RESTRICTED LIE ALGEBRAS AND SIMPLE ASSOCIATIVE ALGEBRAS OF CHARACTERISTIC p

BY

G. HOCHSCHILD

Introduction. Let F be a field of characteristic p, and let C be a finite algebraic extension field of F such that $C^p \subset F$. It has been shown in [4] that there is a one to one correspondence (up to isomorphisms) between the simple finite dimensional algebras with center F and containing C as a maximal commutative subring and the regular restricted Lie algebra extensions of C by the derivation algebra of C/F. This led to a very simple description of the group of similarity classes of these algebras. The main task of the present paper is to investigate the connection between restricted Lie algebras and simple associative algebras of characteristic p quite generally. For this purpose, we generalize the notion of a regular extension of C by the derivation algebra of C/F to that of a regular extension of a simple algebra A with center C by the derivation algebra of C/F. The correspondence mentioned above is then generalized to a one to one correspondence between these extensions and the simple algebras with center F which contain A as the commutator algebra of C (Theorem 3). We shall then show how every simple algebra containing a purely inseparable extension field of its center as a maximal commutative subring can be built up in a series of steps from regular Lie algebra extensions. With a suitable composition of regular extensions, which we define in §2, this reduces the structure of the group of algebra classes with a fixed purely inseparable splitting field to the structural elements of restricted Lie algebras, at least in principle. However, it does not yield a direct description of this group, as was the case for splitting fields of exponent one.

In §3 we show that the tensor multiplication with a purely inseparable extension field C of F maps the Brauer group of algebra classes over F *onto* the Brauer group over C (Theorem 5). Although this result seems not to have been stated before, it may well be regarded as one of the culminating points of Albert's theory of p-algebras. In fact, Chapter VII of [1] contains all the essential points of a proof along classical lines, which is the first proof we give in §3. Here, the main tools are Galois theory and the theory of cyclic p-extensions. Our second proof is entirely different. It proceeds within the framework of the first part of this paper, replacing the field theory with the theory of Lie algebras. In particular, we use the theory of restricted Lie algebra kernels, [3], in order to show that if A is a simple algebra with center C and $C^p \subset F$ then there always exists a regular extension of A by the derivation algebra of C/F, whence (by Theorem 3) A can be imbedded as the

commutator algebra of C in a simple algebra with center F. Theorem 5 then follows almost immediately.

1. **Regular extensions.** Let F be a field of characteristic $p \neq 0$, and let C be a finite algebraic extension of F such that $C^p \subset F$. Let T be the derivation algebra of C/F, regarded as a restricted Lie algebra over F. Observe that T has also the structure of a vector space over C in the natural way. The scalar multiplications are connected with the commutation in T by the identity $[c_1 t_1, c_2 t_2] = c_1 t_1(c_2) t_2 - c_2 t_2(c_1) t_1 + c_1 c_2 [t_1, t_2]$, where $c_i \in C$ and $t_i \in T$. Furthermore, by Lemma 1 of $[4]$, the scalar multiplications are connected with the pth power map in T by the identity $(ct)^p = c^p t^p + (ct)^{p-1}(c)t$.

Now let A be a simple associative algebra with center C. Let S be a restricted Lie algebra over F, and suppose that A, with its natural structure as a restricted Lie algebra over F, is contained as an ideal in S in such a way that, for every $s \in S$, the restriction to A of the inner derivation effected by s is even a derivation of the associative algebra A, i.e., that for all $a_i \in A$, we have

(*) $$[s, a_1 a_2] = [s, a_1]a_2 + a_1[s, a_2].$$

Then these derivations map C into itself, and if $\phi(s)$ denotes the restriction to C of the inner derivation effected by s, ϕ is a restricted Lie algebra homomorphism of S into T. We shall say that the pair (S, ϕ) constitutes a *regular extension* of A by T if the kernel of ϕ coincides with A, $\phi(S) = T$, and S can be given the structure of a vector space over C, extending the C-space structure of A, such that ϕ is C-linear and the following regularity conditions hold, for all c, c_i in C and all s, s_i in S:

(i) $$[c_1 s_1, c_2 s_2] = c_1 \phi(s_1)(c_2)s_2 - c_2 \phi(s_2)(c_1)s_1 + c_1 c_2 [s_1, s_2];$$

(ii) $$(cs)^p = c^p s^p + \phi(cs)^{p-1}(c)s.$$

Such a C-space structure on S will then be called an *admissible C-space structure*. We say that two such regular extensions of A by T are *equivalent* if there exists a restricted Lie algebra isomorphism α of S onto S' which leaves the elements of A fixed and for which $\phi'\alpha = \phi$.

If B is a simple finite dimensional algebra with center F and containing C then the commutator algebra A of C in B is simple and has center C. Let S be the set of all elements $s \in B$ for which $sc - cs \in C$ whenever $c \in C$, and let $\phi(s)$ denote this derivation $c \rightarrow sc - cs$ of C. Then it is easily seen (using Lemma 1 of $[4]$ in order to verify condition (ii)) that (S, ϕ) is a regular extension of A by T.

In order to deal adequately with regular extensions we require the following auxiliary notion. A simple finite dimensional algebra A with center C may be regarded as a full matrix algebra D_n where D is division algebra with center C. There exists a separable extension field Z of C which is a maximal

commutative subring of D. Let R denote the subring of A which consists of all those matrices whose diagonal entries lie in Z and whose other entries are 0. Then R contains C and is C-isomorphic with the direct sum of n copies of Z. Thus R is a separable commutative algebra over C. Furthermore, R is a maximal commutative subring of A. Generally, if R is any maximal commutative subring of A which contains C and is separable over C, we shall say that R is a *regulator* of A. We have then $CR^p = R$, and if F is a subfield of C as above, FR^p is separable over F.

THEOREM 1. *Let F be a field of characteristic $p \neq 0$, C a finite algebraic extension field of F such that $C^p \subset F$, T the derivation algebra of C/F. Let A be a simple finite dimensional algebra with center C, and let (S, ϕ) be a regular extension of A by T. Then, for any regulator R of A and any admissible C-space structure of S, there exists a C-linear Lie algebra isomorphism ψ of T into S such that, for any $t \in T$, $\phi\psi(t) = t$, the inner derivation $D_{\psi(t)}$ effected by $\psi(t)$ maps R into itself, and $\psi(t)^p - \psi(t^p) \in R^p$.*

Proof. Let S' be the restricted subalgebra of S which consists of all those elements $s \in S$ for which $D_s(R) \subset R$. Since R is separable over C, every derivation t of C can be extended (uniquely) to a derivation t' of R. Let $s \in S$ and consider the restriction to R of D_s; call this δ_s. Then $\delta_s - \phi(s)'$ is a derivation of R into A which annihilates C. Since R is a semisimple subalgebra of A, we can apply a well known result of Jacobson's[1] to conclude that there is an element $a \in A$ such that $\delta_s - \phi(s)'$ coincides with δ_a. Now $\delta_{s-a} = \phi(s)'$ and therefore maps R into itself, which means that $s - a \in S'$. Hence $\phi(S') = T$, and if ϕ' denotes the restriction of ϕ to S' then (S', ϕ') is a restricted Lie algebra extension of $A \cap S'$ by T. Since R is commutative, every derivation of R annihilates R^p. Hence every element of $A \cap S'$ commutes with every element of R^p, and therefore also with every element of $CR^p = R$. Hence $A \cap S' = R$, so that (S', ϕ') is a regular extension of R by T. Now the proof of Theorem 4 of [4] applies without any changes to this extension (S', ϕ') and gives the desired result.

Furthermore, one can now proceed exactly as in that proof to obtain:

THEOREM 2. *Let (S, ϕ) and (S', ϕ') be any two equivalent regular extensions of A by T. Then, for any given admissible C-space structures of S and S', there is a C-linear equivalence isomorphism of S onto S'.*

Let (S, ϕ) be a regular extension of A by T, and let U_S denote the restricted universal enveloping algebra of the restricted Lie algebra S[2]. Let U_S^+ denote the ideal of U_S which is generated by the canonical images s' in U_S of the elements $s \in S$. Now equip S with an admissible C-space structure,

---

([1]) See Theorem 7 of [5], or Theorem 3 of [4].

([2]) For this notation, and for the results we take from the theory of restricted Lie algebras (due to Jacobson) and their cohomology groups, see [2].

and let J be the ideal of U_S^+ which is generated by the elements of the form $c's' - (cs)'$, with $c \in C$ and $s \in S$. Put $V_S = U_S^+/J$. Then V_S is a finite dimensional associative algebra over F. It is clear from Theorem 2 that, although the construction of V_S involves the choice of an admissible C-space structure on S, V_S is determined up to an isomorphism by the equivalence class of the extension (S, ϕ). More precisely, if α is a C-linear equivalence isomorphism of (S, ϕ) onto (S', ϕ'), then α induces an isomorphism α^* of V_S onto $V_{S'}$, such that if ρ and ρ' are the natural maps of S into V_S and of S' into $V_{S'}$, respectively, we have $\alpha^*\rho = \rho'$. We are now in a position to prove the following generalization of Theorem 5 of [4].

THEOREM 3. *Let (S, ϕ) be a regular extension of A by T. Then the canonical map of S into V_S is $1-1$, and its restriction to A is an associative algebra isomorphism by means of which we identify A with a subalgebra of V_S. V_S is then a finite dimensional simple algebra with center F, and A is the commutator algebra of C in V_S. Furthermore, the canonical image of S in V_S coincides with the set of all elements $v \in V_S$ for which $D_v(C) \subset C$, and the corresponding regular extension of A by T is equivalent with (S, ϕ) by the canonical map of S into V_S. Conversely, if B is a finite dimensional simple algebra with center F and containing C, if A is the commutator algebra of C in B, and if (S, ϕ) is the resulting regular extension of A by T, then the homomorphism of U_S^+ into B which extends the injection $S \to B$ induces an isomorphism of V_S onto B.*

Proof. We have $C = F[u_1, \cdots, u_k]$ and corresponding derivations $t_1, \cdots, t_k$ of C such that $t_i(u_j) = \delta_{ij}u_j$, whence $t_it_j = t_jt_i$ and $t_i^p = t_i$. (Cf. §1 of [4]). Let R be a regulator of A, and let ψ be a C-linear Lie algebra isomorphism of T into S such as is given by Theorem 1. Write $\psi(t_i) = s_i$. Then $s_i^p = s_i + r_i$, with $r_i \in R^p$. Put $FR^p = R_0$, and construct the commutative polynomial ring $R_0[x_1, \cdots, x_k]$ in elements x_i which are algebraically independent over R_0. Let I be the ideal of this polynomial ring which is generated by the elements $x_i^p - x_i - r_i$. Then $R_0[x_1, \cdots, x_k]/I = R_0[y_1, \cdots, y_k]$, where y_i is the coset of x_i, so that $y_i^p = y_i + r_i$. Put $V = A \otimes_{R_0} R_0[y_1, \cdots, y_k]$, this tensor product being taken for the natural structure of A as a right R_0-module and the natural structure of $R_0[y_1, \cdots, y_k]$ as a left R_0-module. We regard V as a left A-module in the natural fashion. Since the inner derivation effected by s_i maps R into itself, it must annihilate R^p and hence R_0. It follows that there is a unique additive endomorphism z_i of V such that, for $a \in A$ and $y \in R_0[y_1, \cdots, y_k]$, $z_i(a \otimes y) = [s_i, a] \otimes y + a \otimes y_iy$. We may identify the elements of A with the module operations they effect in V, and it is easy to check that we have then $z_ia - az_i = [s_i, a]$, and $z_i^p = z_i + r_i$. Also, we evidently have $z_iz_j = z_jz_i$. Let M be the ring of endomorphisms of V which is generated by the z_i and the elements of A. Then it is easily seen that the monomials $z_1^{e_1} \cdots z_k^{e_k}$, with $0 \le e_i < p$, are (left) A-independent in M and span M over A.

Now consider an element of M, writing it in the form $m = m_0 + m_1z_i + \cdots$

$+m_q z_i^q$, where $q < p$ and the m_r are A-linear combinations of monomials in the z_j with $j \neq i$. Then the m_r commute with u_i, and it follows that $mu_i - u_i m = qm_q u_i z_i^{q-1} + m'$, where m' is of degree less than $q-1$ in z_i. It is easily seen from this that if m commutes with every element of C then $m \in A$. Hence the commutator algebra of C in M coincides with A. At the same time we see that the center of M is contained in A, and hence also in the center C of A. Since a central element commutes with every z_i, and since an element of C which is annihilated by each t_i must belong to F, it follows that the center of M coincides with F. Finally, by repeatedly forming $mu_i - u_i m$ (with suitable choices of the index i at each stage), starting with any nonzero element m, we eventually find a nonzero element of A which belongs to the ideal MmM. Since A is simple, we conclude then that $1 \in MmM$, whence $MmM = M$. Thus M is simple.

Now every element of S can be written uniquely in the form

$$s = a + \sum_{i=1}^{k} c_i s_i,$$

where $a \in A$ and $c_i \in C$. We define a C-linear map α of S into M by setting $\alpha(s) = a + \sum_{i=1}^{k} c_i z_i$. If we regard M as a restricted Lie algebra over F in the usual way, we see from the regularity conditions (*) and (i) that α is a Lie algebra isomorphism, and from the regularity condition (ii) that α is even a *restricted* Lie algebra isomorphism. Hence α can be extended uniquely to a homomorphism of U_S^+ into M which is evidently onto and annihilates the ideal J by means of which we have defined V_S. Hence the canonical map of S into V_S, which is a right factor of α, must be 1-1. Clearly, the ordered monomials in the canonical images of the s_i in V_S, with non-negative exponents less than p, span V_S over the canonical image of A in V_S. Hence we have the dimensionality relations $[V_S : F] \leq p^k [A : F] = [M : F]$. It follows that the homomorphism of V_S onto M which is induced by α is actually an isomorphism. Hence we may identify A with its canonical image in V_S, and V_S is a simple algebra with center F which contains A as the commutator algebra of C. Furthermore, if m is an element of M such that $mc - cm \in C$, for every $c \in C$, our above computation of $mu_i - u_i m$ shows that $m \in \alpha(S)$. Hence S may be identified with the set of all $v \in V_S$ for which $D_v(C) \subset C$, and then the corresponding regular extension of A by T evidently coincides with (S, ϕ).

There remains only to prove the last part of Theorem 3. It is evident that the canonical homomorphism of U_S^+ into B which extends the injection $S \to B$ annihilates J and therefore induces a homomorphism of V_S into B which evidently leaves the elements of A fixed. Since we know already that V_S is simple, we may conclude that this homomorphism is an isomorphism of V_S into B. Also, we know that $[V_S : F] = p^k [A : F] = [C : F][A : F]$, and since A is the commutator algebra of C in B we have $[C : F][A : F] = [B : F]$. Hence $[V_S : F] = [B : F]$, whence our isomorphism must map V_S onto B. This com-

pletes the proof of Theorem 3.

Now let A be a simple algebra with center F which contains a purely inseparable extension field C of F as a maximal commutative subring. We can insert a sequence of fields $F = C^{(e)} \subset C^{(e-1)} \subset \cdots \subset C^{(0)} = C$ such that $F(C^{(r-1)})^p = C^{(r)}$, for each r. Let $A^{(r)}$ be the commutator algebra of $C^{(r)}$ in A, and let $S^{(r)}$ be the set of all elements $a \in A$ for which $D_a(C^{(r)}) \subset C^{(r)}$. If $T^{(r)}$ denotes the derivation algebra of $C^{(r)}/C^{(r+1)}$, we have in the natural way the regular extensions $(S^{(r)}, \phi^{(r)})$ of $A^{(r)}$ by $T^{(r)}$. It follows at once from Theorem 3 that $V_S{}^{(r)}$ is isomorphic with $A^{(r+1)}$ by the map which extends the injection of $S^{(r)}$ into $A^{(r+1)}$. In particular, we conclude that *the subalgebra of A which is generated by the elements of $S^{(r)}$ coincides with $A^{(r+1)}$*. Moreover, it is now clear how A can be built up from C by a sequence of regular extensions. If $C^p \subset F$ we have $e = 1$, and we know from [4] that our construction establishes an isomorphism between the group of similarity classes of the simple algebras split by C and the group of equivalence classes of the regular extensions of C by T. It is therefore of interest to generalize the composition of regular extensions of C by T to a composition of our present more general regular extensions. This is the purpose of the next section.

2. Composites of regular extensions. Suppose we are given two regular extensions (S, ϕ) and (S', ϕ') of simple algebras A and A', with the common center C, by the same derivation algebra T of C/F. We shall define a composite regular extension of $A \otimes_C A'$ by T. Let D be the restricted subalgebra of the direct sum (S, S') of S and S' which consists of all elements (s, s') in which $\phi(s) = \phi'(s')$. Corresponding to each element $d = (s, s')$ of D, there is a unique derivation δ_d of $A \otimes_C A'$ such that $\delta_d(a \otimes a') = [s, a] \otimes a' + a \otimes [s', a']$. The map $d \to \delta_d$ is clearly a restricted Lie algebra homomorphism of D into the derivation algebra of $A \otimes_C A'$, relative to F. Now we regard $A \otimes_C A'$ as a restricted Lie algebra over F and use δ for defining the semidirect sum $U = (A \otimes_C A', D)_\delta$. The commutation in U is given by the formula

$$[(x_1, d_1), (x_2, d_2)] = (x_1 x_2 - x_2 x_1 + \delta_{d_1}(x_2) - \delta_{d_2}(x_1), [d_1, d_2]),$$

where $x_i \in A \otimes_C A'$ and $d_i \in D$. It is known from the elementary theory of restricted Lie algebras that there is one and only one p-map in U which coincides with the given p-maps on the ideal $A \otimes_C A'$ and on the complementary subalgebra D. When equipped with this p-map, U is a restricted Lie algebra containing $A \otimes_C A'$ as a restricted ideal in such a way that the regularity condition (*) is satisfied. Now let V be the subspace of U which is spanned by the elements $(a \otimes 1, -(a, 0))$, with $a \in A$, and the elements $(1 \otimes a', -(0, a'))$, with $a' \in A'$. It is easily verified that V is a restricted ideal in U. We put $E = U/V$. The canonical map of $A \otimes_C A'$ into E is evidently an isomorphism by means of which we shall identify $A \otimes_C A'$ with a restricted ideal of E. The homomorphism ϕ (or ϕ') induces a restricted homomorphism ψ of E onto T whose kernel clearly coincides with $A \otimes_C A'$. Hence (E, ψ) is a

restricted extension of $A \otimes_C A'$ by T which evidently satisfies the regularity condition (*). Furthermore, any admissible C-space structures on S and S' induce a C-space structure on U, and hence on E, which evidently satisfies the regularity condition (i). In order to see that the regularity condition (ii) is also satisfied, we must make a precise analysis of the p-map. We must show that $(ce)^p = c^p e^p + D_{ce}^{p-1}(c)e$, for all $c \in C$ and all $e \in E$. This holds clearly if $e \in A \otimes_C A'$, and also if e is the canonical image in E of an element of D. Hence it suffices to prove that if the formula holds for $e = e_1$ and for $e = e_2$ then it holds also for $e = e_1 + e_2$. In order to do this, we consider the ordinary universal enveloping algebra R_E of E. Let I be the ideal of R_E which is generated by the elements $c'e' - (ce)'$, for $e \in E$ and $c \in C$, where $e \to e'$ denotes the canonical isomorphism of E into R_E. If e_1 is any other element of E, we have

$$e_1'(c'e' - (ce)') - (c'e' - (ce)')e_1' = e_1'c'e' - c'e'e_1' + [ce, e_1]'$$
$$= c'[e_1, e]' - (c[e_1, e])' + [e_1, c]'e' - ([e_1, c]e)'.$$

Hence I actually coincides with the *right* ideal which is generated by the elements $c'e' - (ce)'$. Hence we see easily that $I \cap E' = (0)$, so that we may identify the C-space E with a subspace of R_E/I. Now let us momentarily indicate the p-map in E by $e \to e^{[p]}$, and let e^p stand for the pth power of e as an element of R_E/I, i.e., e^p now denotes the coset mod I of $(e')^p$. Observe that, by our definition of I, we have $c^{[p]} = c^p$, for every $c \in C$. It follows at once from the definition of a p-map in a restricted Lie algebra that the map $e \to e^p - e^{[p]}$ of E into R_E/I is additive. If we apply Lemma 1 of [4] in R_E/I we find that $(ce)^p = c^p e^p + D_{ce}^{p-1}(c)e$, for all $c \in C$ and all $e \in E$. Now suppose that e_1 and e_2 are elements of E which satisfy our regularity condition (ii), i.e., in our present notation, $(ce_i)^{[p]} = c^p e_i^{[p]} + D_{ce_i}^{p-1}(c)e_i$. In R_E/I, we have

$$(c(e_1 + e_2))^{[p]} = (c(e_1 + e_2))^p - (ce_1)^p - (ce_2)^p + (ce_1)^{[p]} + (ce_2)^{[p]}.$$

If we expand the first three terms on the right by using the regularity of R_E/I as noted above, and the last two terms by using our hypothesis that (ii) holds for e_1 and e_2, we find, on recombining the terms, that (ii) holds for $e_1 + e_2$. Hence (E, ψ) is a regular extension of $A \otimes_C A'$ by T.

THEOREM 4. *Let (E, ψ) be the composite of two regular extensions (S, ϕ) and (S', ϕ'). Then V_E is similar to $V_S \otimes_F V_{S'}$.*

Proof. Let V_S^* be the algebra of the right multiplications in V_S, and regard V_S as a module for $V_S \otimes_F V_S^*$ in the natural fashion. Since V_S is simple with center F, $V_S \otimes_F V_S^*$ is thereby faithfully represented as the algebra of all F-linear transformations of V_S. Now let A be the kernel of ϕ, so that A is the commutator algebra of its center C in V_S. Then our representation of $V_S \otimes_F V_S^*$ maps $A \otimes_F V_S^*$ isomorphically onto the algebra of all C-linear trans-

formations of V_S, where we regard V_S as a vector space over C, with C operating by left multiplication on V_S. Similarly, we represent $A' \otimes_F V_{S'}^*$ as the algebra of all C-linear transformations of $V_{S'}$. Now let W be the tensor product, relative to C, of the C-spaces V_S and $V_{S'}$; thus, W is obtained from $V_S \otimes_F V_{S'}$ by reducing mod the subspace spanned by the elements $cv \otimes v' - v \otimes cv'$, with $c \in C$, $v \in V_S$, and $v' \in V_{S'}$. The corresponding tensor product of our representations of $A \otimes_F V_S^*$ and $A' \otimes_F V_{S'}^*$ defines the structure of a module for $(A \otimes_F V_S^*) \otimes_C (A' \otimes_F V_{S'}^*)$ on W, and represents this algebra faithfully as the algebra of all C-linear transformations of W. We can write our tensor product in the form $(A \otimes_C A') \otimes_F (V_S^* \otimes_F V_{S'}^*)$ and accordingly regard W as a module for $V_S^* \otimes_F V_{S'}^*$. This gives an imbedding of $A \otimes_C A'$ in the algebra B of all $V_S^* \otimes_F V_{S'}^*$ endomorphisms of W, whereby $A \otimes_C A'$ is identified with the commutator algebra of C in B. By a standard result of the theory of representations of simple algebras, B is similar to $V_S \otimes_F V_{S'}$. Hence it will suffice to prove that V_E is isomorphic with B. In doing this, we shall use the notation of the definition of (E, ψ). An element (s, s') of D determines a unique element of B which sends an element $v \otimes v'$ of W into $sv \otimes v' + v \otimes s'v'$. If this map of D into B is augmented by the canonical injection of $A \otimes_C A'$ into B, there results a restricted Lie algebra homomorphism of U into B whose kernel is easily seen to coincide with V. Hence we obtain a restricted Lie algebra isomorphism β of E into B which leaves the elements of $A \otimes_C A'$ fixed. Since $A \otimes_C A'$ is the commutator algebra of C in B, the regular extension corresponding to the pair $C \subset B$ is a regular extension (R, ρ) of $A \otimes_C A'$ by T, and we have evidently $\beta(E) \subset R$ and $\rho\beta = \psi$. This is enough to conclude that β is an equivalence isomorphism of (E, ψ) onto (R, ρ). Hence V_E is isomorphic with V_R, which is isomorphic with B, by Theorem 3. This completes the proof of Theorem 4.

Now let B_F denote the group of similarity classes of the simple algebras with center F, and similarly define B_C, where C is an extension field of F with $C^p \subset F$. The map $A \to A \otimes_F C$ induces a homomorphism γ of B_F into B_C whose kernel is the group $B_F(C)$ of the similarity classes of those simple algebras with center F which are split by C. We shall show in the next section that $\gamma(B_F) = B_C$. For the moment, we merely recall the well known fact that, quite generally, *the similarity class of an algebra A with center C belongs to* $\gamma(B_F)$ *if and only if there exists a simple algebra U with center F such that A is contained as the commutator algebra of C in U.* In fact, suppose first that such an algebra U exists. We may regard U as a module for $C \otimes_F U^*$ in the natural way. Then we see that A may be identified with the algebra of all $C \otimes_F U^*$-endomorphisms of U, whence it follows that A is similar to $U \otimes_F C$. Conversely, let us suppose that there is a simple algebra V with center F such that A is similar to $A' = V \otimes_F C$. Put $[C:F] = n$. Then we can imbed C in the full matrix algebra F_n over F so that it coincides with its own commutator algebra in F_n. Hence we can identify A' with the commutator algebra of C

in $V \otimes_F F_n$. Since A is similar to A', there are positive integers m and m' such that the full matrix algebra A_m over A is isomorphic with $A'_{m'}$. Since A' is the commutator algebra of C in $V \otimes_F F_n = V_n$, $A'_{m'}$ may be identified with the commutator algebra of C in $(V_n)_{m'} = V_{nm'}$. Since $A'_{m'}$ is isomorphic with A_m, it contains a copy of F_m, and therefore $V_{nm'}$ contains a copy of F_m. Hence we may write $V_{nm'} = U \otimes_F F_m$, where U is the commutator algebra of this copy of F_m in $V_{nm'}$. Since A is the commutator algebra of F_m in A_m, our isomorphism of A_m into $V_{nm'}$ (via $A'_{m'}$) must map A into U. Finally, since A is the commutator algebra of C_m in A_m, the image of A in $U \otimes_F F_m$ is the commutator algebra of $C \otimes_F F_m$ in the image of A_m, i.e., in the commutator algebra of C in $U \otimes_F F_m$ which, in any case, must contain the commutator algebra of $C \otimes_F F_m$. Hence the image of A is the commutator algebra of $C \otimes_F F_m$ in $U \otimes_F F_m$, i.e., the commutator algebra of C in U. This completes the proof of the characterization of $\gamma(B_F)$, in the general case.

Now let A be a simple algebra with center C, and suppose that the similarity class of A belongs to $\gamma(B_F)$. By the above, every similarity class in B_F which maps into the similarity class of A has a unique (to within isomorphisms) representative U such that A is contained in U as the commutator algebra of C. Hence, by Theorem 3, *the preimage in B_F of the similarity class of A is in one to one correspondence with the set of equivalence classes of the regular extensions of A by T. The coset structure of this preimage, with respect to the subgroup $B_F(C)$, is reflected in the set of equivalence classes of the regular extensions of A by T by their composition with the regular extension classes of C by T,* as follows at once from Theorem 4. Furthermore, if A' is a second simple algebra with center C, then *the preimage in B_F of the similarity class of $A \otimes_C A'$ is represented by the composites of the regular extensions of A by T with the regular extensions of A' by T.*

Next we observe that *an algebra A with center C is of the form $U \otimes_F C$, where U is a simple algebra with center F if and only if there exists a trivial regular extension of A by T.* Indeed, it is evident that $U \otimes_F C$ has a trivial extension by T. Conversely, suppose that (S, ϕ) is a trivial extension of A by T. This means that there exists a restricted Lie algebra isomorphism ψ of T into S such that $\phi\psi$ is the identity map of T onto itself. Then $\psi(T) + C$ is a restricted subalgebra of S which, together with the restriction of ϕ to $\psi(T) + C$, constitutes a trivial regular extension of C by T. The corresponding simple algebra with center F is evidently a subalgebra of V_S. On the other hand, we know from [4] that it is the full matrix algebra F_n, where $n = [C : F]$. Hence we may write $V_S = U \otimes_F F_n$, where U is the commutator algebra of F_n in V_S. Now C is contained in F_n and coincides with its commutator algebra in F_n, while A is the commutator algebra of C in V_S. Hence $A = U \otimes_F C$, and clearly U is simple with center F.

3. Existence of regular extensions and related questions. It is clear from the above that the following result implies the existence of regular extensions.

THEOREM 5. *Let F be a field of characteristic p, and let C be a finite algebraic extension of F which is purely inseparable over F. Then every finite dimensional simple algebra A with center C is similar to a tensor product $B \otimes_F C$, where B is a simple algebra with center F.*

Proof. The algebra A is similar to a tensor product $U \otimes_C V$, where the exponent of U (in the group of algebra classes over C) is not divisible by p, while the exponent of V is a power p^n of p. Furthermore, we may take U to be a crossed product, and it suffices to prove Theorem 5 in the two cases $A = U$, or $A = V$. The case $A = U$ is quite easy. We write $U = Z(G, f)$, where Z/C is a normal extension with Galois group G, and f is a factor set for G in Z. Let u denote the exponent of U. Then f^u is a trivial factor set. Let e be the exponent of C relative to F, so that $C^{p^e} \subset F$. Since p does not divide u, we can find integers a and b such that $au + bp^e = 1$. Then the factor set f^{bp^e} is equivalent to f and takes its values in Z^{p^e}. Since $C^{p^e} \subset F$, and Z is separable over C, Z is isomorphic with $FZ^{p^e} \otimes_F C$. Furthermore, FZ^{p^e} is normal over F, and the restriction map sends G isomorphically onto the Galois group of FZ^{p^e}/F, which we may therefore identify with G. But then we can form the crossed product $FZ^{p^e}(G, f^{bp^e}) = U'$, say; and clearly U is isomorphic with $U' \otimes_F C$. Now consider the more difficult case $A = V$. Since V has exponent p^n, V has a cyclic normal splitting field of degree a power of p. This is shown in Chap. VII of [1]. Actually, it suffices to use the easier result that V is similar to a tensor product of cyclic crossed products of degree a power of p. In any case, it suffices to dispose of the case where V is a crossed product of a cyclic extension field Z of C, with $[Z:C] = p^t$. The case $t = 0$ being trivial, we have to dispose of the case $t > 0$. But then it is known from Albert's theorem on cyclic extensions of p-power degree of a field of characteristic p that there exists a cyclic extension Y/C such that $Z \subset Y$ and $[Y:C] = p^{t+e}$. Let σ be a generator for the Galois group of Y/C, and let σ' be the restriction of σ to Z. Then σ' is a generator for the Galois group of Z/C, and we have $V = Z(\sigma', c)$, with $c \in C$. Now $Z \subset Y$ and $[Y:Z] = p^e$. Hence, by a well-known result on cyclic algebras, V is similar to the crossed product $Y(\sigma, c^{p^e})$. (See Lemma 11, Chap. VII of [1]; this result is due to Albert, and Hasse). Since $c^{p^e} \in F$, we can now make the same argument as above (for U) to conclude that V is similar to $FY^{p^e}(\sigma, c^{p^e}) \otimes_F C$. This completes the proof of Theorem 5.

Theorem 5 implies that every derivation of C/F can be extended to a derivation of A. Actually, a more general result on derivations holds over arbitrary fields (also in characteristic 0) and can be proved in a completely elementary fashion. Our result extends Jacobson's result, which we have already used in the proof of Theorem 1, that if A is a finite dimensional simple algebra with center C, and if B is a semisimple subalgebra of A containing C, then every derivation of B into A which annihilates C can be extended to an inner derivation of A.

THEOREM 6[3]. *Let A be a simple algebra of finite dimension over its center C, and let B be a semisimple subalgebra of A containing C. Then every derivation of B into A which maps C into itself can be extended to a derivation of A.*

Proof. We observe first that it will suffice to prove that every derivation of C can be extended to a derivation of A. Indeed, let t be a derivation of B into A which maps C into itself, and let t_C be the restriction of t to C. Suppose that t_C can be extended to a derivation s of A, and let s_B be the restriction of s to B. Then $t - s_B$ is a derivation of B into A which annihilates C, and hence, by the result of Jacobson's cited above, can be extended to a derivation u of A. Now $s + u$ is a derivation of A whose restriction to B coincides with t.

The extendability of a derivation of C to a derivation of A depends only on the similarity class of A. For, suppose that a given derivation t of C can be extended to a derivation t' of a simple algebra A' which is similar to A. There are positive integers m and m' such that A_m is isomorphic with $A'_{m'}$. Let $t'_{m'}$ be the map of $A'_{m'}$ into itself which sends the matrix with entries a'_{ij} into the matrix with entries $t'(a'_{ij})$. Then $t'_{m'}$ is evidently a derivation of $A'_{m'}$ which extends t. The isomorphism between A_m and $A'_{m'}$ transports $t'_{m'}$ into a derivation s of A_m which extends t. On the other hand, t can be extended to the derivation t_m of C_m (defined in the same way as $t'_{m'}$ was defined above). Let s_{C_m} be the restriction of s to $C_m \subset A_m$. Then $s_{C_m} - t_m$ is a derivation of C_m into A_m which annihilates C, and can therefore be extended to a derivation u of A_m. Now consider the derivation $s - u$ of A_m. Its restriction to C_m coincides with t_m, whence $s - u$ maps C_m into itself. Since A is the commutator algebra of C_m in $A_m = A \otimes_C C_m$, it follows that $s - u$ must also map A into itself, and therefore provides the desired extension of t to a derivation of A.

Hence we may now assume that A is a crossed product $Z(G, f)$, where Z is a normal extension field of C, G is the Galois group of Z/C, and f is a factor set, i.e., a map of $G \times G$ into the multiplicative group of the nonzero elements of Z such that, for all ρ, σ, τ in G, $\rho(f(\sigma, \tau))f(\rho\sigma, \tau)^{-1}f(\rho, \sigma\tau)f(\rho,\sigma)^{-1} = 1$. More explicitly, $Z(G, f)$, as a left vector space over Z, has a basis u_σ in one to one correspondence with the elements σ of G such that $u_\sigma u_\tau = f(\sigma, \tau)u_{\sigma\tau}$, and, for $z \in Z$, $u_\sigma z = \sigma(z)u_\sigma$. Since Z is separable over C, there is one and only one derivation of Z which coincides with the given derivation t of C. We shall denote this extended derivation of Z by the same letter t. Clearly, the map $\sigma t \sigma^{-1}$ is also a derivation of Z which extends our given derivation of C, whence $\sigma t \sigma^{-1} = t$. In other words, the extended derivation t to Z is also a G-endomorphism of Z. Now we define a map h of $G \times G$ into Z by setting $h(\sigma, \tau) = t(f(\sigma, \tau))f(\sigma, \tau)^{-1}$. Using that t is a derivation and a G-endomorphism, we

---

[3] In the case where C is finite over the subfield annihilated by the given derivation (and hence is of characteristic $\neq 0$ and purely inseparable of exponent 1 over that subfield), this theorem was already proved by Jacobson in [5]; one merely has to combine (in [5]) Theorem 7 with the part of §10 that precedes Theorem 13, using the argument of the first paragraph of our proof below. The rest of our proof is quite different from that of Jacobson.

derive from the above multiplicative identity for f the corresponding additive identity for its logarithmic derivative, h, i.e., $\rho(h(\sigma, \tau)) - h(\rho\sigma, \tau) + h(\rho, \sigma\tau) - h(\rho, \sigma) = 0$. It is a well-known result (due to Witt) that such an additive factor set must be a transformation set, i.e., that there is a map g of G into Z such that $\sigma(g(\tau)) - g(\sigma\tau) + g(\sigma) = h(\sigma, \tau)$. Indeed, there is an element $z_1 \in Z$ whose trace is 1, i.e., $\sum_{\sigma \in G} \sigma(z_1) = 1$. Define $g(\rho) = \sum_{\sigma \in G} \rho\sigma(z_1)h(\rho, \sigma)$. Then it is easily verified that g satisfies the above requirement. Now we define the additive endomorphism t^* of $Z(G, f)$ by the formula

$$t^*\Big(\sum_{\sigma \in G} z_\sigma u_\sigma\Big) = \sum_{\sigma \in G} (t(z_\sigma) + z_\sigma g(\sigma))u_\sigma,$$

where the z_σ are elements of Z. It is easy to check directly that t^* is a derivation of $Z(G, f)$ which coincides with t on C. This completes the proof of Theorem 6.

We shall now indicate briefly how Theorem 5 can be obtained from Theorem 6 and the theory of restricted Lie algebras. It is evidently sufficient to prove Theorem 5 in the case where $C^p \subset F$. In view of Theorem 3, it suffices then to show that there always exists a regular extension (S, ϕ) of A by the derivation algebra T of C/F, where C is the center of A. As in the proof of Theorem 3, we write $C = F[u_1, \cdots, u_k]$, and consider the derivations $t_1, \cdots, t_k$ of C/F such that $t_i(u_j) = \delta_{ij}u_j$. If T_0 is the subspace of T which is spanned, over F, by these elements t_i then T_0 is a restricted abelian Lie algebra over F, the p-map in T_0 is nondegenerate in the sense that the image of T_0 under the p-map spans T_0 over F, and we have $T = CT_0$. The key result for our proof is that the restricted cohomology groups of T_0 are trivial. This was shown in §1 of [4]. Before we can make use of this fact, we must modify the p-map in A. Let $a \to a'$ be any p-semilinear of A into F such that $c' = c^p$, for every $c \in C$. (The phrase p-semilinear means that, for a, b in F and u, v in A, we have $(au + bv)' = a^p u' + b^p v'$.) We define a new p-map by setting $a^{[p]} = a^p - a'$. With this p-map, and the usual commutation, A is a restricted Lie algebra, which we shall denote by A_0. Our new p-map annihilates the center C of A_0. By Theorem 6, every element of T_0 can be extended to a derivation of the associative algebra A, and such a derivation is then also a restricted derivation of the restricted Lie algebra A_0. Since the extension of a derivation of C to a derivation of A is unique up to an inner derivation of A, we thus have the structure of a restricted T_0-kernel on A_0, in the sense of [3]. Since the p-map in A_0 annihilates the center of A_0, and since the restricted 3-dimensional cohomology group for T_0 in C is (0), it follows from Theorem 3.1 of [3] that the kernel A_0 is extendable, i.e., that there exists a restricted Lie algebra extension (S_0, ϕ_0) of A_0 by T_0 which induces our kernel structure on A_0, and in particular satisfies the regularity condition (*). Now we extend the map $a \to a'$ to a p-semilinear map of S_0 into F and then redefine the p-map in S_0 by $s \to s^{[p]} + s' = s^p$, where $s \to s^{[p]}$ is the original p-map in S_0. There results a

restricted extension (S_1, ϕ_1) of A by T_0, where A is now again regarded as a restricted Lie algebra in the usual way, S_1 is the same as S_0 except for the changed p-map, and ϕ_1 is the same map as ϕ_0. The regularity condition (*) continues to hold in S_1, of course. The same argument which gave the proof of Theorem 2 (which uses the vanishing of the 2-dimensional cohomology groups of T_0; cf. [4]) shows that there is an ordinary Lie algebra isomorphism ψ of T_0 into S_1 which is inverse to ϕ_1. Now we enlarge S_1 to a Lie algebra S whose space is $A + C \otimes_F \psi(T_0)$, and where the commutation is that extension of the commutation in S_1 which results from enforcing the regularity condition (i), with the natural C-space structure of S. There remains to define a p-map in S. For $s_i = \psi(t_i)$ and $c \in C$, define $(c \otimes s_i)^p = c^p s_i^p + (ct_i)^{p-1}(c) \otimes s_i$. Then the inner derivation effected by $(c \otimes s_i)^p$ coincides with the pth power of the inner derivation effected by $c \otimes s_i$. Indeed, this holds on A, by Lemma 1 of [4], and since $C \otimes_F \psi(T_0)$ is isomorphic with T, this holds also on $C \otimes_F \psi(T_0)$. Now it follows from the elementary theory of restricted Lie algebras that there is one and only one p-map on S which coincides with the map $a \rightarrow a^p$ on A and which maps the elements $c \otimes s_i$ into $(c \otimes s_i)^p$. Clearly, this p-map is an extension of the given p-map on S_1. Furthermore, the analysis of the regularity condition (ii) which we made immediately before stating Theorem 4 shows that S satisfies the regularity condition (ii). Finally, ϕ_1 can be extended in one and only one way to a C-linear map ϕ of S onto T, and it is clear that (S, ϕ) is a regular extension of A by T. This completes our proof for the existence of regular extensions.

REFERENCES

1. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloquium Publications, vol. 24, 1952.

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

3. ———, *Lie algebra kernels and cohomology*, Amer. J. Math. vol. 76 (1954) pp. 698–716.

4. ———, *Simple algebras with purely inseparable splitting fields of exponent* 1, Trans. Amer. Math. Soc. vol. 79 (1955) pp. 477–489.

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

UNIVERSITY OF ILLINOIS
    URBANA, ILL.