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 \( g \) be both a \( C \)-module and a restricted Lie ring of derivations on \( C \) and denote by \( A \) the kernel of \( g \), i.e., the set of all \( x \) in \( C \) such that \( dx = 0 \) for all \( d \) in \( g \). 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 \( C[g] = \text{Hom}_A(C, C) \). In this paper, we present a Galois correspondence between the restricted Lie subrings of \( g \) which are also \( C \)-module direct summands of \( g \) and the intermediate rings between \( C \) and \( A \) over which locally \( C \) admits \( p \)-basis. The Galois hypothesis \( C[g] = \text{Hom}_A(C, C) \) 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

\[ 0 \to L(C/A) \to P(A) \to P(C) \to \mathcal{E}(g, C) \to B(C/A) \to 0, \]

where \( B(C/A) \) is the Brauer group for \( C \) over \( A \), \( \mathcal{E}(g, C) \) is Hochschild's group of regular restricted Lie algebra extensions of \( C \) by \( g \), \( P \) 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 \( H^{n+2}_1(C/A, G_m) \), \( n \geq 0 \), are isomorphic to Hochschild's groups \( \mathcal{E}(C^n \otimes_A g, C^{n+1}) \) of regular restricted Lie algebra extensions of \( C^{n+1} \), the \( n+1 \)-fold tensor product \( C \otimes_A \cdots \otimes_A C \), by \( C^n \otimes_A g \).

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 \( \text{Spec} \ C \) is canonically homeomorphic to \( \text{Spec} \ A \).
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 \( \text{Spec } A \) and \( \text{Spec } C \).

2. Remark. In view of the above lemma, we may regard the structural sheaf \( \mathcal{A} \) associated to \( \text{Spec } A \) as a subsheaf of the structural sheaf \( \mathcal{C} \) associated to \( \text{Spec } C \). Moreover given any \( q \) in \( \text{Spec } A \), we shall always denote by \( \mathcal{C} \) the corresponding element in \( \text{Spec } C \) 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 \( \mathcal{C} \) is any prime ideal in \( C \) then

\[
M_{\mathcal{C}} = M \otimes_A A_q
\]

for all \( C \)-modules \( M \).

Proof. We have a map

\[
C \otimes_A A_q \rightarrow C_{\mathcal{C}},
\]

\[
x \otimes (a/s) \rightarrow (ax)/s \quad (s \in A - q)\]

Given any \( x/t \) in \( C_{\mathcal{C}} \) with \( t \in C - \mathcal{C} \), 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 \( x = \sum a_i x_i (\prod_j s_j) \) and \( s = \prod_i s_i \). If \( x \otimes (1/s) \) goes to zero in \( C_{\mathcal{C}} \), then for some \( t \in C - \mathcal{C} \), \( tx \) 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 \( C_{\mathcal{C}} \). If \( M \) is any \( C \)-module, we have

\[
M_{\mathcal{C}} = M \otimes_C C_{\mathcal{C}} = M \otimes_C C \otimes_A A_q = M \otimes_A A_q.
\]

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 $\mathcal{C}$ 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 $\mathcal{L}(\text{Spec } C, \mathcal{C}/\mathcal{A})$ 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 $A$(1). Denote by $\mathfrak{g}(C/A)$ the $C$-module of all $A$-derivations on $C$. Then the sheaf $\mathcal{L}_{\mathcal{C}/\mathcal{A}}$ is isomorphic to $\mathfrak{g}(C/A)$.

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

$$\mathcal{L}(D(f), \mathcal{C}/\mathcal{A}) \cong \mathcal{L}(\text{Spec } C_f, \mathcal{C}_f/\mathcal{A}_f)$$

$$\cong \mathfrak{g}(C_f/A_f)$$

$$\cong \mathfrak{g}(C/A).$$

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 $C_{\mathfrak{q}} = C \otimes_A A_{\mathfrak{q}}$ form a $p$-basis over $A_{\mathfrak{q}}$. If $\{\gamma_i\}$ 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 $\{\gamma_i\}$ 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 $\mathcal{C}$-module $\mathcal{L}_{\mathcal{C}/\mathcal{A}}$ of all $\mathcal{A}$-derivations on $\mathcal{C}$ is isomorphic to $\mathfrak{g}(C/A)$.

---

(1) By a $p$-basis of $C$ over $A$ we mean a subset $\{t_1, \ldots, t_r\}$ in $C$ such that $\{t_1^{e_1} \cdots t_r^{e_r} | 0 \leq e_i < p\}$ 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. $A = \{ t \in C \mid \partial t = 0 \text{ for all } \partial \in \mathfrak{g}(C/A) \} = \text{kernel } \mathfrak{g};$
3. $\text{Hom}_A(C, C) = C[\mathfrak{g}].$

**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 $q$, the map $A_q \hookrightarrow \text{kernel } \mathfrak{g}_q = (\text{kernel } \mathfrak{g})_q$ is onto [1, p. 111, Theorem 1]. By the same token the inclusion map $C[\mathfrak{g}] \hookrightarrow \text{Hom}_A(C, C)$ 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 $\mathfrak{g}$ 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 $\text{Hom}_A(C, C) = C[\mathfrak{g}]$ 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 $q$ be any prime ideal in $A$. We have, by [1, p. 98, Proposition 19], $\text{Hom}_{A_q}(C_q, C_q) = C_q[\mathfrak{g}_q]$. For simplicity of notations write $\bar{A} = A_q/qA_q$, $\bar{C} = C_q/qC_q$, and denote by $\bar{\mathfrak{g}}$ the image of $\mathfrak{g} \otimes_{A_q} \bar{A}$ in $\text{Hom}_{\bar{A}}(\bar{C}, \bar{C}) = C[\bar{\mathfrak{g}}]$. 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 $C_q$ 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 $\mathfrak{g} \hookrightarrow \mathfrak{g}(C/A)$ is onto. In view of [1, p. 111, Theorem 1], it suffices to show that at each prime $\mathfrak{p} \in \text{Spec } C$, the corresponding map $\mathfrak{g}_\mathfrak{p} \to \mathfrak{g}(C/A)_\mathfrak{p}$ is onto. Now $\bar{\mathfrak{g}}$ is a free $\bar{C}$-module [5, Lemma 3.2]. Let $\bar{\partial}_1, \ldots, \bar{\partial}_r$ 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 $\{ \bar{\partial}_1^e \cdots \bar{\partial}_r^e \mid 0 \leq e_i < p \}$ form a set of generators for the $\bar{C}$-module $\text{Hom}_{\bar{A}}(\bar{C}, \bar{C}) = C[\bar{\mathfrak{g}}]$. 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 $r p^{r'} = [\bar{\mathfrak{g}} : \bar{A}] \leq [\mathfrak{g}(\bar{C}/\bar{A}) : \bar{A}] = r' p^{r'}$. 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 $p^{r} p^{r'} \leq p^{2r'}$. This shows $r = r'$ and therefore $\bar{\mathfrak{g}} = \mathfrak{g}(\bar{C}/\bar{A})$. So $\bar{\partial}_1, \ldots, \bar{\partial}_r$ form a $\bar{C}$-module basis for $\mathfrak{g}(\bar{C}/\bar{A})$. Let $\partial_i$ be a pre-image of $\bar{\partial}_i$ in $\mathfrak{g}_\mathfrak{p}$. Then $\partial_1, \ldots, \partial_r$ form a $C_\mathfrak{p}$-module basis for $\mathfrak{g}(C_\mathfrak{p}/A_\mathfrak{p})$. This proves that $\mathfrak{g}_\mathfrak{p} = \mathfrak{g}(C_\mathfrak{p}/A_\mathfrak{p})$ because $\mathfrak{g}_\mathfrak{p} \subseteq \mathfrak{g}(C_\mathfrak{p}/A_\mathfrak{p}) = \sum C_\mathfrak{p} \partial_i \subseteq \mathfrak{g}_\mathfrak{p}$. Consequently $\mathfrak{g}_\mathfrak{p} = \mathfrak{g}(C_\mathfrak{p}/A_\mathfrak{p}) = \mathfrak{g}(C/A)_\mathfrak{p}$ because $C$ is a Galois extension over $A$.

11. **Theorem.** Let $A \subseteq B \subseteq C$ 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 \( \mathfrak{h} = \{ d \in g(B/A) \mid dB \subseteq B \} \). Then there is a \( B \)-module homomorphism \( g(B/A) \to \mathfrak{h} \) which followed by the restriction map \( \mathfrak{h} \to g(B/A) \) 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 \( \mathfrak{h} \). Then

\[
C \cdot G(B/A) \oplus g(C/B) = g(C/A).
\]

**Proof.** Let \( \mathfrak{p} \) be a prime ideal in \( C \) and denote by \( q \) 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 \( \alpha \in A - q \) such that \( C_{A_\alpha} \) is a free module of finite dimension both over \( A_{A_\alpha} \) and over \( B_{A_\alpha} \). The \( A_{A_\alpha} \)-module \( B_{A_\alpha} \) as a direct summand of \( C_{A_\alpha} \) is therefore finitely generated projective. So \( B \) is finitely generated projective as \( A \)-module. We would like to show that \( B_{A_\alpha} \) admits a \( p \)-basis over \( A_{A_\alpha} \). For simplicity of notations, write \( A = A_q/q_A, B = B_q/q_B \) and \( C = C_{C_0}/q_{C_0} \). Let \( b_1, \ldots, b_r \) be a basis for the free \( B \)-module \( C \). Let \( \partial \) be an \( A \)-derivation on \( C \). For any \( x \in B \), \( \partial x \) may be expressed in the form \( (\partial b_1)b_1 + \cdots + (\partial b_r)b_r \), with \( \partial b_i \in B \). It is easily seen that the map \( x \to \partial x \) is an \( A \)-derivation on \( B \). By Theorem 9 we have \( C[g(C/A)] = \text{Hom}_A(C, C) \) and hence

\[
\bar{C}[\bar{a}] = \text{Hom}_A(\bar{C}, \bar{C})
\]

where \( \bar{a} = g(C/A)_{C_0}/q_{g(C/A)_{C_0}} \). So no nontrivial ideal in \( \bar{C} \) is stable under \( \bar{a} \). Let \( I \) be a nonzero proper ideal in \( \bar{B} \). Then there is an \( \bar{A} \)-derivation \( \bar{\partial} \) on \( \bar{C} \) such that \( \bar{\partial}(IC) \) is not contained in \( IC \). This means \( \bar{\partial} I \) 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 \( B_{A_\alpha} \) admits a \( p \)-basis over \( A_{A_\alpha} \) [1, p. 107, Corollaire].

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

\[
\sum_{i=1}^{\lambda} C_{A_\lambda}d_i + \sum_{i=1}^{\lambda} B_{A_\lambda}d_{i+\lambda}.
\]

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

Given any open set \( U \) in \( \text{Spec} A \), let \( H(U) \) be the set of all \( \bar{A}_U \)-derivations on \( \bar{C}_U \) leaving \( \bar{B}_U \) invariant. The set \( H(U) \) has an obvious \( \bar{B}(U) \)-module structure. So the sheaf \( U \to H(U) \) is a \( \bar{B} \)-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 \( \mathfrak{h} \) associated to \( \mathfrak{h} \). Hence by [2, p. 90, Theorem 1.4.1] \( H \) is always the sheaf \( \mathfrak{h} \) 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 \( g(B/A) \) factors through the restriction map \( \mathfrak{h} \mapsto g(B/A) \). 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 \( [C \cdot G(B/A)]_\mathfrak{h} \) can be written in the form \( \sum_{i=1}^n u_i \partial_{i+1} \) with \( u_i \in C_C \) where \( \partial_{i+1} \) is the image of \( d_{i+1} \) in \( \mathfrak{h}_q \). So \( u_j = (\sum_{i=1}^n u_i \partial_{i+1} t_{i+1} = \partial_q t_{i+1} = 0 \) because \( \partial_q \in g(C_C/B_q) \) and \( t_{i+1} \in B_q \). This shows \( \partial_q = 0 \) as desired.

12. Remark. Given a tower of rings \( A \subseteq B \subseteq C \) 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 \( C \). 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 \( \text{Hom}_B(C, C) = C[d] \). 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 \( B = \text{kernel } \mathfrak{h} \). 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 \( t_1, \ldots, t_r \) 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 \( g(C/A) \). 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 \( \partial_{i,0} = \sum_{j=1}^n (\partial_{i,0} t_j) d_j \). Clearly given any \( i \), \( \partial_{i,0} t_j \) must be an invertible element in \( C \) for at least one \( j \) \((1 \leq j \leq r)\). We claim that there exist \( \partial_{1,1}, \ldots, \partial_{1,r} \) a basis for \( \mathfrak{h} \) and elements \( y_1, \ldots, y_r \) in \( C \) such that \( \partial_{i,j} y_j = \delta_{ij} \). Suppose we have already proven \( y_1, \ldots, y_s \) in \( C \) and a \( C \)-module basis \( \partial_{1,s}, \ldots, \partial_{1,s} \) for \( \mathfrak{h} \) such that \( \partial_{1,s} y_j = \delta_{ij} \) for \( 1 \leq i \leq s \) and \( 1 \leq j \leq s \). If \( s < r \), then there is an element \( y_{s+1} \) in \( C \) such that \( \partial_{s+1, s+1} y_{s+1} \) is invertible in \( C \). We set

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

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 \( 1 \leq i \leq s \) and \( 1 \leq j \leq s+1 \), 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 \( y_1, \ldots, y_s \) in \( C \) and \( \partial_i = \partial_{1,i} \) 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 $[\partial_i, \partial_j] = \sum_{s+1} v_s \partial_s$ 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 $B[y_1, \ldots, y_s]$ and which is annihilated by every $\partial_i$ with $i < s$. Since $\partial_p = 0$ there is an exponent $e$ ($0 < e < p$) such that $\partial_i^{p + 1}$ but not $\partial_i^p$ maps $u_s$ into $B[y_1, \ldots, y_l]$. We have $\partial_i \partial_i^p (u_s) = \partial_i^p \partial_i (u_s)$ which is zero for $i < s$. Hence replacing $u_s$ by $\partial_i^p (u_s)$, we may suppose that $\partial_i (u_s) \in B[y_1, \ldots, y_l]$. Since $\partial_i (u_s)$ is annihilated by each $\partial_i$ with $i < s$ it follows then that $\partial_i (u_s) \in B[y_s, \ldots, y_l]$. 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 $\partial_s^{p - 1}$ (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 $\partial_i (u_s) = \partial_i u$. Now put $u_{s+1} = u - u$. 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 $\partial$ 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 $[C_q : B_q]$ is equal to the $[h_q : C_q]$th power of $p$. So $[C_q : B_q]$ is locally constant in Spec $C$ because $[h_q : C_q]$ is. Hence $C$ over $B$ is finitely generated projective and therefore must be a Galois extension. Finally $h_q$ is equal to $g(C/B)\mathfrak{p}$ at every $\mathfrak{p} \in$ 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 $\Xi \rightarrow \Theta$, $\Theta \rightarrow \Xi$ given respectively by $g \rightarrow$ kernel $g$; $B \rightarrow g_{C/B}$ are inverses to each other.

REFERENCES


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