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 \( \partial \) 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 \( C[\mathfrak{g}] = \text{Hom}_A(C, C) \). 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 \( C[\mathfrak{g}] = \text{Hom}_A(C, C) \) 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 \( 0 \to L(C/A) \to P(A) \to P(C) \to \mathfrak{e}(\mathfrak{g}, C) \to B(C/A) \to 0 \), where \( B(C/A) \) is the Brauer group for \( C \) over \( A \), \( \mathfrak{e}(\mathfrak{g}, C) \) 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 \( H^{n+2}(C/A, G_m) \), \( n \geq 0 \), are isomorphic to Hochschild's groups \( \mathfrak{e}(C^n \otimes_A \mathfrak{g}, C^{n+1}) \) 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 \( t^n \in A \) for all \( t \) in \( C \). Then \( \text{Spec} \, C \) is canonically homeomorphic to \( \text{Spec} \, A \).

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.

Copyright © 1970, American Mathematical Society

163
Proof. We have two ring homomorphisms between $A$ and $C$.

$$A \rightarrow C; \quad C \rightarrow A,$$

$$x \rightarrow x; \quad x \rightarrow x^p$$

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 $\mathcal{A}$ associated to Spec $A$ as a subsheaf of the structural sheaf $\mathcal{C}$ associated to Spec $C$. Moreover given any $q$ in Spec $A$, we shall always denote by $\mathcal{O}$ 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 $\mathcal{O}$ is any prime ideal in $C$ then

$$M_{\mathcal{O}} = M \otimes_A A_q$$

for all $C$-modules $M$.

Proof. We have a map

$$C \otimes_A A_q \rightarrow C_{\mathcal{O}},$$

$$x \otimes (a/s) \rightarrow (ax)/s \quad (s \in A - q).$$

Given any $x/t$ in $C_{\mathcal{O}}$ with $t \in C - \mathcal{O}$, 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 $C \otimes_A A_q$ can be written in the form $x \otimes (1/s)$ with $x = \sum_i a_i x_i (\prod_j s_j)$ and $s = \prod_i s_i$. If $x \otimes (1/s)$ goes to zero in $C_{\mathcal{O}}$ then for some $t \in C - \mathcal{O}$, $tx$ is zero in $C$. So $x \otimes (1/s) = (t^p x) \otimes (1/t^p s)$ is already zero in $C \otimes_A A_q$. This shows $C \otimes_A A_q$ may be identified with $C_{\mathcal{O}}$. If $M$ is any $C$-module, we have

$$M_{\mathcal{O}} = M \otimes_C C_{\mathcal{O}} = M \otimes_C C \otimes_A A_q = M \otimes_A A_q.$$

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 $d: S^+ \rightarrow S^+$ such that for any open set $U$ in $X$, $d(U): S(U) \rightarrow S(U)$ is a derivation where $S^+$ is the underlining sheaf of abelian groups of $S$. If $R$ is a subsheaf of $S$, then the set $\mathcal{L}(U, S/R)$ of all $R$-derivations on the sheaf $S_U$ has an obvious $S(U)$-module structure. We shall call the sheaf $\mathcal{L}_{S/R} = \mathcal{L}(\ , S/R)$ the $S$-module of all $R$-derivations on $S$.

Given a derivation $\partial$ on a ring $C$, then for any multiplicatively closed subset $\Sigma$ of $C$ there is a unique derivation, which we again denote by $\partial$, on $C_{\Sigma}$ making the diagram

$$\begin{array}{ccc}
C & \longrightarrow & C_{\Sigma} \\
\partial \downarrow & & \partial \downarrow \\
C & \longrightarrow & C_{\Sigma}
\end{array}$$
commutative. Thus a derivation $d$ on $C$ 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 $d \mapsto d(\text{Spec } C)$ is an isomorphism between the $C$-module $\mathcal{L}(\text{Spec } C, \mathcal{O}/\mathcal{A})$ 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 $A$. Denote by $\mathfrak{g}(C/A)$ the $C$-module of all $A$-derivations on $C$. Then the sheaf $\mathcal{L}_{\mathcal{O}/\mathcal{A}}$ is isomorphic to $(\mathfrak{g}(C/A))$.

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

$$\mathcal{L}(D(f), \mathcal{O}/\mathcal{A}) \cong \mathcal{L}(\text{Spec } C_f, \mathcal{O}/\mathcal{A}_f) \cong \mathfrak{g}(C_f/A_f) \cong \mathfrak{g}(C/A).$$

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 $\mathfrak{p}$ in $C$, then $C_{\mathfrak{p}}$ admits a $p$-basis over $A_{\mathfrak{p}}$.

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 $C_\alpha$ is a free $A_\alpha$-module of finite dimension. Let $t_1, \ldots, t_m$ be elements in $C_\alpha$ such that their images in $C_{\alpha} = C \otimes A_\alpha$ form a $p$-basis over $A_\alpha$. If $\{\gamma_1\}$ is an $A_\alpha$-module basis for $C_\alpha$, then there is an $m^p$ by $m^p$ matrix $\mu$ with entries from $A_\alpha$ which takes $\{\gamma_1\}$ to $\{t_1^{e_1} \cdots t_m^{e_m} | 0 \leq e_i < p\}$ because $t_1^{e_1} \cdots t_m^{e_m}$ can be expressed as a linear combination in the $\gamma_i$'s with coefficients from $A_\alpha$. Write (determinant $\mu$) $= \beta/\alpha^e$ where $e$ is a nonnegative integer and $\beta$ 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 $\mathcal{O}/\mathcal{A}$-module $\mathcal{L}_{\mathcal{O}/\mathcal{A}}$ of all $\mathcal{A}$-derivations on $C$ is isomorphic to $(\mathfrak{g}(C/A))$.\(^{(1)}\)

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

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
9. **Theorem.** Let $C$ be a Galois extension over $A$, and denote by $g = g(C/A)$ the $C$-module of all $A$-derivations on $C$. Then

1. the $C$-module $g$ is finitely generated and projective;
2. $A = \{ t \in C \mid \partial t = 0 \text{ for all } \partial \in g(C/A) \} = \text{kernel } g$;
3. $\text{Hom}_A (C, C) = C[g]$.

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

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

**Proof.** Let $q$ be any prime ideal in $A$. We have, by [1, p. 98, Proposition 19], $\text{Hom}_A (C_C, C_C) = C_C[\mathfrak{g}_C]$. For simplicity of notations write $\bar{A} = A_q/\mathfrak{q}_A$, $\bar{C} = C_C/qC_C$, and denote by $\bar{g}$ the image of $g \otimes A_q \bar{A}$ in $\text{Hom}_{A_q} (C_C, C_C) \otimes A_q \bar{A} = \text{Hom}_{A_q} (C, C)$.

So $\text{Hom}_{A_q} (\bar{C}, \bar{C}) = \bar{C}[\bar{g}]$. This means no nontrivial ideal in $\bar{C}$ is stable under $\bar{g}$. 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 $\mathfrak{g}_C$ admits a $p$-basis over $A_q$ [1, p. 107, Corollaire 1] and $C$ is a Galois extension over $A$.

It remains to show the inclusion map $g \rightarrow g(C/A)$ is onto. In view of [1, p. 111, Theorem 1], it suffices to show that at each prime $\mathfrak{p} \subseteq \text{Spec } C$, the corresponding map $\mathfrak{g}_C \rightarrow g(C/A)_C$ is onto. Now $\bar{g}$ is a free $\bar{C}$-module [5, Lemma 3.2]. Let $\bar{e}_1, \ldots, \bar{e}_r$ be a $\bar{C}$-module basis for $\bar{g}$. The fact that $\bar{g}$ is a restricted Lie ring implies that the set $\{ \bar{e} \bar{t}^1 \cdots \bar{e} \bar{t}^r \mid 0 \leq e_i < p \}$ form a set of generators for the $\bar{C}$-module $\text{Hom}_{\bar{A}} (\bar{C}, \bar{C}) = \bar{C}[\bar{g}]$. But $g(\bar{C}/A)$ is also a free $\bar{C}$-module because $\bar{C}$ admits a $p$-basis over $\bar{A}$. Let $r'$ be the dimension of $g(\bar{C}/A)$ over $\bar{C}$. Then $[\bar{C} : A] = r'$. Now as vector spaces over $\bar{A}$, $\bar{g}$ is a subspace of $g(\bar{C}/A)$, so $rp' = [\bar{g} : \bar{A}] \leq [g(\bar{C}/A) : \bar{A}] = r'p'$. Hence $r \leq r'$. On the other hand the $\bar{A}$-module $\text{Hom}_{\bar{A}} (\bar{C}, \bar{C})$ is of dimension $p^{2r'}$ but has a set of generators of cardinality $p^{r+r'} \leq p^{2r'}$. This shows $r = r'$ and therefore $\bar{g} = g(\bar{C}/A)$. So $\bar{e}_1, \ldots, \bar{e}_r$ form a $\bar{C}$-module basis for $g(\bar{C}/A)$. Let $\mathfrak{e}_i$ be a pre-image of $\bar{e}_i$ in $\mathfrak{g}_C$. Then $\mathfrak{e}_1, \ldots, \mathfrak{e}_r$ form a $C_C$-module basis for $g(C_C/A_C)$. This proves that $\mathfrak{g}_C = g(C_C/A_C)$ because $g_C \subseteq g(C_C/A_C) = \mathop{\sum}\nolimits C_C \mathfrak{e}_i \subseteq \mathfrak{g}_C$. Consequently $g_C = g(C_C/A_C) = g(C/A)$ 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 $A$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
(2) Let \( \mathfrak{g} = \{ d \in g(C/A) \mid dB \subseteq B \} \). Then there is a \( B \)-module homomorphism \( g(B/A) \to \mathfrak{g} \) which followed by the restriction map \( \mathfrak{g} \to g(B/A) \) given by \( d \to d|_B \) is the identity map on \( g(B/A) \).

(3) Let \( G(B/A) \) be the image of \( g(B/A) \) in \( \mathfrak{g} \). Then
\[
C \cdot G(B/A) \oplus g(C/B) = g(C/A).
\]

**Proof.** Let \( \mathfrak{q} \) be a prime ideal in \( C \) and denote by \( q \) and \( \mathfrak{q} \) 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 \( \alpha \in A - q \) such that \( C_{\alpha} \) is a free module of finite dimension both over \( A_{\alpha} \) and over \( B_{\alpha} \). The \( A_{\alpha} \)-module \( B_{\alpha} \) as a direct summand of \( C_{\alpha} \) is therefore finitely generated projective. So \( B \) is finitely generated projective as \( A \)-module. We would like to show that \( B_{\mathfrak{q}} \) admits a \( p \)-basis over \( A_{\mathfrak{q}} \). For simplicity of notations, write \( A = A_{\mathfrak{q}} / qA_{\mathfrak{q}} \), \( B = B_{\mathfrak{q}} / qB_{\mathfrak{q}} \) and \( \overline{C} = C_{\mathfrak{q}} / qC_{\mathfrak{q}} \). Let \( b_1, \ldots, b_r \) be a basis for the free \( \overline{B} \)-module \( \overline{C} \). Let \( \partial \) be an \( \overline{A} \)-derivation on \( \overline{C} \). For any \( x \in \overline{B} \), \( \partial x \) may be expressed in the form \( (\partial_1 x)b_1 + \cdots + (\partial_r x)b_r \), with \( \partial_i x \in \overline{B} \). It is easily seen that the map \( x \to \partial_i x \) is an \( \overline{A} \)-derivation on \( \overline{B} \). By Theorem 9 we have \( C[\{g(C/A)\}] = \text{Hom}_{A}(C, C) \) and hence
\[
\overline{C}[\mathfrak{g}] = \text{Hom}_{A}(\overline{C}, \overline{C})
\]
where \( \mathfrak{g} = g(C/A)_{\mathfrak{q}} / qg(C/A)_{\mathfrak{q}} \). So no nontrivial ideal in \( \overline{C} \) is stable under \( \mathfrak{g} \). Let \( I \) be a nonzero proper ideal in \( \overline{B} \). Then there is an \( \overline{A} \)-derivation \( \partial \) on \( \overline{C} \) such that \( \partial(I\overline{C}) \) is not contained in \( I\overline{C} \). This means \( \partial I \) cannot be contained in \( I \) for some \( i \). But \( \overline{B} \) is a finite dimensional vector space over \( \overline{A} \) so by [5, Corollary 2.8], \( \overline{B} \) admits a \( p \)-basis over \( \overline{A} \). Hence \( B_{\mathfrak{q}} \) admits a \( p \)-basis over \( A_{\mathfrak{q}} \) [1, p. 107, **Corollaire**].

To show the identity map \( g(B/A) \to g(B/A) \) factors through the restriction map \( \mathfrak{g} \to g(B/A) \), it suffices to show at each prime ideal \( q \) in \( B \) the identity map \( g(B/A)_q \to g(B/A)_q \) factors through \( \mathfrak{g}_q \to g(B/A)_q \). Let \( t_1, \ldots, t_l \) be a \( p \)-basis for \( C_\mathfrak{q} \) over \( B_\mathfrak{q} \) and let \( t_{l+1}, \ldots, t_{l+\lambda} \) be a \( p \)-basis for \( B_\mathfrak{q} \) over \( A_\mathfrak{q} \). If we denote by \( d_i \) the \( A_\mathfrak{q} \)-derivation on \( C_\mathfrak{q} \) given by \( d_i t_i = \delta_{ij} \), then the \( B_\mathfrak{q} \)-module \( H^q \) of all \( A_\mathfrak{q} \)-derivations on \( C_\mathfrak{q} \) leaving \( B_\mathfrak{q} \) invariant is just
\[
\sum_{i=1}^l C_i d_i + \sum_{i=1}^\lambda B_i d_{l+i}.
\]
It is obvious that the identity map on \( g(B/A)_q = g(B_q/A_q) \) factors through the restriction map \( H^q \to g(B/A)_q \). So it suffices to show \( \mathfrak{g}_q = H^q \).

Given any open set \( U \) in \( \text{Spec} A \), let \( H(U) \) be the set of all \( \overline{A}_U \)-derivations on \( \overline{C}_U \) leaving \( \overline{B}_U \) invariant. The set \( H(U) \) has an obvious \( \overline{B}(U) \)-module structure. So the sheaf \( U \to H(U) \) is a \( \overline{B} \)-module and its fibre at a point \( q \) in \( \text{Spec} B \) 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 \( \mathfrak{g} \) associated to \( \mathfrak{g} \). Hence by [2, p. 90, Theorem 1.4.1] \( H \) is always the sheaf \( \mathfrak{g} \) associated to \( \mathfrak{g} \) 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 \( g(B/A) \) factors through the restriction map \( \mathfrak{h} \to g(B/A) \). In particular \( \mathfrak{h} = G(B/A) \oplus g(C/B) \). Hence \( g(C/A) = C \cdot G(B/A) + g(C/B) \) because \( C \cdot \mathfrak{h} = g(C/A) \). Assume \( \partial \in [C \cdot G(B/A)] \cap g(C/B) \). We claim that \( \partial = 0 \). It suffices to show the corresponding derivation \( \partial_q \) at \( q \in \text{Spec } A \) is zero. Now \( \partial_q \) as an element in \([C \cdot G(B/A)]_q\) can be written in the form \( \sum_{i=1}^r u_i \partial_{i+1} \) with \( u_i \in C_\mathfrak{h} \) where \( \partial_{i+1} \) is the image of \( d_{i+1} \) in \( \mathfrak{h} \). So \( u_j = (\sum_{i=1}^r u_i \partial_{i+1}) t_{i+1} = \partial_q t_{i+1} = 0 \) because \( \partial_q \in g(C_\mathfrak{h}/C) \) and \( t_{i+1} \in B_\mathfrak{h} \). This shows \( \partial_q = 0 \) 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 \( \partial \) 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 \( B = \ker d \) and \( \text{Hom}_B (C, C) = C[d] \). 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 \( g(C/A) \) such that \( \mathfrak{h} \) is also a \( C \)-module direct summand of \( g(C/A) \). Put \( B = \ker \mathfrak{h} \). Then \( C \) is a Galois extension over \( B \) and \( g(C/B) = \mathfrak{h} \).

**Proof.** We shall first prove the theorem under the additional assumption that \( C \) is a local ring\(^2\). So \( C \) admits a \( p \)-basis \( t_1, \ldots, t_s \) 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 \( g(C/A) \). Now the \( C \)-module \( \mathfrak{h} \) as a direct summand of \( g(C/A) \) is also free. Let \( \partial_{1,0}, \ldots, \partial_{1,0} \) be a basis for \( \mathfrak{h} \). We have \( \delta_{i,0} = \sum_{j=1}^r (\partial_{i,0} t_j) \). Clearly given any \( i, \delta_{i,0} t_j \) must be an invertible element in \( C \) for at least one \( j \) \((1 \leq j \leq r)\). We claim that there exist \( \partial_1, \ldots, \partial_s \), a basis for \( \mathfrak{h} \) and elements \( y_1, \ldots, y_s \) in \( C \) such that \( \delta_{i,j} = \delta_{ij} \). Suppose we have already proven \( y_1, \ldots, y_s \) in \( C \) and a \( C \)-module basis \( \delta_{1,s}, \ldots, \delta_{1,s} \) for \( \mathfrak{h} \) such that \( \delta_{i,s} y_j = \delta_{ij} \) for \( 1 \leq i \leq l \) and \( 1 \leq j \leq s \). If \( s < l \), then there is an element \( y_{s+1} \) in \( C \) such that \( \delta_{s+1,s+1} y_{s+1} \) is invertible in \( C \). We set \( \delta_{s+1,s+1} = (\delta_{s+1,s} y_{s+1})^{-1} \delta_{s+1,s} \) so that \( \delta_{s+1,s+1} y_{s+1} = 1 \). For every \( j \neq s+1 \), we set \( \delta_{j,s+1} = \delta_{j,s} - (\delta_{j,s} y_{s+1}) \delta_{s+1,s+1} \).

Then we have \( \delta_{i,s+1} y_j = \delta_{ij} \) for \( 1 \leq i \leq l \) and \( 1 \leq j \leq s+1 \), and that \( \delta_{i,s+1} \) are still a basis for \( \mathfrak{h} \). Proceeding in this fashion, starting from the case \( s = 0 \), we finally obtain \( y_1, \ldots, y_s \) in \( C \) and \( \delta_i = \delta_{i,l} \) 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 \[ \partial_s v_s \partial_s = \sum_{s=1}^{n} v_s \partial_s \] with \( v_s \in C \), we get \( v_s = [\partial_s, \partial_s] y_s = 0 \) whence \([\partial_s, \partial_s] = 0\). In the same way we find that \( \partial_s^p = 0 \). 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 \( u_s \in C \) which is not in \( B[y_1, \ldots, y_s] \) and which is annihilated by every \( \partial_i \) with \( i < s \). Since \( \partial_s^p = 0 \) there is an exponent \( e (0 \leq e < p) \) such that \( \partial_s^{e+1} \) but not \( \partial_s^e \) 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 \( \partial_s(u_s) \), we may suppose that \( \partial_s(u_s) \in B[y_1, \ldots, y_l] \). Since \( \partial_s(u_s) \) is annihilated by each \( \partial_i \) with \( i < s \) it follows then that \( \partial_s(u_s) \in B[y_n, \ldots, y_l] \). 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 \( \partial_s^{p-1} \) (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 \( u \in B[y_1, \ldots, y_l] \) such that \( \partial_s(u) = \partial_s u \). Now put \( u_{s+1} = u_s - u \). Then \( u_{s+1} \notin B[y_1, \ldots, y_l] \) and \( \partial_s(u_{s+1}) = 0 \) for all \( i < s + 1 \). We can repeat this construction until we obtain \( u_{i+1} \notin B[y_1, \ldots, y_l] \) such that \( \partial_s(u_{i+1}) = 0 \) for all \( i = 1, \ldots, I \). But then \( u_{i+1} \in B \), and we have a contradiction. Hence \( C = B[y_1, \ldots, y_l] \). Moreover, if \( \partial \) 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 \( g(C/B) = \mathfrak{h} \). Since \( C \) is finitely generated as \( A \)-module so surely finitely generated over \( B \) also. At each prime \( \mathfrak{p} \) in \( C \), \( C_{\mathfrak{p}} \) admits a \( p \)-basis over \( B_q \) with \( q = \mathfrak{p} \cap B \). Moreover, the dimension \([C_{\mathfrak{p}} : B_q]\) is equal to the \([h_{C_{\mathfrak{p}} : C_{\mathfrak{p}}} : h_{B_q : B_q}]\)th power of \( p \). So \([C_{\mathfrak{p}} : B_q]\) is locally constant in \( \text{Spec} \ C \) because \([B_q : C_{\mathfrak{p}}]\) is. Hence \( C \) over \( B \) is finitely generated projective and therefore must be a Galois extension. Finally \( h_{C_{\mathfrak{p}}} \) is equal to \( g(C/B)_{\mathfrak{p}} \) at every \( \mathfrak{p} \in \text{Spec} \ C \). So the inclusion map \( \mathfrak{h} \rightarrow g(C/B) \) must be onto.

Summarizing the above results, we get

13. THEOREM. Let \( C \) be a Galois extension over \( A \) and denote by \( g_{C/A} \) the \( C \)-module of all \( A \)-derivations on \( C \). Put

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

\[ \Xi = \{g|g \text{ is a restricted Lie subring and a } C\text{-module direct summand of } g_{C/A}\}. \]

Then the mappings \( \Xi \rightarrow \Theta \rightarrow \Xi \) given respectively by \( g \rightarrow \text{kernel } g; B \rightarrow g_{C/B} \) are inverses to each other.

REFERENCES


STATE UNIVERSITY OF NEW YORK AT BUFFALO,
AMHERST, NEW YORK 14226