TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 149, May 1970

INSEPARABLE GALOIS THEORY OF EXPONENT ONE

BY
SHUEN YUAN

Abstract. An exponent one inseparable Galois theory for commutative ring extensions of prime characteristic $p\neq 0$ is given in this paper.

Let C be a commutative ring of prime characteristic $p\neq 0$. Let $\mathfrak{g}$ be both a C-module and a restricted Lie ring of derivations on C and denote by A the kernel of $\mathfrak{g}$, i.e., the set of all x in C such that $\partial x=0$ for all ∂ in $\mathfrak{g}$. We say C over A is a purely inseparable Galois extension of exponent one if and only if C is finitely generated projective as A-module and $C[\mathfrak{g}]=\mathrm{Hom}_A(C, C)$. In this paper, we present a Galois correspondence between the restricted Lie subrings of $\mathfrak{g}$ which are also C-module direct summands of $\mathfrak{g}$ and the intermediate rings between C and A over which locally C admits p-basis. The Galois hypothesis $C[\mathfrak{g}]=\mathrm{Hom}_A(C, C)$ used here is an analog of the separable Galois hypothesis used in [7] and [8]. In case C is a field, our theory reduces to Jacobson's Galois theory for purely inseparable field extensions of exponent one.

In a subsequent paper [6], we shall present the attendant Galois cohomology results. Among other things, we shall show that there is an exact sequence $0\to L(C/A)\to P(A)\to P(C)\to \mathscr{E}(\mathfrak{g}, C)\to B(C/A)\to 0$, where $B(C/A)$ is the Brauer group for C over A, $\mathscr{E}(\mathfrak{g}, C)$ is Hochschild's group of regular restricted Lie algebra extensions of C by $\mathfrak{g}$, P is the functor of taking rank one projective class group and $L(C/A)$ is the logarithmic derivative group. We also show that the Amitsur cohomology groups $H^{n+2}(C/A, G_m)$, $n\geqq 0$, are isomorphic to Hochschild's groups $\mathscr{E}(C^n\otimes_A \mathfrak{g}, C^{n+1})$ of regular restricted Lie algebra extensions of C^{n+1}, the $n+1$-fold tensor product $C\otimes_A\cdots\otimes_A C$, by $C^n\otimes_A\mathfrak{g}$.

All rings in the following are assumed to be commutative with 1. If A is a subring of a ring C we understand that both A and C have the same identity. By an A-algebra C we mean that A is a subring of C. Finally all ring-homomorphisms and modules are unitary.

1. Lemma. *Let C be a ring of prime characteristic $p\neq 0$, and let A be a subring of C such that $t^p\in A$ for all t in C. Then* Spec C *is canonically homeomorphic to* Spec A.

Received by the editors July 8, 1968 and, in revised form, October 2, 1969.

AMS Subject Classifications. Primary 1370.

Key Words and Phrases. Restricted Lie ring, derivation, p-basis.

Proof. We have two ring homomorphisms between A and C.

$$A \to C; \qquad C \to A,$$
$$x \to x; \qquad x \to x^p$$

which produce continuous mappings inverses to each other between Spec A and Spec C.

2. Remark. In view of the above lemma, we may regard the structural sheaf $\tilde{A}$ associated to Spec A as a subsheaf of the structural sheaf $\tilde{C}$ associated to Spec C. Moreover given any $\mathfrak{q}$ in Spec A, we shall always denote by $\mathfrak{Q}$ the corresponding element in Spec C and vice versa.

Another simple fact which we repeatedly use is the following

3. Lemma. *Let C be a ring of prime characteristic $p \neq 0$ and let A be a subring of C such that $t^p \in A$ for all $t \in C$. If $\mathfrak{Q}$ is any prime ideal in C then*

$$M_{\mathfrak{Q}} = M \otimes_A A_{\mathfrak{q}}$$

for all C-modules M.

Proof. We have a map

$$C \otimes_A A_{\mathfrak{q}} \to C_{\mathfrak{Q}},$$
$$x \otimes (a/s) \to (ax)/s \qquad (s \in A - \mathfrak{q}).$$

Given any x/t in $C_{\mathfrak{Q}}$ with $t \in C - \mathfrak{Q}$, then x/t is the image of $(xt^{p-1}) \otimes (1/t^p)$. So the map is onto. Now every element $\sum x_i \otimes (a_i/s_i)$ in $C \otimes_A A_{\mathfrak{q}}$ can be written in the form $x \otimes (1/s)$ with $x = \sum_i a_i x_i (\prod_{j \neq i} s_j)$ and $s = \prod_i s_i$. If $x \otimes (1/s)$ goes to zero in $C_{\mathfrak{Q}}$ then for some $t \in C - \mathfrak{Q}$, tx is zero in C. So $x \otimes (1/s) = (t^p x) \otimes (1/t^p s)$ is already zero in $C \otimes_A A_{\mathfrak{q}}$. This shows $C \otimes_A A_{\mathfrak{q}}$ may be identified with $C_{\mathfrak{Q}}$. If M is any C-module, we have

$$M_{\mathfrak{Q}} = M \otimes_C C_{\mathfrak{Q}} = M \otimes_C C \otimes_A A_{\mathfrak{q}} = M \otimes_A A_{\mathfrak{q}}.$$

This completes the proof of the lemma.

Let S be a sheaf of rings over a topological space X. By a derivation d on S we mean a sheaf map $d: S^+ \to S^+$ such that for any open set U in X, $d(U)$: $S(U) \to S(U)$ is a derivation where S^+ is the underlining sheaf of abelian groups of S. If R is a subsheaf of S, then the set $\mathscr{L}(U, S/R)$ of all R_U-derivations on the sheaf S_U has an obvious $S(U)$-module structure. We shall call the sheaf $\mathscr{L}_{S/R} = \mathscr{L}(\ \ , S/R)$ the S-module of all R-derivations on S.

Given a derivation ∂ on a ring C, then for any multiplicatively closed subset Σ of C there is a unique derivation, which we again denote by ∂, on C_Σ making the diagram

$$\begin{array}{ccc} C & \longrightarrow & C_\Sigma \\ \partial \downarrow & & \downarrow \partial \\ C & \longrightarrow & C_\Sigma \end{array}$$

commutative. Thus a derivation d on $\tilde{C}$ is completely determined by $d(\text{Spec } C)$: $C \to C$. So we have the following

4. LEMMA. *Let C be a ring of prime characteristic $p \neq 0$. Let A be a subring of C such that $t^p \in A$ for all $t \in C$. Then the correspondence $d \to d(\text{Spec } C)$ is an isomorphism between the C-module $\mathscr{L}(\text{Spec } C, \tilde{C}/\tilde{A})$ and the C-module $\mathfrak{g}(C/A)$ of all A-derivations on C.*

5. LEMMA. *Let C be a ring of prime characteristic $p \neq 0$. Let A be a subring of C such that C admits a p-basis over A(1). Denote by $\mathfrak{g}(C/A)$ the C-module of all A-derivations on C. Then the sheaf $\mathscr{L}_{\tilde{C}/\tilde{A}}$ is isomorphic to $(\tilde{\mathfrak{g}}(C/A))$.*

Proof. Given any distinguished open set $D(f)$ in Spec $C(f \in A)$, we have

$$\begin{aligned} \mathscr{L}(D(f), \tilde{C}/\tilde{A}) &\cong \mathscr{L}(\text{Spec } C_f, \tilde{C}_f/\tilde{A}_f) \\ &\cong \mathfrak{g}(C_f/A_f) \\ &\cong \mathfrak{g}(C/A)_f. \end{aligned}$$

The last isomorphism follows from the fact that C has a p-basis over A. This completes the proof of the lemma.

6. DEFINITION. Let A be a ring of prime characteristic $p \neq 0$. An A-algebra C is called a Galois extension of A provided

(i) C is finitely generated projective as A-module,

(ii) $t^p \in A$ for all $t \in C$,

(iii) Given any prime ideal $\mathfrak{Q}$ in C, then $C_{\mathfrak{Q}}$ admits a p-basis over $A_{\mathfrak{q}}$.

The equivalence of this definition with the one given in the introduction is a consequence of Theorems 9 and 10 below.

7. LEMMA. *Given a Galois extension C over A, then for any prime ideal $\mathfrak{q}$ in A, there is some $f \in A - \mathfrak{q}$ such that C_f admits a p-basis over A_f.*

Proof. Since C is a finitely generated projective A-module, there is an $\alpha \in A - \mathfrak{q}$ such that C_α is a free A_α-module of finite dimension. Let $t_1, \ldots, t_m$ be elements in C_α such that their images in $C_{\mathfrak{Q}} = C \otimes_A A_{\mathfrak{q}}$ form a p-basis over $A_{\mathfrak{q}}$. If $\{\gamma_i\}$ is an A_α-module basis for C_α, then there is an m^p by m^p matrix μ with entries from A_α which takes $\{\gamma_i\}$ to $\{t_1^{e_1} \cdots t_m^{e_m} \mid 0 \leqq e_i < p\}$ because $t_1^{e_1} \cdots t_m^{e_m}$ can be expressed as a linear combination in the γ_i's with coefficients from A_α. Write (determinant μ) $= \beta/\alpha^e$ where e is a nonnegative integer and β is from A. Put $f = \alpha\beta$. It is clear that $f \in A - \mathfrak{q}$ and the images of $t_1, \ldots, t_m$ in C_f form a p-basis over A_f.

As an immediate consequence of Lemma 7 and [2, p. 90, Theorem 1.4.1] we get

8. LEMMA. *Let C be a Galois extension over A. Then the $\tilde{C}$-module $\mathscr{L}_{\tilde{C}/\tilde{A}}$ of all $\tilde{A}$-derivations on $\tilde{C}$ is isomorphic to $(\tilde{\mathfrak{g}}(C/A))$.*

(1) By a p-basis of C over A we mean a subset $\{t_1, \ldots, t_r\}$ in C such that $\{t_1^{e_1} \cdots t_r^{e_r} \mid 0 \leqq e_i < p\}$ form an A-module basis for C.

9. THEOREM. *Let C be a Galois extension over A, and denote by $\mathfrak{g}=\mathfrak{g}(C/A)$ the C-module of all A-derivations on C. Then*

(1) *the C-module $\mathfrak{g}$ is finitely generated and projective;*

(2) $A=\{t\in C \mid \partial t=0$ *for all* $\partial\in\mathfrak{g}(C/A)\}\equiv\text{kernel }\mathfrak{g}$;

(3) $\operatorname{Hom}_A(C,C)=C[\mathfrak{g}]$.

Proof. Only the last two statements are not already proven. That the inclusion map $A\hookrightarrow\text{kernel }\mathfrak{g}$ must be onto follows from the fact that at each prime $\mathfrak{q}$, the map $A_{\mathfrak{q}}\hookrightarrow\text{kernel }\mathfrak{g}_{\mathfrak{Q}}=(\text{kernel }\mathfrak{g})_{\mathfrak{q}}$ is onto [1, p. 111, Theorem 1]. By the same token the inclusion map $C[\mathfrak{g}]\hookrightarrow\operatorname{Hom}_A(C,C)$ is onto because the corresponding map at each $\mathfrak{q}\in\operatorname{Spec}A$ is onto.

10. THEOREM. *Let C be a ring of prime characteristic $p\neq 0$. Let $\mathfrak{g}$ be a C-module of derivations on C. Put $A=\text{kernel }\mathfrak{g}$ and assume that C is finitely generated projective as A-module. If $\operatorname{Hom}_A(C,C)=C[\mathfrak{g}]$ then C is a Galois extension over A. If in addition $\mathfrak{g}$ is a restricted Lie ring, then $\mathfrak{g}=\mathfrak{g}(C/A)$.*

Proof. Let $\mathfrak{q}$ be any prime ideal in A. We have, by [1, p. 98, Proposition 19], $\operatorname{Hom}_{A_{\mathfrak{q}}}(C_{\mathfrak{Q}},C_{\mathfrak{Q}})=C_{\mathfrak{Q}}[\mathfrak{g}_{\mathfrak{Q}}]$. For simplicity of notations write $\bar{A}=A_{\mathfrak{q}}/\mathfrak{q}A_{\mathfrak{q}}$, $\bar{C}=C_{\mathfrak{Q}}/\mathfrak{q}C_{\mathfrak{Q}}$, and denote by $\bar{\mathfrak{g}}=$ the image of $\mathfrak{g}_{\mathfrak{Q}}\otimes_{A_{\mathfrak{q}}}\bar{A}$ in

$$\operatorname{Hom}_{A_{\mathfrak{q}}}(C_{\mathfrak{Q}},C_{\mathfrak{Q}})\otimes_{A_{\mathfrak{q}}}\bar{A}=\operatorname{Hom}_{\bar{A}}(\bar{C},\bar{C}).$$

So $\operatorname{Hom}_{\bar{A}}(\bar{C},\bar{C})=\bar{C}[\bar{\mathfrak{g}}]$. This means no nontrivial ideal in $\bar{C}$ is stable under $\bar{\mathfrak{g}}$. Since $\bar{C}$ is finite dimensional over $\bar{A}$, it follows from [5, Corollary 2.8] that $\bar{C}$ admits a p-basis over $\bar{A}$. Hence $C_{\mathfrak{Q}}$ admits a p-basis over $A_{\mathfrak{q}}$ [1, p. 107, Corollaire 1] and C is a Galois extension over A.

It remains to show the inclusion map $\mathfrak{g}\to\mathfrak{g}(C/A)$ is onto. In view of [1, p. 111, Theorem 1], it suffices to show that at each prime $\mathfrak{Q}\in\operatorname{Spec}C$, the corresponding map $\mathfrak{g}_{\mathfrak{Q}}\to\mathfrak{g}(C/A)_{\mathfrak{Q}}$ is onto. Now $\bar{\mathfrak{g}}$ is a free $\bar{C}$-module [5, Lemma 3.2]. Let $\bar{\partial}_1,\dots,\bar{\partial}_r$ be a $\bar{C}$-module basis for $\bar{\mathfrak{g}}$. The fact that $\bar{\mathfrak{g}}$ is a restricted Lie ring implies that the set $\{\bar{\partial}_1^{e_1}\cdots\bar{\partial}_r^{e_r}\mid 0\leqq e_i<p\}$ form a set of generators for the $\bar{C}$-module $\operatorname{Hom}_{\bar{A}}(\bar{C},\bar{C})=\bar{C}[\bar{\mathfrak{g}}]$. But $\mathfrak{g}(\bar{C}/\bar{A})$ is also a free $\bar{C}$-module because $\bar{C}$ admits a p-basis over $\bar{A}$. Let r' be the dimension of $\mathfrak{g}(\bar{C}/\bar{A})$ over $\bar{C}$. Then $[\bar{C}:\bar{A}]=p^{r'}$. Now as vector spaces over $\bar{A}$, $\bar{\mathfrak{g}}$ is a subspace of $\mathfrak{g}(\bar{C}/\bar{A})$, so $rp^{r'}=[\bar{\mathfrak{g}}:\bar{A}]\leqq[\mathfrak{g}(\bar{C}/\bar{A}):\bar{A}]=r'p^{r'}$. Hence $r\leqq r'$. On the other hand the $\bar{A}$-module $\operatorname{Hom}_{\bar{A}}(\bar{C}:\bar{C})$ is of dimension $p^{2r'}$ but has a set of generators of cardinality $p^{r+r'}\leqq p^{2r'}$. This shows $r=r'$ and therefore $\bar{\mathfrak{g}}=\mathfrak{g}(\bar{C}/\bar{A})$. So $\bar{\partial}_1,\dots,\bar{\partial}_r$ form a $\bar{C}$-module basis for $\mathfrak{g}(\bar{C}/\bar{A})$. Let ∂_i be a preimage of $\bar{\partial}_i$ in $\mathfrak{g}_{\mathfrak{Q}}$. Then $\partial_1,\dots,\partial_r$ form a $C_{\mathfrak{Q}}$-module basis for $\mathfrak{g}(C_{\mathfrak{Q}}/A_{\mathfrak{q}})$. This proves that $\mathfrak{g}_{\mathfrak{Q}}=\mathfrak{g}(C_{\mathfrak{Q}}/A_{\mathfrak{q}})$ because $\mathfrak{g}_{\mathfrak{Q}}\subset\mathfrak{g}(C_{\mathfrak{Q}}/A_{\mathfrak{q}})=\sum C_{\mathfrak{Q}}\partial_i\subset\mathfrak{g}_{\mathfrak{Q}}$. Consequently $\mathfrak{g}_{\mathfrak{Q}}=\mathfrak{g}(C_{\mathfrak{Q}}/A_{\mathfrak{q}})=\mathfrak{g}(C/A)_{\mathfrak{Q}}$ because C is a Galois extension over A.

11. THEOREM. *Let $A\subset B\subset C$ be a tower of rings such that C is a Galois extension both over A and over B. Then*

(1) *B is a Galois extension over A.*

(2) *Let* $\mathfrak{h}=\{d\in\mathfrak{g}(C/A)\mid dB\subset B\}$. *Then there is a* B*-module homomorphism* $\mathfrak{g}(B/A)\to\mathfrak{h}$ *which followed by the restriction map* $\mathfrak{h}\to\mathfrak{g}(B/A)$ *given by* $d\to d|_B$ *is the identity map on* $\mathfrak{g}(B/A)$.

(3) *Let* $G(B/A)$ *be the image of* $\mathfrak{g}(B/A)$ *in* $\mathfrak{h}$. *Then*

$$C\cdot G(B/A)\oplus\mathfrak{g}(C/B)=\mathfrak{g}(C/A).$$

Proof. Let $\mathfrak{Q}$ be a prime ideal in C and denote by $\mathfrak{q}$ and q the corresponding prime ideals in A and B respectively. Since C is finitely generated projective both as A-module and as B-module, there is $\alpha\in A-\mathfrak{q}$ such that C_α is a free module of finite dimension both over A_α and over B_α. The A_α-module B_α as a direct summand of C_α is therefore finitely generated projective. So B is finitely generated projective as A-module. We would like to show that B_q admits a p-basis over $A_\mathfrak{q}$. For simplicity of notations, write $\bar{A}=A_\mathfrak{q}/\mathfrak{q}A_\mathfrak{q}$, $\bar{B}=B_q/\mathfrak{q}B_q$ and $\bar{C}=C_\mathfrak{Q}/\mathfrak{q}C_\mathfrak{Q}$. Let $b_1,\dots,b_r$ be a basis for the free $\bar{B}$-module $\bar{C}$. Let ∂ be an $\bar{A}$-derivation on $\bar{C}$. For any $x\in\bar{B}$, ∂x may be expressed in the form $(\partial_1 x)b_1+\cdots+(\partial_r x)b_r$ with $\partial_i x\in\bar{B}$. It is easily seen that the map $x\to\partial_i x$ is an $\bar{A}$-derivation on $\bar{B}$. By Theorem 9 we have $C[\mathfrak{g}(C/A)]=\operatorname{Hom}_A(C,C)$ and hence

$$\bar{C}[\bar{\mathfrak{g}}]=\operatorname{Hom}_{\bar{A}}(\bar{C},\bar{C})$$

where $\bar{\mathfrak{g}}=\mathfrak{g}(C/A)_\mathfrak{Q}/\mathfrak{q}\mathfrak{g}(C/A)_\mathfrak{Q}$. So no nontrivial ideal in $\bar{C}$ is stable under $\bar{\mathfrak{g}}$. Let I be a nonzero proper ideal in $\bar{B}$. Then there is an $\bar{A}$-derivation ∂ on $\bar{C}$ such that $\partial(I\bar{C})$ is not contained in $I\bar{C}$. This means $\partial_i I$ cannot be contained in I for some i. But $\bar{B}$ is a finite dimensional vector space over $\bar{A}$ so by [5, Corollary 2.8], $\bar{B}$ admits a p-basis over $\bar{A}$. Hence B_q admits a p-basis over $A_\mathfrak{q}$ [1, p. 107, Corollaire].

To show the identity map $\mathfrak{g}(B/A)\to\mathfrak{g}(B/A)$ factors through the restriction map $\mathfrak{h}\to\mathfrak{g}(B/A)$, it suffices to show at each prime ideal q in B the identity map $\mathfrak{g}(B/A)_q\to\mathfrak{g}(B/A)_q$ factors through $\mathfrak{h}_q\to\mathfrak{g}(B/A)_q$. Let $t_1,\dots,t_l$ be a p-basis for $C_\mathfrak{Q}$ over B_q and let $t_{l+1},\dots,t_{l+\lambda}$ be a p-basis for B_q over $A_\mathfrak{q}$. If we denote by d_i the $A_\mathfrak{q}$-derivation on $C_\mathfrak{Q}$ given by $d_i t_j=\delta_{ij}$, then the B_q-module H^q of all $A_\mathfrak{q}$-derivations on $C_\mathfrak{Q}$ leaving B_q invariant is just

$$\sum_{i=1}^{l}C_\mathfrak{Q}d_i+\sum_{i=1}^{\lambda}B_q d_{l+i}.$$

It is obvious that the identity map on $\mathfrak{g}(B/A)_q=\mathfrak{g}(B_q/A_\mathfrak{q})$ factors through the restriction map $H^q\to\mathfrak{g}(B/A)_q$. So it suffices to show $\mathfrak{h}_q=H^q$.

Given any open set U in Spec A, let $H(U)$ be the set of all $\tilde{A}_U$-derivations on $\tilde{C}_U$ leaving $\tilde{B}_U$ invariant. The set $H(U)$ has an obvious $\tilde{B}(U)$-module structure. So the sheaf $U\to H(U)$ is a $\tilde{B}$-module and its fibre at a point q in Spec B is just H^q. It is easily seen that if C admits a p-basis over B and B admits a p-basis over A, then the sheaf H is just the sheaf $\tilde{\mathfrak{h}}$ associated to $\mathfrak{h}$. Hence by [2, p. 90, Theorem 1.4.1] H is always the sheaf $\tilde{\mathfrak{h}}$ associated to $\mathfrak{h}$ whenever C is a Galois extension both over A and over B because locally C admits a p-basis over B as does B over A.

This shows the identity map on $\mathfrak{g}(B/A)$ factors through the restriction map $\mathfrak{h} \to \mathfrak{g}(B/A)$. In particular $\mathfrak{h} = G(B/A) \oplus \mathfrak{g}(C/B)$. Hence $\mathfrak{g}(C/A) = C \cdot G(B/A) + \mathfrak{g}(C/B)$ because $C \cdot \mathfrak{h} = \mathfrak{g}(C/A)$. Assume $\partial \in [C \cdot G(B/A)] \cap \mathfrak{g}(C/B)$. We claim that $\partial = 0$. It suffices to show the corresponding derivation $\partial_{\mathfrak{q}}$ at $\mathfrak{q} \in \operatorname{Spec} A$ is zero. Now $\partial_{\mathfrak{q}}$ as an element in $[C \cdot G(B/A)]_{\mathfrak{q}}$ can be written in the form $\sum_{i=1}^{\lambda} u_i \partial_{l+i}$ with $u_i \in C_{\mathfrak{Q}}$ where ∂_{l+i} is the image of d_{l+i} in $\mathfrak{h}_q$. So $u_j = (\sum_{i=1}^{\lambda} u_i \partial_{l+i}) t_{l+j} = \partial_{\mathfrak{q}} t_{l+j} = 0$ because $\partial_{\mathfrak{q}} \in \mathfrak{g}(C_{\mathfrak{Q}}/B_q)$ and $t_{l+j} \in B_q$. This shows $\partial_{\mathfrak{q}} = 0$ as desired.

12. Remark. Given a tower of rings $A \subset B \subset C$ such that both B and C are Galois extensions over A, in general C need not be a Galois extension over B and not every A-derivation on B can be extended to a derivation on C. As an example, let $C = K[[x, y]]$ be the formal power series ring over a coefficient field K of characteristic $p \neq 0$. Put $A = K[[x^p, y^p]]$ and $B = K[[x^p, y^p, xy]]$. The A-derivation ∂ on B given by $\partial(xy) = 1$ cannot be extended to C. So in view of the above theorem, C cannot be a Galois extension over B. If d is the K-derivation on C given by $dx = x$ and $dy = y$, then $B = \text{kernel } d$ and $\operatorname{Hom}_B(C, C) = C[d]$. This means that C is not a projective B-module.

12. Theorem. *Let C be a Galois extension over A. Let $\mathfrak{h}$ be a restricted Lie subring of $\mathfrak{g}(C/A)$ such that $\mathfrak{h}$ is also a C-module direct summand of $\mathfrak{g}(C/A)$. Put $B = \text{kernel } \mathfrak{h}$. Then C is a Galois extension over B and $\mathfrak{g}(C/B) = \mathfrak{h}$.*

Proof. We shall first prove the theorem under the additional assumption that C is a local ring(2). So C admits a p-basis $t_1, \ldots, t_r$ over A. Let d_i be the A-derivation on C given by $d_i t_j = \delta_{ij}$. Then $d_1, \ldots, d_r$ form a C-module basis for $\mathfrak{g}(C/A)$. Now the C-module $\mathfrak{h}$ as a direct summand of $\mathfrak{g}(C/A)$ is also free. Let $\partial_{1,0}, \ldots, \partial_{l,0}$ be a basis for $\mathfrak{h}$. We have $\partial_{i,0} = \sum_{j=1}^{r} (\partial_{i,0} t_j) d_j$. Clearly given any i, $\partial_{i,0} t_j$ must be an invertible element in C for at least one j $(1 \leqq j \leqq r)$. We claim that there exist $\partial_1, \ldots, \partial_l$ a basis for $\mathfrak{h}$ and elements $y_1, \ldots, y_l$ in C such that $\partial_i y_j = \delta_{ij}$. Suppose we have already proven $y_1, \ldots, y_s$ in C and a C-module basis $\partial_{1,s}, \ldots, \partial_{l,s}$ for $\mathfrak{h}$ such that $\partial_{i,s} y_j = \delta_{ij}$ for $1 \leqq i \leqq l$ and $1 \leqq j \leqq s$. If $s < l$, then there is an element y_{s+1} in C such that $\partial_{s+1,s} y_{s+1}$ is invertible in C. We set

$$\partial_{s+1,s+1} = (\partial_{s+1,s} y_{s+1})^{-1} \partial_{s+1,s}$$

so that $\partial_{s+1,s+1} y_{s+1} = 1$. For every $j \neq s+1$, we set

$$\partial_{j,s+1} = \partial_{j,s} - (\partial_{j,s} y_{s+1}) \partial_{s+1,s+1}.$$

Then we have $\partial_{i,s+1} y_j = \delta_{ij}$ for $1 \leqq i \leqq l$ and $1 \leqq j \leqq s+1$, and that $\partial_{i,s+1}$ are still a basis for $\mathfrak{h}$. Proceeding in this fashion, starting from the case $s = 0$, we finally obtain $y_1, \ldots, y_l$ in C and $\partial_i = \partial_{i,l}$ which satisfy the requirements of our assertion.

(2) Hochschild's proof of the main theorem of Jacobson's Galois theory for purely inseparable field extensions of exponent one is used here practically without change; (c.f. [4, Lemma 2.1] and [5, Theorem 1]).

Writing $[\partial_i, \partial_j]=\sum_{s=1}^{l} v_s\partial_s$ with $v_s \in C$, we get $v_s=[\partial_i, \partial_j]y_s=0$ whence $[\partial_i, \partial_j]=0$. In the same way we find that $\partial_i^p=0$. It is clear that $y_1, \ldots, y_l$ form a p-basis for $B[y_1, \ldots, y_l]$. It remains to prove that $C=B[y_1, \ldots, y_l]$. Suppose that this is false, i.e., that there is an element u_1 in C which does not belong to $B[y_1, \ldots, y_l]$. Assume inductively that we have already found an element u_s of C which is not in $B[y_1, \ldots, y_l]$ and which is annihilated by every ∂_i with $i<s$. Since $\partial_s^p=0$ there is an exponent e $(0\leqq e<p)$ such that ∂_s^{e+1} but not ∂_s^e maps u_s into $B[y_1, \ldots, y_l]$. We have $\partial_i\partial_s^e(u_s)=\partial_s^e\partial_i(u_s)$ which is zero for $i<s$. Hence replacing u_s by $\partial_s^e(u_s)$, we may suppose that $\partial_s(u_s) \in B[y_1, \ldots, y_l]$. Since $\partial_s(u_s)$ is annihilated by each ∂_i with $i<s$ it follows then that $\partial_s(u_s) \in B[y_s, \ldots, y_l]$. Write $\partial_s u_s$ as a polynomial of degree $p-1$ in y_s with coefficients in $B[y_{s+1}, \ldots, y_l]$. Since this polynomial is annihilated by ∂_s^{p-1} (for $\partial_s^p=0$) the coefficient of y_s^{p-1} must be 0. Hence we can integrate this polynomial with respect to y_s, i.e., there is an element $u \in B[y_s, \ldots, y_l]$ such that $\partial_s(u_s)=\partial_s u$. Now put $u_{s+1}=u_s-u$. Then $u_{s+1} \notin B[y_1, \ldots, y_l]$ and $\partial_i(u_{s+1})=0$ for all $i<s+1$. We can repeat this construction until we obtain $u_{l+1} \notin B[y_1, \ldots, y_l]$ such that $\partial_i u_{l+1}=0$ for all $i=1, \ldots, l$. But then $u_{l+1} \in B$, and we have a contradiction. Hence $C=B[y_1, \ldots, y_l]$. Moreover, if ∂ is any B-derivation on C we have $\partial=\sum (\partial y_i)\partial_i \in \mathfrak{h}$. This proves the theorem when C is local.

To complete the proof of the theorem, it remains to show that C is finitely generated projective as B-module and that $\mathfrak{g}(C/B)=\mathfrak{h}$. Since C is finitely generated as A-module so surely finitely generated over B also. At each prime $\mathfrak{Q}$ in C, $C_{\mathfrak{Q}}$ admits a p-basis over B_q with $q=\mathfrak{Q} \cap B$. Moreover, the dimension $[C_{\mathfrak{Q}}:B_q]$ is equal to the $[\mathfrak{h}_{\mathfrak{Q}}:C_{\mathfrak{Q}}]$th power of p. So $[C_{\mathfrak{Q}}:B_q]$ is locally constant in Spec C because $[\mathfrak{h}_{\mathfrak{Q}}:C_{\mathfrak{Q}}]$ is. Hence C over B is finitely generated projective and therefore must be a Galois extension. Finally $\mathfrak{h}_{\mathfrak{Q}}$ is equal to $\mathfrak{g}(C/B)_{\mathfrak{Q}}$ at every $\mathfrak{Q} \in \operatorname{Spec} C$. So the inclusion map $\mathfrak{h} \to \mathfrak{g}(C/B)$ must be onto.

Summarizing the above results, we get

13. Theorem. *Let C be a Galois extension over A and denote by $\mathfrak{g}_{C/A}$ the C-module of all A-derivations on C. Put*

$$\Theta = \{B|B \text{ is an } A\text{-subalgebra of } C \text{ and } C/B \text{ is a Galois extension}\},$$

$$\Xi = \{\mathfrak{g}|\mathfrak{g} \text{ is a restricted Lie subring and a } C\text{-module direct summand of } \mathfrak{g}_{C/A}\}.$$

Then the mappings $\Xi \xrightarrow[\theta]{} \Theta$, $\Theta \xrightarrow[\xi]{} \Xi$ *given respectively by* $\mathfrak{g} \to \operatorname{kernel} \mathfrak{g}$; $B \to \mathfrak{g}_{C/B}$ *are inverses to each other.*

References

1. N. Bourbaki, *Algèbre commutative*, Chapitres 1, 2, Actualités Sci. Indust., no. 1290, Hermann, Paris, 1961. MR **36** #146.

2. A. Grothendieck and J. Dieudonné, *Éléments de géométrie algébrique*. I: *Le langage des schemas*, Inst. Hautes Etudes Sci. Publ. Math. No. 4 (1960). MR **36** #177a.

3. G. Hochschild, *Double vector spaces over division rings*, Amer. J. Math. **71** (1949), 443–460. MR **10**, 676.

4. G. Hochschild, *Simple algebras with purely inseparable splitting fields of exponent* 1, Trans. Amer. Math. Soc. **79** (1955), 477–489. MR **17**, 61.

5. S. Yuan, *Differentiably simple rings of prime characteristic*, Duke Math. J. **31** (1964), 623–630. MR **29** #4772.

6. ———, *Inseparable exponent one Galois cohomolgy* (to appear).

7. S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965), 15–33. MR **33** #4118.

8. O. E. Villamayor and D. Zelinsky, *Galois theory with infinitely many idempotents*, Nagoya Math. J. **35** (1969), 83–98.

State University of New York at Buffalo,
Amherst, New York 14226