ON STRONGLY RADICIAL EXTENSIONS

Yasuji Takeuchi
ON STRONGLY RADICIAL EXTENSIONS

YASUJI TAKEUCHI

Let $A$ be a commutative ring and $C$ a commutative ring-extension of $A$ such that the canonical morphism: $\text{Spec}(C) \to \text{Spec}(A)$ induced by the inclusion map: $A \to C$ is radicial. In this paper a Galois theory of such extension $C/A$ is given, with certain additional assumptions.

Let $A$ be a commutative ring with an identity such that for each prime ideal $\mathfrak{p}$ in $A$ the residue ring $A/\mathfrak{p}$ is of prime characteristic. We say that a commutative ring-extension $C$ of $A$ is strongly radicial if $C$ is finitely generated projective as an $A$-module and the Kernel of the multiplication map: $C \otimes_A C \to C$ is a nil-ideal. In this paper, we shall study a Galois theory of strongly radicial extensions. The main tool used here is higher order derivations, which have been studied in [5], [6], and [7]. The reader should consult them, especially [5], [6], for relevant definitions and basic properties.

In §1 we introduce differentiably simple rings and exhibit a structure theorem. We shall later apply this to study the structure of strongly radicial extensions.

In §2 we give criteria for strongly radiciality. We also generalize some of the results about purely inseparable field-extensions to our case. Moreover, we show a structure theorem of strongly radicial extensions.

In §3 we give a Galois correspondence theorem for a strongly radicial extension.

In all that follows all rings are commutative with an identity, and all homomorphisms and all modules are unitary. Unadorned $\otimes$ will mean $\otimes_A$. If $A$ is a subring of a ring $C$, both $A$ and $C$ are assumed to have the same identity.

1. Differentiably simple rings. Let $C$ be a commutative ring. For any $q$th order derivation $D$ on $C$ and any $a \in C$, $[D, a](x)$ denotes a $(q - 1)$th order derivation on $C$ which is defined by $[D, a](x) = D(ax) - aD(x) - D(a)x$ for $x \in C$. Let $\mathcal{H}$ be any nonempty set of higher order derivations on $C$ with $[D, a] \in \mathcal{H}$ for all $D \in \mathcal{H}$, all $a \in C$. In this case, the set $\{a \in C \mid D(a) = 0 \text{ for all } D \in \mathcal{H}\}$ forms a subring of $C$, denoted by $\text{Ker}(\mathcal{H})$. If $C$ has no nontrivial $\mathcal{H}$-stable ideal, $C$ will be called an $\mathcal{H}$-simple ring. For an $\mathcal{H}$-simple ring $C$, let $A$ denote $\text{Ker}(\mathcal{H})$. Then the following properties hold:

(1) $A$ is a field.

1 For the definition of radicial, see [Grothendieck: E. G. A. I (3.5.4)].
The exponent of $C$ over $A$ is finite if $A$ is of prime characteristic and $C$ is finite dimensional over $A$.

The proof is omitted, because it is quite similar to the proof of Lemma 2.1 in [12].

**Proposition 1.** Let $C$ be a commutative ring of prime characteristic $p$ and $\mathcal{H}$ any nonempty set of higher order derivations on $C$ with $[D, a] \in \mathcal{H}$ for all $D \in \mathcal{H}$, all $a \in C$. Suppose that the orders of the derivations in $\mathcal{H}$ are bounded and $C$ is $\mathcal{H}$-simple. Then $C$ is a local ring whose radical $Q$ is a nil-ideal. Moreover, we have $C = F + Q$ for a subfield $F$ of $C$ containing $\ker(\mathcal{H})$.

Proof. Let $q$ be the supremum of orders of the derivations in $\mathcal{H}$. For any $x \in C$, we have $D(x^q) = 0$ for $D \in \mathcal{H}$ where $p^s > q$, and so $x^q \in \ker(\mathcal{H})$ [c.f., 5, Chap. I, Prop. 10]. Since $\ker(\mathcal{H})$ is a field, we obtain $x^q = 0$ for any nonunit $x \in C$. This shows the radical $Q$ of $C$ is a nil-ideal and is a uniquely maximal ideal. Now we shall show the second statement. Let $E^i(S)$ denote a set $\{x^q \mid x \in S\}$ for a subset $S$ of $C$. Let $s$ be the minimal positive integer with $E^s(C) \subseteq \ker(\mathcal{H})$. Then $E^s(C)$ is a field. We shall show $E^i(C) = F_i + E^i(Q)$ for $i = 0, 1, \ldots, s$ where $F_i$ are a subfield of $E^i(C)$, respectively. Assume we have already proved this fact for $i = r+1, \ldots, s$. Let $F_r$ be a maximal field contained in $E^r(C)$ with $F_{r+1} \subseteq F_r$. Suppose $F_r + E^r(Q) \neq E^r(C)$. Then there is an $x \in E^r(C)$ not belonging to $F_r + E^r(Q)$. We can write $x^p = a + y$ for $a \in F_{r+1}, y \in E^{r+1}(Q)$. Since $E^{r+1}(Q) = E^r(E^r(Q))$, we obtain $(x - y)^p = a$ for $y \in E^r(Q)$. Then $x - y$ does not belong to $F_r + E^r(Q)$, which is denoted by $x_0$. Since $\pi(F_r)[\pi(x_0)]$ is a field properly containing $\pi(F_r)$ where $\pi$ is the canonical map of $E^r(C)$ onto the field $E^r(C)/E^r(Q)$, a polynomial $X^p - a$ is irreducible in $F_r[X]$. So $F_r[x_0]$ is a field, which is a contradiction. So we have $C = F_0 + Q$. Unless $F_0$ contains $\ker(\mathcal{H})$, take a maximal subfield $F$ of $F_0 \ker(\mathcal{H})$ containing $\ker(\mathcal{H})$. Then we claim $C = F + Q$. Assume this is not the case. Then there is an element $x$ in $F_0$ not belonging to $F + Q$. Let $t$ be the minimal positive integer with $x^{qt} \in F$. Then a polynomial $X^{qt} - x^{qt}$ in $F[X]$ is irreducible. Hence $F[x]$ is isomorphic to a residue field $F[X]/(X^{qt} - x^{qt})$, that is a contradiction to the maximality of $F$. This completes the proof.

2. Strongly radicial extensions. Let $A$ be a commutative ring and $C$ a commutative ring-extension of $A$. Let $J_{cl, A}$ denote the Kernel of the multiplication map $\mu: C \otimes C \to C$.

**Definition.** Let $A$ and $C$ be as above. Suppose the integral
domain $A/p$ is of prime characteristic for each $p \in \text{Spec}(A)$. We shall call $C$ a strongly radicial extension of $A$ if the following conditions are satisfied:

1. $C$ is finitely generated and projective as an $A$-module.
2. The ideal $J_{C/A}$ is nilpotent.

The $C$-module of $q$th order $A$-derivations on $C$ is denoted by $Der_q(C/A)$. We shall set $\text{Der}(C/A) = \bigcup_{q=1}^{\infty} \text{Der}_q(C/A)$. Then there are $C$-module isomorphisms $\varphi_q : \text{Hom}_C(\Omega^q_A(C), C) \rightarrow \text{Der}_q(C/A)$ by $\varphi_q(f) = f \cdot \delta^{(q)}$ and $\varphi : \text{Hom}_C(J_{C/A}, C) \rightarrow \text{Der}(C/A)$ by $\varphi(f) = f \cdot \delta$ where $\delta$ is an $A$-module map: $C \rightarrow J_{C/A}$ by $\delta(c) = 1 \otimes e - c \otimes 1$ for $c \in C$ and $\delta^{(q)}$ is an $A$-module map: $C \rightarrow \Omega^q_A(C)$ by $\delta^{(q)}(c) = \{\text{class of } \delta(c) \text{ modulo } (J_{C/A})^{q+1}\}$. The map $\delta^{(q)}$ is called the canonical $q$th order derivation of $C/A$.

Let $\nu$ be the map: $C \rightarrow \text{Hom}_A(C, C)$ by $\nu(c)(x) = cx$ for $c, x \in C$. We shall put $\mathcal{D}_q(C/A) = \nu(C) + \text{Der}_q(C/A)$ and $\mathcal{D}(C/A) = \nu(C) + \text{Der}(C/A)$. Then $\mathcal{D}(C/A)$ forms an $A$-algebra [c.f., 5].

**Proposition 2.** Let $A$ be a commutative ring such that the domain $A/p$ is of prime characteristic for each $p \in \text{Spec}(A)$. Let $C$ be a commutative ring-extension of $A$ which is finitely generated projective as an $A$-module. Then the necessary and sufficient condition that $C$ is a strongly radicial extension of $A$ is $\mathcal{D}(C/A) = \text{Der}(C/A)$.

**Proof.** The necessity is obvious. Suppose $\mathcal{D}(C/A) = \text{Der}(C/A)$. Then the $C$-module $\text{Der}(C/A)$ is generated by finitely many derivations, because it is a $C$-module direct summand of the finitely generated $C$-module $\text{Hom}_A(C, C)$. So $\mathcal{D}_q(C/A) = \text{Hom}_A(C, C)$ for the supremum $q$ of orders of their derivations. In order to show $J_{C/A}$ is nilpotent, it is sufficient to observe the canonical epimorphism: $J_{C/A} \rightarrow \Omega^q_A(C)$ is injective, accordingly so is the canonical epimorphism: $J_{C/pA} \rightarrow \Omega^q_A(C)$ for each $p \in \text{Spec}(A)$. This is obvious from the following lemma, because $\{1 \otimes u_i - u_i \otimes 1 \mid i = 1, 2, \ldots, m\}$ form a $C_p$-module basis for $J_{C/pA}$ where $\{1, u_1, u_2, \ldots, u_m\}$ is an $A_p$-module basis for $C_p$.

**Lemma 3.** Let $A$ be a commutative ring and $C$ a commutative $A$-algebra which is a finitely generated free $A$-module with a basis $\{1, u_1, u_2, \ldots, u_m\}$. If $\mathcal{D}_q(C/A) = \text{Hom}_A(C, C)$ for some positive integer $q$, then $\Omega^q_A(C)$ is a free $C$-module with a basis $\{\delta^{(q)}(u_i), \delta^{(q)}(u_2), \ldots, \delta^{(q)}(u_m)\}$ where $\delta^{(q)}$ is the canonical $q$th order derivation of $C/A$.

**Proof.** From the hypothesis, we have a $C$-module isomorphism $\varphi : C \oplus \text{Hom}_C(\Omega^q_A(C), C) \rightarrow \text{Hom}_A(C, C)$ by $\varphi(c + f) = cx + (f \cdot \delta^{(q)})(x)$

---

\[\Omega^q_A(C)\] denotes the module of $q$th order differentials $J_{C/A}^q(J_{C/A})^{q+1}$ [c.f., 5].
for \( c, x \in C, f \in \text{Hom}_C(\Omega^i(C), C) \). Let \( D_t(i = 1, 2, \ldots, m) \) be elements of \( \text{Hom}_A(C, C) \) such that \( D_t(1) = 0 \) for all \( i \) and \( D_t(u_j) = \delta_{i,j} \) for \( i, j = 1, 2, \ldots, m \). Moreover, let \( f_t \) be elements of \( \text{Hom}_C(\Omega^i(C), C) \) with \( \psi(f_t) = D_t \). Then we have \( f_t(\delta^{(q)}(u_j)) = \delta_{i,j} \). Since the set \( \{\delta^{(q)}(u_1), \delta^{(q)}(u_2), \ldots, \delta^{(q)}(u_m)\} \) forms a set of generators of \( \Omega^q(C) \) as a \( C \)-module, \( \Omega^q(C) \) is a free \( C \)-module with \( \{\delta^{(q)}(u_1), \delta^{(q)}(u_2), \ldots, \delta^{(q)}(u_m)\} \) as a basis.

We obtain a following corollary to Proposition 2.

**Corollary.** Let \( A \) be a commutative ring of prime characteristic \( p \) and \( C \) a commutative ring-extension of \( A \) which is finitely generated projective as an \( A \)-module. Then \( C \) is a strongly radicial extension of \( A \) if and only if \( C \) has a finite exponent over \( A \).

**Proof.** If \( C \) has a finite exponent over \( A \), then \( J_{C/A} \) is a nil-ideal. This shows the "if" part, because \( J_{C/A} \) is finitely generated as a \( C \)-module. Conversely assume \( C \) is a strongly radicial extension of \( A \). Then \( \mathcal{D}(C/A) = \text{Hom}_A(C, C) \) for some positive integer \( q \). Since \( A = \text{Ker}(\text{Der}_q(C/A)) \), it follows from [5, Chap. I, Prop. 10] that \( E^q(C) \) is contained in \( A \) for a positive integer \( e \) with \( p^e > q \). This completes the proof.

Now we give a structure theorem of strongly radicial extensions.

**Theorem 4.** Let \( A \) be a commutative ring such that the domain \( A/p \) is of prime characteristic for each \( p \in \text{Spec}(A) \). Then, for a strongly radicial extension \( C \) of \( A \), the followings hold:

1. The map \( *i : \text{Spec}(C) \rightarrow \text{Spec}(A) \) induced canonically by the inclusion map \( i : A \rightarrow C \) is bijective.
2. For each prime ideal \( p \) in \( A \) we have \( C \otimes A(p)^3 = F_p + Q_p \) where \( F_p \) is a subfield of \( C \otimes A(p) \) being purely inseparable over \( A(p) \) and \( Q_p \) is a nilpotent maximal ideal in \( C \otimes A(p) \).

**Proof.** For simplicity of notation set \( \bar{A} = A(p) \) for any \( p \in \text{Spec}(A) \), and set \( \bar{C} = C \otimes A(p) \). Then we have \( \mathcal{D}(C/A) \otimes \bar{A} \cong \text{Hom}_A(\bar{C}, \bar{C}) \) and so \( D(C/A) = \text{Hom}_A(\bar{C}, \bar{C}) \). Hence \( \bar{C} \) is a \( \text{Der}(C/A) \)-simple ring and \( \text{Ker}(\text{Der}(\bar{C}/\bar{A})) \) is equal to \( \bar{A} \). So (2) follows from Proposition 1. Since \( C \otimes A(p) \) is local for any \( p \in \text{Spec}(A) \), the map \( *i \) is injective. Since \( C \) is integral over \( A \), the map \( *i \) is surjective. This completes the proof.

**Corollary.** Let \( A \) and \( C \) be as above. Then an \( A/R_A \)-automorphism of \( C/R_C \) induced canonically by any \( A \)-automorphism of \( A(p) \) usually denotes the residue field \( A_p/A_p \).
C reduces always to the identity map on $C/R_c$ where $R_A$, $R_c$ are the nil-radical of $A$, $C$, respectively.

Proof. Let $\sigma$ be any $A$-automorphism of $C$. For any prime ideal $\mathfrak{P}$ of $C$, we have $\sigma(\mathfrak{P}) = \mathfrak{P}$, because $^\ast i(\sigma(\mathfrak{P})) = ^\ast i(\mathfrak{P})$ where $^\ast i$ is as above. So $\sigma$ induces canonically an automorphism of $C/\mathfrak{P}$, which reduces to the identity map on $C/\mathfrak{P}$. This shows $x - \sigma(x) \in \mathfrak{P}$ for all $x \in C$ and so $x \equiv \sigma(x) \mod R_c$.

**Proposition 5.** Let $A$ be a commutative ring such that the domain $A/p$ is of prime characteristic for each prime ideal $p$ in $A$. Let $C$ be a commutative ring-extension of $A$ which is a finitely generated projective $A$-module. Then $C$ is a strongly radicial extension of $A$ if and only if $C_p$ is a strongly radicial extension of $A_p$ for each $p \in \text{Spec}(A)$.

Proof. The “only if” part is obvious. In order to show the “if” part, it is sufficient to prove the fact that the canonical injection: $C \oplus \text{Der}(C/A) \rightarrow \text{Hom}_A(C, C)$ is an epimorphism, accordingly so is the canonical injection: $C_p \oplus \text{Der}(C/A)_p \rightarrow \text{Hom}_A(C, C)_p$ for each $p \in \text{Spec}(A)$. Let $\varphi$ be the composition of the following canonical maps

$$C_p \oplus \text{Der}(C/A)_p \rightarrow \text{Hom}_A(C, C)_p \rightarrow \text{Hom}_A(C_p, C_p) \rightarrow C_p \oplus \text{Der}(C/A)_p.$$  

Then we have $\varphi(\text{Der}(C/A)_p) \subseteq \text{Der}(C_p/A_p)$. We shall show $\varphi$ maps $\text{Der}(C/A)_p$ onto $\text{Der}(C_p/A_p)$. By the above isomorphisms any element $D_p$ of $\text{Der}(C_p/A_p)$ can be identified with an element of form $(1/s)D$ in $\text{Hom}_A(C, C)_s$ for $s \in A - p$, $D \in \text{Hom}_A(C, C)$. If $D_s$ is of order $q$, we have finitely many equalities in $C_p$,

$$\frac{1}{s} D(x_0 x_1 \cdots x_q) = \sum_{k=1}^{q} (-1)^{k-1} \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k} \left( \frac{1}{s} \right) D(x_0 \cdots \hat{x}_{i_1} \cdots \hat{x}_{i_k} \cdots x_q),$$

where $x_i (i = 0, 1, \cdots, q)$ range over a finite set of generators for the $A$-module $C$. So there is an element $t$ in $A - p$ such that $tD$ is a $q$th order $A$-derivation on $C$. Hence we have $(1/s)D = (1/st) tD \in \text{Der}(C/A)_s$ and $\varphi((1/s)D) = D_s$.

**Corollary.** If $C$ is a strongly radicial extension of a commutative ring $B$ and $B$ is a strongly radicial extension of a commutative ring $A$, then $C$ is also a strongly radicial extension of $A$.

Proof. By the above proposition we may assume, without loss
of generality, that $A$ and $B$ are local. Hence $C$ is $B$-free and $B$ is $A$-free. Then we have a $C$-module exact sequence $0 \rightarrow (C \otimes C)J_{B/A} \rightarrow J_{C/A} \rightarrow J_{C/B} \rightarrow 0$. Since both $J_{C/B}$ and $(C \otimes C)J_{B/A}$ are nilpotent, $J_{C/A}$ is also nilpotent.

We conclude this section, showing a converse to Theorem 4 under certain assumption on the basic ring.

**Proposition 6.** Let $A$ be a commutative ring such that, for each $p \in \mathrm{Spec}(A)$, $A_p$ is artinian and $A(p)$ is of prime characteristic. Let $C$ be a commutative ring-extension of $A$ which is finitely generated projective as an $A$-module. Then $C$ is a strongly radicial extension of $A$ if, for each $p \in \mathrm{Spec}(A)$, we have $C \otimes A(p) = F_p + Q_p$ where $Q_p$ is the nil-radical of $C \otimes A(p)$ and $F_p$ is a subfield of $C \otimes A(p)$ which is purely inseparable over $A(p)$.

**Proof.** From Proposition 5 if suffices to prove when $A$ is local. Let $m$ be the maximal ideal of $A$. Then $m$ is nilpotent. Now we have a commutative diagram

\[
\begin{array}{ccccccccc}
0 & \rightarrow & C \otimes C \otimes m & \rightarrow & C \otimes C & \rightarrow & C(m) \otimes C(m) & \rightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
J_{C/A} & \rightarrow & J_{C(m)/A(m)} & & & & & & \\
0 & \rightarrow & C \otimes m & \rightarrow & C & \rightarrow & C(m) & \rightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
0 & & 0 & & 0 & & 0 & &
\end{array}
\]

whose all the vertical and horizontal sequence are exact where $\mu$ is the multiplication map: $C \otimes C \rightarrow C$ and the other maps are also canonical. From this diagram, we obtain an exact sequence $0 \rightarrow \ker (\mu \otimes 1) \rightarrow J_{C/A} \rightarrow J_{C(m)/A(m)}$. Since $\ker (\mu \otimes 1) = J_{C(A)} \otimes m$, $\ker (\mu \otimes 1)$ is nilpotent. So $J_{C/A}$ is nilpotent. This completes the proof.

3. The Galois correspondence theorem. An aim in this section is to show a Galois correspondence theorem on strongly radical extensions as follows.

**Theorem 7.** Let $C$ be a strongly radicial extension of a commutative ring $A$. Let $A$ be the set of $C$-module direct summands $\mathcal{S}$
of $\text{Der}(C/A)$ with $DD' \in \mathcal{E}$ and $[D, x] \in \mathcal{E}$ for all $D, D' \in \mathcal{E}$ and all $x \in C$. Let $\Gamma$ be the set of intermediate rings between $A$ and $C$, over which $C$ is projective. Then correspondences $\delta: \Delta \to \Gamma$, $\gamma: \Gamma \to \Delta$ given respectively by $\delta(\mathcal{E}) = \ker(\mathcal{E})$, $\gamma(B) = \text{Der}(C/B)$ are inverse to each other.

In order to prove this theorem two lemmas are necessary.

**Lemma 8.** Let $A, C$ be as above and $B$ an intermediate ring between $A$ and $C$. If $C$ is projective as a $B$-module, then $C$ is a strongly radicial extension of $B$ and $B$ is also a strongly radicial extension of $A$. In this case, the $C$-module $\text{Der}(C/B)$ is a $C$-module direct summand of $\text{Der}(C/A)$.

Proof. In order to show the first statement, it suffices to observe $\text{Hom}_B(C, C)$ is contained in $\mathcal{E}(C/B)$. For any $f \in \text{Hom}_B(C, C)$, we have $f = c + D$ for $c \in C$, $D \in \text{Der}(C/A)$. Then $cbx + D(bx) = f(bx) = bf(x) = cbx + bD(x)$ for any $b \in B$, any $x \in C$. This shows $D$ belongs to $\text{Der}(C/B)$. The second assertion follows obviously from the fact that $B$ is an $A$-module direct summand of $C$ and $J_{B/A}$ is contained in the nilpotent ideal $J_{C/A}$. Now we shall prove the last statement. For any $p \in \text{Spec}(A)$, a sequence of canonical $C_p$-module homomorphisms

$$0 \to (C \otimes A_p)J_{B_p/A_p} \to J_{C_p/A_p} \to J_{C_p/B_p} \to 0$$

is exact, because both $B_p$ and $C_p$ are $A_p$-free. Hence a sequence of canonical $C_p$-module homomorphisms

$$0 \to (C \otimes C)J_{B/A} \to J_{C/A} \to J_{C/B} \to 0$$

is exact and so is split, since $J_{C/B}$ is $C$-projective. So we have a $C$-module isomorphism:

$$\text{Hom}_C(J_{C/A}, C) \to \text{Hom}_C(J_{C/B}, C) \oplus \text{Hom}_C((C \otimes C)J_{B/A}, C).$$

Since $\text{Der}(C/A) \cong \text{Hom}_C(J_{C/A}, C)$ and $\text{Der}(C/B) \cong \text{Hom}_C(J_{C/B}, C)$, our requirement is obtained.

**Lemma 9.** Let $C$ be strongly radicial extension of a local ring $A$. Let $\mathcal{E}$ be a $C$-module direct summand of $\text{Hom}_A(C, C)$ which is finitely generated free. Then there exist elements $c_1, c_2, \ldots, c_n$ in $C$ and a $C$-module basis $D_1, D_2, \ldots, D_n$ for $\mathcal{E}$ with $D_i(c_j) = \delta_{i,j}$ for $i, j = 1, 2, \ldots, n$.

Proof. In this case $C$ is local by Theorem 4. Let $m$ be the maximal ideal in $A$ and $Q$ the maximal ideal in $C$. Put $\bar{A} = A/m$
and \( \bar{C} = \mathcal{C}/m\mathcal{C} \). Since \( \mathcal{E}(\bar{C}/\bar{A}) = \text{Hom}_\mathcal{A}(\bar{C}, \bar{C}) \), \( \bar{C} \) is a \( \text{Der}(\bar{C}/\bar{A}) \)-simple ring. Let \( D_{0,1}, D_{0,2}, \ldots, D_{0,n} \) be a \( \mathcal{C} \)-module basis for \( \mathcal{E} \). We show first \( D_{0,i} = 0 \) for all \( i \). Assume this is not the case. For the minimal positive integer \( e \) with \( Q^e \subseteq m\mathcal{C} \), we have \( xD_{0,i} = 0 \) mod. \( m\mathcal{C} \) where \( x \) ranges over the elements of \( Q^{e-1} \). Since \( D_{0,i} \) is free mod. \( m\mathcal{C} \), we obtain \( x \in m\mathcal{C} \), which is a contradiction. Suppose we have already found \( c_1, c_2, \ldots, c_t \) in \( \mathcal{C} \) and a \( \mathcal{C} \)-module basis \( D_{t+1,1}, D_{t+1,2}, \ldots, D_{t+1,n} \) for \( \mathcal{E} \) with \( D_{t+1,i}(c_j) = \delta_{i,j} \) for \( 1 \leq i \leq n, 1 \leq j \leq t \). If \( l < r \), there is an element \( c_{t+1} \) in \( \mathcal{C} \) such that \( D_{t+1,i}(c_{t+1}) \) is a unit in \( \mathcal{C} \). Set \( D_{t+1,i+1} = (D_{t+1,i}(c_{t+1}))^{-1}D_{t+1,i} \) and \( D_{t+1,i} = D_{t+1,i} - D_{t+1,i}(c_{t+1})D_{t+1,i+1} \) for \( i \neq l + 1 \). Then we have \( D_{t+1,i}(c_j) = \delta_{i,j} \) for \( 1 \leq i \leq n, 1 \leq j \leq l + 1 \) and the \( D_{t+1,i} \)'s are a basis for \( \mathcal{E} \). Proceeding in this fashion, we find \( c_1, c_2, \ldots, c_n \) and \( D_1, D_2, \ldots, D_n \) as desired.

Now we can prove Theorem 7.

Proof of Theorem 7. It follows from Lemma 8 that \( \gamma \) is well-defined. We have to show \( \delta \) is well-defined. For any \( \mathcal{E} \in \Delta \), put \( B = \text{Ker}(\mathcal{E}) \). In the case of any local ring \( A \), we shall first observe \( \mathcal{C} \) is free over \( B \). From the above lemma there are elements \( c_1, c_2, \ldots, c_r \) in \( \mathcal{C} \) and a \( \mathcal{C} \)-module basis \( D_1, D_2, \ldots, D_r \) for \( \mathcal{E} \) with \( D_i(c_j) = \delta_{i,j} \) \( (i, j = 1, 2, \ldots, r) \). Then we have \( D_iD_j = 0 \) for \( i, j = 1, 2, \ldots, r \). In fact, we can write \( D_iD_j = x_iD_1 + \cdots + x_rD_r \) for \( x_i, \ldots, x_r \in \mathcal{C} \). Then we have \( x_k = (\sum_{i=1}^r x_iD_i)(c_k) = D_iD_j(c_k) = 0 \) for \( k = 1, 2, \ldots, r \) and so \( D_iD_j = 0 \). Since \( D(bx) = bD(x) + xD(b) + [D, x](b) \) for any \( D \in \mathcal{E}, \) \( b \in B \), \( x \in \mathcal{C} \), any element of \( \mathcal{E} \) is a \( B \)-homomorphism. Set \( C_1 = B + Bc_1 + \cdots + Bc_r \). Then \( C_1 \) is \( B \)-free. We shall show \( C = C_1 \).

Assume this is not the case. Then there is an element \( u \) in \( \mathcal{C} \) not belonging to \( C_1 \). Suppose inductively that we have already found an element \( u_i \) in \( \mathcal{C} \) not belonging to \( C_i \) with \( D_k(u_i) = 0 \) for all \( k \leq i \). Then \( D_{i+1}(u_i) \) belongs to \( B \). Set \( u_{i+1} = u_i - D_{i+1}(u_i)c_{i+1} \). Then \( u_{i+1} \) does not belong to \( C_i \) and we have \( D_k(u_{i+1}) = 0 \) for all \( k \leq i + 1 \), because \( D_iD_j = 0 \) for \( i, j = 1, 2, \ldots, r \). Repeating this construction, we can obtain an element \( u_r \) in \( \mathcal{C} \) with \( u_r \in C_1 \) and \( D_i(u_r) = 0 \) for \( i = 1, 2, \ldots, r \). Then \( u_r \) belongs to \( B \), which is absurd. Hence we have \( C = C_1 \) and so \( \mathcal{C} \) is a free \( B \)-module when \( A \) is local. In the case of any general ring \( A \), \( \mathcal{E}_\mathfrak{p} \) is a \( C_\mathfrak{p} \)-module direct summand of \( \text{Der}(C_\mathfrak{p}/A_\mathfrak{p}) \) for each \( \mathfrak{p} \in \text{Spec}(A) \). Moreover, we have \( B_\mathfrak{p} = \text{Ker}(\mathcal{E}_\mathfrak{p}) \). So, from the result above, \( C_\mathfrak{p} \) is a free \( B_\mathfrak{p} \)-module of rank equal to \( \text{rank}_{C_\mathfrak{p}}(\mathcal{E}_\mathfrak{p}) + 1 \). Since \( C_\mathfrak{p} \) is a finitely generated projective \( C_\mathfrak{p} \)-module, the map of \( \text{Spec}(A) \) into the domain of rational integers by \( \mathfrak{p} \mapsto \text{rank}_{C_\mathfrak{p}}(\mathcal{E}_\mathfrak{p}) + 1 \) is locally constant [2, Chap. II, §5, No 2, Theorem 1]. On the other hand, by Theorem 4, we have \( \text{Spec}(C) \cong \text{Spec}(B) \cong \text{Spec}(A) \) as the topological spaces and \( \text{rank}_{C_\mathfrak{p}}(\mathcal{E}_\mathfrak{p}) + 1 = \text{rank}_{C_\mathfrak{p}}(\mathcal{E}_\mathfrak{p}) + 1 \) for any \( \mathfrak{p} \in \text{Spec}(B), \mathfrak{p} = \mathfrak{p} \cap A \). By [2, ibid], \( C \) is projective over \( B \).
and so \( \delta \) is well-defined. Hence we have \( \text{Der}(C_v/B_v) \cong \text{Hom}_{C_v}(J_{C_v}/B_v, C_v) \) for each \( v \in \text{Spec}(A) \). This shows \( \text{Der}(C_v/B_v) \) is generated by such a \( C \)-module basis \( D_1, D_2, \ldots, D_r \) for \( S_v \) as the above argument. So we obtain \( \mathcal{E}_v = \text{Der}(C_v/B_v) \) for each \( v \in \text{Spec}(A) \) and so \( \mathcal{E} = \text{Der}(C/B) \). This shows \( \gamma \cdot \delta \) is the identity map on \( \Lambda \). It is obvious that \( \delta \cdot \gamma \) is the identity map on \( \Gamma \). This completes the proof.

**References**

9. ———, *On Galois objects which are strongly radicial over its basic ring*, to appear.

Received May 21, 1973 and in revised form September 17, 1974.

Kobe University
Walter Allegretto, *On the equivalence of two types of oscillation for elliptic operators* .................................................................................................................. 319
Edward Arthur Bertram, *A density theorem on the number of conjugacy classes in finite groups* ................................................................. 329
Arne Brøndsted, *On a lemma of Bishop and Phelps* .................................................. 335
Jacob Burbea, *Total positivity and reproducing kernels* ........................................... 343
Ed Dubinsky, *Linear Pincherle sequences* ............................................................ 361
Benny Dan Evans, *Cyclic amalgamations of residually finite groups* .............. 371
Barry J. Gardner and Patrick Noble Stewart, *A “going down” theorem for certain reflected radicals* ............................................................. 381
Sav Roman Harasymiv, *Groups of matrices acting on distribution spaces* .......... 403
Robert Winship Heath and David John Lutzer, *Dugundji extension theorems for linearly ordered spaces* ................................................. 419
Chung-Wu Ho, *Deforming p. l. homeomorphisms on a convex polygonal 2-disk* ............................................................................................................. 427
Richard Earl Hodel, *Metrizability of topological spaces* ...................................... 441
Wilfried Imrich and Mark E. Watkins, *On graphical regular representations of cyclic extensions of groups* ................................................ 461
Jozef Krasinkiewicz, *Remark on mappings not raising dimension of curves* ................. 479
Melven Robert Krom, *Infinite games and special Baire space extensions* .......... 483
S. Leela, *Stability of measure differential equations* ...................................................... 489
M. H. Lim, *Linear transformations on symmetric spaces* ........................................ 499
Teng-Sun Liu, Arnoud C. M. van Rooij and Ju-Kwei Wang, *On some group algebra modules related to Wiener’s algebra $M_1$* ....................... 507
Dale Wayne Myers, *The back-and-forth isomorphism construction* ................... 521
Donovan Harold Van Osdol, *Extensions of sheaves of commutative algebras by nontrivial kernels* ............................................................... 531
Alan Rahilly, *Generalized Hall planes of even order* .................................................. 543
Joylyn Newberry Reed, *On completeness and semicompleteness of first countable spaces* ......................................................................................... 553
Alan Schwartz, *Generalized convolutions and positive definite functions associated with general orthogonal series* ........................................ 565
Thomas Jerome Scott, *Monotonic permutations of chains* ........................................ 583
Eivind Stensholt, *An application of Steinberg’s construction of twisted groups* .... 595
Yasuji Takeuchi, *On strongly radical extensions* ....................................................... 619
William P. Ziener, *Some remarks on harmonic measure in space* ....................... 629
John Grant, *Corrections to: “Automorphisms definable by formulas”* ............... 639
Peter Michael Rosenthal, *Corrections to: “On an inversion for the general Mehler-Fock transform pair”* ....................................................... 640
Carl Clifton Faith, *Corrections to: “When are proper cyclics injective”* ............ 640