (S_0, ϕ_0) is a restricted extension of K by T_0. We define a new p-map $s\to s^{[p]}$ in S_0 by putting $s^{[p]}=s^p-s'$, where $s\to s'$ is any p-semilinear map of S_0 into C such that, for $v\in K$, $v'=v^p$.

Then we have $v^{[p]}=0$, and with this new p-map (S_0, ϕ_0) is a restricted extension of K by T_0, where now K is regarded as an abelian restricted Lie algebra with p-map 0. Since $H^2_*(T_0, K)=(0)$, it follows from Theorem 3.3 of [2] that this restricted Lie algebra extension is trivial. In particular, ignoring the p-map now, there is an ordinary Lie algebra isomorphism ψ_0 of T_0 into S_0 such that $\phi_0\psi_0$ is the identity map on T_0. Now equip S with an admissible K-space structure and let ψ be the unique extension of ψ_0 to a K-linear isomorphism of T (which, as a vector space over K, is isomorphic with the tensor product $K\otimes T_0$, taken with respect to C) into S. Then $\phi\psi$ is the identity map on T. It follows from the identity (i) that ψ is an ordinary Lie algebra isomorphism of T into S. Furthermore, if $\sigma\in T_0$, we have $\psi(\sigma)^p-\psi(\sigma^p)=\psi(\sigma)'\in C$. Also, if $v\in K$, we have, by the identity (ii), $(v\psi(\sigma))^p=v^p\psi(\sigma)^p+i^{p-1}_{v\psi(\sigma)}(v)\psi(\sigma)=v^p\psi(\sigma)^p+(v\sigma)^{p-1}(v)\psi(\sigma)=v^p\psi(\sigma)'+v^p\psi(\sigma)^{[p]}+(v\sigma)^{p-1}(v)\psi(\sigma)=v^p\psi(\sigma)'+\psi(v^p\sigma^p+(v\sigma)^{p-1}(v)\sigma)=v^p\psi(\sigma)'+\psi((v\sigma)^p)$, whence $(\psi(v\sigma))^p-\psi((v\sigma)^p)=v^p\psi(\sigma)'\in C$. Finally, in any restricted Lie algebra, $(a+b)^p=a^p+b^p+s(a, b)$, where $s(a, b)$ is a certain sum of commutators formed from a and b, whence $\psi(s(a, b))=s(\psi(a), \psi(b))$. Hence our above result extends to sums of elements of the form $v\sigma$, i.e., to arbitrary elements of T. This completes the proof of the second assertion of Theorem 4.

Now let (S', ϕ') be a second regular extension of K by T, and let α be an equivalence isomorphism of S onto S'. Equip S' with an admissible K-space structure. We can evidently find a basis for S over K which is of the form $1, s_1, \cdots, s_k$, where each $s_i\in\psi(T_0)$. We claim that the set $1=\alpha(1), \alpha(s_1), \cdots, \alpha(s_k)$ is K-linearly independent in S', and therefore constitutes a basis for S' over K. In fact, suppose that we have a relation $v+\sum_{i=1}^k v_i\alpha(s_i)=0$, where v and the v_i belong to K. Apply ϕ', noting that ϕ' is K-linear and $\phi'\alpha=\phi$. There results the relation $\sum_{i=1}^k v_i\phi(s_i)=0$. Since ϕ is K-linear, we may conclude from this that $\sum_{i=1}^k v_is_i\in K$, whence each $v_i=0$, whence also $v=0$. Now define β as the K-linear isomorphism of S onto S' which sends 1 into 1 and each s_i into $\alpha(s_i)$. Then β evidently coincides with α on $K+\psi(T_0)=S_0$. Since the K-space structures of S and S' satisfy the regularity condition (i), it follows from the fact that β is a Lie algebra isomorphism on S_0 that β is also a Lie algebra isomorphism on $KS_0=S$. Similarly, using the regularity condition (ii), we find that $\beta(vs)^p=\beta((vs)^p)$, for all $v\in K$ and all $s\in S_0$. As in our proof of the second assertion of Theorem 4, we may now conclude from this that β is a restricted Lie algebra isomorphism of S onto S'. Clearly, β leaves the elements of K fixed and $\phi'\beta=\phi$, so that β is the desired K-linear equivalence isomorphism. This completes the proof of Theorem 4.

4. **Differential crossed products.** Let (S, ϕ) be a regular extension of K by T, and construct the restricted universal enveloping algebra U_S of S. Let U_S^+ denote the ideal of U_S which is generated by the canonical images s' in U_S of the elements $s\in S$. Let J be the ideal of U_S^+ which is generated by the elements of the form $v's'-(vs)'$, where $v\in K$, $s\in S$, and vs denotes the v-multiple

of s in an admissible K-space structure of S. Put $V_S = U_S^+/J$. Although our construction of V_S uses an admissible K-space structure of S, it is clear from the first part of Theorem 4 that V_S is essentially determined by the equivalence class of (S, ϕ).

THEOREM 5. *Let (S, ϕ) be a regular extension of K by T, equipped with an admissible K-space structure on S. Then the canonical map of S into V_S is $1-1$, and its restriction to K is a field isomorphism by means of which we identify K with a subfield of V_S. Then V_S is a simple finite dimensional algebra with center C, and K is a maximal commutative subring of V_S. Furthermore, S becomes identified, by the canonical map, with the set of all $a \in V_S$ for which $D_a(K) \subset K$, and the corresponding regular extension of K by T coincides with (S, ϕ). Conversely, if A is a simple finite dimensional algebra with center C and containing K as a maximal commutative subring, and if (S, ϕ) is the corresponding regular extension of K by T, then the homomorphism of U_S^+ into A which extends the injection of S into A induces an isomorphism of V_S (constructed by using the natural K-space structure on S) onto A.*

Proof. The main difficulty is the proof of the first statement of Theorem 5. Our method will be to construct an algebra A quite explicitly which has the properties asserted for V_S and which is eventually shown to be isomorphic with V_S. Let (S, ϕ) be a regular extension of K by T, and equip S with an admissible K-space structure. Let ψ be a map of T into S such as was found in Theorem 4. Let $\sigma_1, \cdots, \sigma_k$ be a basis for T_0 over C such that $\sigma_i^p = \sigma_i$, and put $s_i = \psi(\sigma_i)$. Then $s_i^p = s_i + c_i$, with $c_i \in C$. In the polynomial ring $C[x_1, \cdots, x_k]$, where the x_i are algebraically independent over C, let I be the ideal which is generated by the elements $x_i^p - x_i - c_i$. Put $R = C[x_1, \cdots, x_k]/I$. Then, if z_i denotes the coset of x_i mod I, we have $R = C[z_1, \cdots, z_k]$, $z_i^p = z_i + c_i$, and the monomials $z_1^{e_1} \cdots z_k^{e_k}$, with $0 \leqq e_i < p$, constitute a basis for R over C. Now put $W = K \otimes R$, the tensor product being taken with respect to C and regarded in the natural fashion as a vector space over K. There is evidently a unique C-linear transformation y_i of W such that $y_i(v \otimes r) = \sigma_i(v) \otimes r + v \otimes (z_i r)$, for all $v \in K$ and all $r \in R$. Let A be the ring of C-linear transformations of W which is generated by the scalar multiplications with elements of K and the y_i's. We identify the canonical image of K in A with K. We have $y_i y_j = y_j y_i$, $y_i^p = y_i + c_i$, and, for $v \in K$, $y_i v = v y_i + \sigma_i(v)$. Furthermore, the monomials $y_1^{e_1} \cdots y_k^{e_k}$, with $0 \leqq e_i < p$, are (left) K-linearly independent in A and span A over K. Now every element of S can be written uniquely in the form $s = v_0 + \sum_{i=1}^k v_i s_i$, with $v_j \in K$. We define then $\alpha(s) = v_0 + \sum_{i=1}^k v_i y_i \in A$. If we regard A as a restricted Lie algebra over C in the usual way, we see at once from the regularity condition (i) that α is a Lie algebra isomorphism of S into A, and from the regularity condition (ii) that α is a *restricted* Lie algebra isomorphism. Hence α can be extended uniquely to a homomorphism of U_S^+ *onto* A, which we shall still denote by α. Evidently, α maps the ideal

J of U_S^+ into (0), and since it maps S' isomorphically we have $J \cap S' = (0)$. Hence we may identify S with its canonical image in V_S. Furthermore, α induces a homomorphism γ of V_S onto A which (with the identifications we have made) leaves the elements of K fixed. Clearly, the cosets mod J of the ordered monomials in the elements s_i^j, with non-negative exponents less than p, span V_S over K. Hence the dimension of V_S over K is no greater than that of A, and since γ maps V_S onto A it must therefore be an isomorphism. Hence we may verify the remaining assertions concerning V_S by operating in A.

We write the elements of A as polynomials in the y_i with coefficients in K, the degree in each y_i being at most $p-1$. Let $u_1, \cdots, u_k$ be the elements of K which we have used repeatedly already, so that $\sigma_i(u_j) = \delta_{ij} u_j$. We claim that if $a \in A$ and $au_i - u_i a \in K$ then the degree of a in y_i is at most 1. In fact, write $a = a_0 + a_1 y_i + \cdots + a_q y_i^q$, where the a_j do not contain y_i and $q < p$. Then we find that

$$\begin{aligned} au_i - u_i a &= a_1 u_i + a_2(u_i y_i + y_i u_i) + \cdots \\ &\quad + a_q(u_i y_i^{q-1} + y_i u_i y_i^{q-2} + \cdots + y_i^{q-1} u_i) \\ &= q a_q u_i y_i^{q-1} + \sum_{j=0}^{q-2} b_j y_i^j, \end{aligned}$$

where the b_j do not contain y_i. This shows that our condition on a implies that $a_q = 0$ when $q > 1$, and thus establishes our claim. We can now conclude that S is precisely the set of all $a \in V_S$ for which $D_a(K) \subset K$. At the same time we conclude that the center of V_S is contained in S, and since the only elements of S which commute with all elements of K are the elements of K, we find that the center of V_S is contained in K and hence that it coincides with C. Now let L be any nonzero 2-sided ideal of A, and let $0 \neq a \in L$. Compute $au_i - u_i a$ as above. Our computation shows that if we repeat this a suitable number of times and with suitable indices i we finally obtain a nonzero element of $L \cap K$. Hence $L = A$, and we have shown that A, and therefore V_S, is simple. It is clear from our construction of V_S that the inner derivation effected by an element s in S coincides with $\phi(s)$ on K, and hence that (S, ϕ) is indeed the extension of K by T which is derived from the simple algebra V_S with the maximal commutative subring K.

There remains to prove the last part of Theorem 5. In the notation used there, it is clear that the canonical homomorphism of U_S^+ into A annihilates the ideal J and hence induces a homomorphism of V_S into A. This homomorphism leaves the elements of K fixed, and in particular is not 0. Since V_S is simple, this homomorphism must therefore be an isomorphism of V_S into A. But $[V_S : C] = [K : C]^2 = [A : C]$, because V_S and A are simple and K is a maximal commutative subring of each. Hence our isomorphism maps V_S onto A, and Theorem 5 is proved.

It will be convenient to look upon our results in the following way: We

consider the Brauer similarity classes of the simple finite dimensional algebras with center C which are split by the (fixed) purely inseparable extension K/C of exponent 1. From each of these similarity classes we pick an algebra which contains K as a maximal commutative subring. Any two such representatives of the same class are isomorphic by an isomorphism which leaves the elements of K fixed. Hence the corresponding regular extensions of K by T are equivalent. Thus there results a map ζ of similarity classes of simple algebras into equivalence classes of regular extensions of K by T. By Theorem 5, ζ maps the subgroup of the Brauer group over C whose members are split by K in a $1-1$ fashion onto the set of all equivalence classes of regular extensions of K by T. It is easily seen that the composite (as defined in [2, §3]) of two regular extensions is again regular, so that the equivalence classes of the regular extensions of K by T constitute a subgroup of the group of all restricted extensions of K by T. We shall prove that ζ is actually a group isomorphism.

Let A denote the algebra of all C-linear transformations of K. If we identify the elements of K with the multiplications effected by them in K we may write $K \subset A$, and K is now a maximal commutative subring of A. The algebra A is a representative of the identity element of the Brauer group over C. The corresponding regular extension (S, ϕ) of K by T is simply the following: $S = K + T$, and ϕ is the natural projection of S onto T. This extension is trivial and so represents the 0-element of the group of equivalence classes of the restricted extensions of K by T. Hence, in order to conclude that ζ is a group isomorphism, we must show only that ζ maps the product of two algebra classes into the composite of the corresponding classes of regular extensions of K by T.

In order to do this, we recall a construction which, starting from any simple finite dimensional algebra B with center C and splitting field K, produces a simple finite dimensional algebra A with center C in which K is a maximal commutative subring and which is similar to B. Let B^* be anti-isomorphic with B, by an anti-isomorphism leaving the elements of C fixed. Then B^* is split by K, whence there exists a finite dimensional vector space W over K which has also the structure of a B^*-module such that the B^*-operators are K-linear and the tensor product $K \otimes B^*$ with respect to C is faithfully represented as the ring of all K-linear transformations of W. Then the required algebra A is simply the ring of all those additive endomorphisms of W which commute with each B^*-operator. If (S, ϕ) is the regular extension of K by T which is derived from A, then, since A is similar to B, (S, ϕ) belongs to the class of regular extensions of K by T that corresponds to the similarity class of B. Now it is easily seen that S is precisely the set of all those B^*-endomorphisms s of W for which (with $v \in K$ and $w \in W$) we have $s(vw) = v'w + vs(w)$, where the map $v \to v'$ is a derivation of K, namely the derivation $\phi(s)$.

Now let A_1 and A_2 be simple finite dimensional algebras with center C which are split by K. Let W_1 and W_2 be modules attached to A_1 and A_2, respectively, as W was attached to B above. Then the tensor product $W_1 \otimes W_2$, taken with respect to K, inherits the structure of an $(A_1 \otimes A_2)^*$-module in the natural fashion, and it is clear that $K \otimes (A_1 \otimes A_2)^*$ is thereby faithfully represented as the ring of all K-linear transformations of $W_1 \otimes W_2$. (Symbolically, we have $K \otimes_C (A_1 \otimes_C A_2)^* \approx (K \otimes_C A_1^*) \otimes_K (K \otimes_C A_2^*)$). It follows that the ring A of all $(A_1 \otimes A_2)^*$-endomorphisms of $W_1 \otimes W_2$ is a suitable representative for the similarity class of $A_1 \otimes A_2$. Now let (S_1, ϕ_1) and (S_2, ϕ_2) be the regular extensions of K by T which are derived from W_1 and W_2, respectively, as explained above. Let $s_i \in S_i$ $(i = 1, 2)$ be such that $\phi_1(s_1) = \phi_2(s_2)$. Then there is a unique endomorphism s of $W_1 \otimes W_2$ such that $s(w_1 \otimes w_2) = s_1(w_1) \otimes w_2 + w_1 \otimes s_2(w_2)$. One checks easily that if (S, ϕ) is the regular extension derived from the module $W_1 \otimes W_2$ we have $s \in S$ and $\phi(s) = \phi_1(s_1) = \phi_2(s_2)$. Moreover, writing $s = (s_1, s_2)$, etc., we verify that $[(s_1, s_2), (t_1, t_2)] = ([s_1, s_2], [t_1, t_2])$ and $(s_1, s_2)^p = (s_1^p, s_2^p)$. It is evident that $(s_1, s_2) = 0$ if and only if s_1 and s_2 are both in K and $s_1 = -s_2$ (i.e., s_1 is the multiplication by an element v of K and s_2 is the multiplication by the element $-v$). Hence we see that the dimension of the K-space spanned by the elements (s_1, s_2) with $\phi_1(s_1) = \phi_2(s_2)$ is equal to the dimension of the K-space S_1, and so is also equal to the dimension of S over K, whence we conclude that every element of S is of this form (s_1, s_2). But then it is clear that (S, ϕ) is precisely the composite of (S_1, ϕ_1) and (S_2, ϕ_2). Hence ζ is a group isomorphism, and we have our main result:

THEOREM 6. *The correspondence which attaches to a simple finite dimensional algebra with center C and containing K as a maximal commutative subring a regular extension of K by T induces a group isomorphism of the subgroup of the Brauer group over C whose members are split by K onto the group of equivalence classes of the regular extensions of K by T.*

In view of this result, it is desirable to obtain an explicit description of the group of all regular equivalence classes of extensions of K by T. This is quite easy to do. By Theorem 4, if (S, ϕ) is any regular extension of K by T, there is a K-linear Lie algebra isomorphism ψ of T into K such that $\phi\psi$ is the identity map on T and $\psi(\tau)^p - \psi(\tau^p) \in C$, for every $\tau \in T$. Put $f(\tau) = \psi(\tau)^p - \psi(\tau^p)$. Then, as we have already seen in the proof of Theorem 4, f is an additive homomorphism of T into C and, if $v \in K$, $f(v\tau) = v^p f(\tau)$. We express these properties by saying that f is a p-semilinear map, with respect to K, of T into C. Let us denote the C-space of all such maps by $S_K(T, C)$. We can describe our extension (S, ϕ) as follows. Put $(\tau, v) = \psi(\tau) + v$. Then $\phi(\tau, v) = \tau$, $[(\tau_1, v_1), (\tau_2, v_2)] = ([\tau_1, \tau_2], \tau_1(v_2) - \tau_2(v_1))$, and $(\tau, v)^p = (\tau^p, v^p + \tau^{p-1}(v) + f(\tau))$. Conversely, if f is an arbitrary element of $S_K(T, C)$ these formulas define a regular extension of K by T, an admissible K-space structure being $v(\tau, v_1) = (v\tau, vv_1)$. This is verified easily in a straightforward fashion (referring to

[2] for the discussion of the p-map), except for the regularity condition (ii). In order to verify that (ii) holds, observe that we have

$$\begin{aligned}(v\tau, vv_1)^p &= ((v\tau)^p, (vv_1)^p + (v\tau)^{p-1}(vv_1) + v^p f(\tau))\\ &= (v^p\tau^p + (v\tau)^{p-1}(v)\tau, v^p v_1^p + (v\tau)^{p-1}(vv_1) + v^p f(\tau))\\ &= v^p(\tau, v_1)^p + ((v\tau)^{p-1}(v)\tau, (v\tau)^{p-1}(vv_1) - v^p\tau^{p-1}(v_1))\\ &= v^p(\tau, v_1)^p + t^{p-1}_{v(\tau,v_1)}(v)(\tau, v_1) + (0, (v\tau)^{p-1}(vv_1) - v^p\tau^{p-1}(v_1)\\ &\qquad - (v\tau)^{p-1}(v)v_1).\end{aligned}$$

This shows that condition (ii) is equivalent to the condition $(v\tau)^{p-1}(vv_1) = v^p\tau^{p-1}(v_1) + (v\tau)^{p-1}(v)v_1$. In order to prove this identity we merely have to consider the ring $K[x]$, where x is transcendental over K, and observe that τ can be extended to a derivation of $K[x]$ (still denoted τ) such that $\tau(x) = v_1$. Then we have $(v\tau)^{p-1}(vv_1) = (v\tau)^p(x)$ which, by Lemma 1, is equal to $v^p\tau^p(x) + (v\tau)^{p-1}(v)\tau(x) = v^p\tau^{p-1}(v_1) + (v\tau)^{p-1}(v)v_1$.

If we have two such regular extensions, defined by elements f_1 and f_2 in $S_K(T, C)$, we can verify directly from the definition that the composite extension is the extension defined by $f_1 + f_2$. Hence the above construction yields a homomorphism of $S_K(T, C)$ onto the group of equivalence classes of the regular extensions of K by T. There remains only to determine the kernel of this homomorphism.

Suppose that $f \in S_K(T, C)$ and that the corresponding extension (S, ϕ) is trivial. By Theorem 4 there exists a restricted Lie algebra isomorphism γ of T into S which is inverse to ϕ and furthermore K-linear. Put $\gamma(\tau) = (\tau, h(\tau))$. Then h is a K-linear map of T into K. Since γ is a Lie algebra isomorphism, we must have $\tau_1(h(\tau_2)) - \tau_2(h(\tau_1)) = h([\tau_1, \tau_2])$ which means that h belongs to the space $Z_K(T, K)$ of the K-linear 1-cocycles for T in K. Since γ is restricted, we must have $(\tau, h(\tau))^p = (\tau^p, h(\tau^p))$ which means that $f(\tau) = h(\tau^p) - h(\tau)^p - \tau^{p-1}(h(\tau)) = h'(\tau)$, say. We know already from [2, p. 571] that if h is any 1-cocycle for T in K then h' is p-semilinear with respect to C, and so, in particular, is additive and takes values in C. If, furthermore, h is K-linear we find that

$$h'(v\tau) = v^p h(\tau^p) + (v\tau)^{p-1}(v)h(\tau) - v^p h(\tau)^p - (v\tau)^{p-1}(vh(\tau))$$

which, by the identity we have proved above, reduces to $v^p h'(\tau)$. Hence $h' \in S_K(T, C)$. By reversing the above computation we see that if f is of the form h' with $h \in Z_K(T, K)$ then the corresponding regular extension of K by T is trivial. Hence we have the following result.

THEOREM 7. *If, for $h \in Z_K(T, K)$, we denote by h' the map given by $h'(\tau) = h(\tau^p) - h(\tau)^p - \tau^{p-1}(h(\tau))$, then $h' \in S_K(T, C)$. The group of equivalence classes of the regular extensions of K by T is isomorphic with the factor group of $S_K(T, C)$ modulo the image of $Z_K(T, K)$ by the map $h \to h'$.*

If we abandon the invariant nature of our description of the regular extension group, we can obtain something much more explicit. Let $\sigma_1, \cdots, \sigma_k$ be a basis for (T_0 over C and hence for) T over K such as we used in the beginning. Then an element f in $S_K(T, C)$ is completely determined by the images $c_i = f(\sigma_i)$. Hence $S_K(T, C)$ may be identified with the group of all vectors $(c_1, \cdots, c_k)$ in C^k. Now suppose that f is of the form h'. Put $h(\sigma_i) = v_i \in K$. Since h is K-linear, the vector $(v_1, \cdots, v_k)$ in K^k determines h completely. The condition that h be a 1-cocycle becomes simply $\sigma_i(v_j) = \sigma_j(v_i)$, for all i and j. We have $c_i = f(\sigma_i) = h'(\sigma_i) = v_i - v_i^p - \sigma_i^{p-1}(v_i)$. Thus our group of regular extension classes is isomorphic with C^k/D, where D is the subgroup consisting of all vectors whose components are of the form $v_i - v_i^p - \sigma_i^{p-1}(v_i)$, where $v_i \in K$ and $\sigma_i(v_j) = \sigma_j(v_i)$, for all i and j.

References

1. G. Hochschild, *Double vector spaces over division rings*, Amer. J. Math. vol. 71 (1949) pp. 443–460.

2. ———, *Cohomology of restricted Lie algebras*, Amer. J. Math. vol. 76 (1954) pp. 555–580.

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

4. ———, *Galois theory of purely inseparable fields of exponent* 1, Amer. J. Math. vol. 66 (1944) pp. 645–648.

University of Illinois,
Urbana, Ill.