PACIFIC JOURNAL OF MATHEMATICS
Vol. 55, No. 2, 1974

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: Spec $(C) \rightarrow$ Spec (A) induced by the inclusion map: $A \rightarrow C$ 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[1] if C is finitely generated projective as an A-module and the Kernel of the multiplication map: $C \otimes_A C \rightarrow C$ 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 qth order derivation D on C and any $a \in C$, $[D, a]$ 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 $\mathscr{H}$ be any nonempty set of higher order derivations on C with $[D, a] \in \mathscr{H}$ for all $D \in \mathscr{H}$, all $a \in C$. In this case, the set $\{a \in C \mid D(a) = 0$ for all $D \in \mathscr{H}\}$ forms a subring of C, denoted by Ker $(\mathscr{H})$. If C has no nontrivial $\mathscr{H}$-stable ideal, C will be called an $\mathscr{H}$-simple ring. For an $\mathscr{H}$-simple ring C, let A denote Ker $(\mathscr{H})$. 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)].

(2) 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 $\mathscr{H}$ any nonempty set of higher order derivations on C with $[D, a] \in \mathscr{H}$ for all $D \in \mathscr{H}$, all $a \in C$. Suppose that the orders of the derivations in $\mathscr{H}$ are bounded and C is $\mathscr{H}$-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* $\mathrm{Ker}(\mathscr{H})$.

Proof. Let q be the supremum of orders of the derivations in $\mathscr{H}$. For any $x \in C$, we have $D(x^{p^e}) = 0$ for $D \in \mathscr{H}$ where $p^e > q$, and so x^{pe} belongs to $\mathrm{Ker}(\mathscr{H})$ [c.f., 5, Chap. I, Prop. 10]. Since $\mathrm{Ker}(\mathscr{H})$ is a field, we obtain $x^{pe} = 0$ 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 $\{x^{pi} \mid x \in S\}$ for a subset S of C. Let s be the minimal positive integer with $E^S(C) \subseteqq \mathrm{Ker}(\mathscr{H})$. Then $E^S(C)$ is a field. We shall show $E^i(C) = F_i + E^i(Q)$ for $i = 0, 1, \cdots, s$ where F_i are a subfield of $E^i(C)$, respectively. Assume we have already proved this fact for $i = r + 1, \cdots, s$. Let F_r be a maximal field contained in $E^r(C)$ with $F_{r+1} \subseteqq F_r$. 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 $E^{r+1}(Q) = E^1(E^r(Q))$, we obtain $(x - y_0)^p = a$ for $y_0 \in E^r(Q)$. Then $x - y_0$ 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 π 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 $\mathrm{Ker}(\mathscr{H})$, take a maximal subfield F of $F_0 \mathrm{Ker}(\mathscr{H})$ containing $\mathrm{Ker}(\mathscr{H})$. 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 $x^{pt} \in F$. Then a polynomial $X^{pt} - x^{pt}$ in $F[X]$ is irreducible. Hence $F[x]$ is isomorphic to a residue field $F[X]/(X^{pt} - x^{pt})$, 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 $J_{C/A}$ denote the Kernel of the multiplication map $\mu\colon C \otimes C \to C$.

DEFINITION. Let A and C be as above. Suppose the integral domain $A/\mathfrak{p}$ is of prime characteristic for each $\mathfrak{p} \in \mathrm{Spec}(A)$. 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 qth order A-derivations on C is denoted by $Der_q(C/A)$. We shall set $Der(C/A) = \bigcup_{q=1}^{\infty} Der_q(C/A)$. Then there are C-module isomorphisms $\varphi_q\colon \mathrm{Hom}_C(\Omega_A^{(q)}(C)$[2], $C) \to Der_q(C/A)$ by $\varphi_q(f) = f \cdot \delta^{(q)}$ and $\varphi\colon \mathrm{Hom}_C(J_{C/A}, C) \to Der(C/A)$ by $\varphi(f) = f \cdot \delta$ where δ is an A-module map: $C \to J_{C/A}$ by $\delta(c) = 1 \otimes e - c \otimes 1$ for $c \in C$ and $\delta^{(q)}$ is an A-module map: $C \to \Omega_A^{(q)}(C)$ by $\delta^{(q)}(c) = \{$the class of $\delta(c)$ modulo $(J_{C/A})^{q+1}\}$. The map $\delta^{(q)}$ is called the canonical qth order derivation of C/A.

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

PROPOSITION 2. *Let A be a commutative ring such that the domain $A/\mathfrak{p}$ is of prime characteristic for each $\mathfrak{p} \in \mathrm{Spec}(A)$. 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 $\mathscr{D}(C/A) = \mathrm{Hom}_A(C, C)$.*

Proof. The necessity is obvious. Suppose $\mathscr{D}(C/A) = \mathrm{Hom}_A(C, C)$. Then the C-module $Der(C/A)$ is generated by finitely many derivations, because it is a C-module direct summand of the finitely generated C-module $\mathrm{Hom}_A(C, C)$. So $\mathscr{D}_q(C/A) = \mathrm{Hom}_A(C, C)$ 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: $J_{C/A} \to \Omega_A^{(q)}(C)$ is injective, accordingly so is the canonical epimorphism: $J_{C_\mathfrak{p}/A_\mathfrak{P}} \to \Omega_{A_\mathfrak{p}}^{(q)}(C_\mathfrak{p})$ for each $\mathfrak{p} \in \mathrm{Spec}(A)$. This is obvious from the following lemma, because $\{1 \otimes u_i - u_i \otimes 1 \mid i = 1, 2, \cdots, m\}$ form a $C_\mathfrak{p}$-module basis for $J_{C_\mathfrak{p}/A_\mathfrak{P}}$ where $\{1, u_1, u_2, \cdots, u_m\}$ is an $A_\mathfrak{p}$-module basis for $C_\mathfrak{p}$.

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 $\{1, u_1, u_2, \cdots, u_m\}$. If $\mathscr{D}_q(C/A) = \mathrm{Hom}_A(C, C)$ for some positive integer q, then $\Omega_A^{(q)}(C)$ is a free C-module with a basis $\{\delta^{(q)}(u_1), \delta^{(q)}(u_2), \cdots, \delta^{(q)}(u_m)\}$ where $\delta^{(q)}$ is the canonical qth order derivation of C/A.*

Proof. From the hypothesis, we have a C-module isomorphism $\psi\colon C \oplus \mathrm{Hom}_C(\Omega_A^{(q)}(C), C) \to \mathrm{Hom}_A(C, C)$ by $\psi(c + f) = cx + (f \cdot \delta^{(q)})(x)$

[2] $\Omega_A^{(q)}(C)$ denotes the module of qth order differentials $J_{C/A}/(J_{C/A})^{q+1}$ [c.f., 5].

for $c, x \in C$, $f \in \mathrm{Hom}_C(\Omega_A^{(q)}(C), C)$. Let $D_i(i = 1, 2, \cdots, m)$ be elements of $\mathrm{Hom}_A(C, C)$ such that $D_i(1) = 0$ for all i and $D_i(u_j) = \delta_{i,j}$ for $i, j = 1, 2, \cdots, m$. Moreover, let f_i be elements of $\mathrm{Hom}_C(\Omega_A^{(q)}(C), C)$ with $\psi(f_i) = D_i$. Then we have $f_i(\delta^{(q)}(u_j)) = \delta_{i,j}$. Since the set $\{\delta^{(q)}(u_1), \delta^{(q)}(u_2), \cdots, \delta^{(q)}(u_m)\}$ forms a set of generators of $\Omega_A^{(q)}(C)$ as a C-module, $\Omega_A^{(q)}(C)$ is a free C-module with $\{\delta^{(q)}(u_1), \delta^{(q)}(u_2), \cdots, \delta^{(q)}(u_m)\}$ 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 $\mathscr{D}_q(C/A) = \mathrm{Hom}_A(C, C)$ for some positive integer q. Since $A = \mathrm{Ker}\,(Der_q(C/A))$, it follows from [5, Chap. I, Prop. 10] that $E^e(C)$ 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 $A/\mathfrak{p}$ is of prime characteristic for each $\mathfrak{p} \in \mathrm{Spec}\,(A)$. Then, for a strongly radicial extension C of A, the followings hold:*

(1) *The map ${}^a i$: $\mathrm{Spec}\,(C) \longrightarrow \mathrm{Spec}\,(A)$ induced canonically by the inclusion map $i: A \longrightarrow C$ is bijective.*

(2) *For each prime ideal $\mathfrak{p}$ in A we have $C \otimes A(\mathfrak{p})$*[3] *$= F_\mathfrak{p} + Q_\mathfrak{p}$ where $F_\mathfrak{p}$ is a subfield of $C \otimes A(\mathfrak{p})$ being purely inseparable over $A(\mathfrak{p})$ and $Q_\mathfrak{p}$ is a nilpotent maximal ideal in $C \otimes A(\mathfrak{p})$.*

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

[3] $A(\mathfrak{p})$ usually denotes the residue field $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$.

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 σ be any A-automorphism of C. For any prime ideal $\mathfrak{P}$ of C, we have $\sigma(\mathfrak{P}) = \mathfrak{P}$, because ${}^a i(\sigma(\mathfrak{P})) = {}^a i(\mathfrak{P})$ where ${}^a i$ is as above. So σ 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 $A/\mathfrak{p}$ is of prime characteristic for each prime ideal $\mathfrak{p}$ 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 $C_\mathfrak{p}$ is a strongly radicial extension of $A_\mathfrak{p}$ for each $\mathfrak{p} \in \operatorname{Spec}(A)$.*

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: $C \oplus Der(C/A) \to \operatorname{Hom}_A(C, C)$ is an epimorphism, accordingly so is the canonical injection: $C_\mathfrak{p} \oplus Der(C/A)_\mathfrak{p} \to \operatorname{Hom}_A(C, C)_\mathfrak{p}$ for each $\mathfrak{p} \in \operatorname{Spec}(A)$. Let φ be the composition of the following canonical maps

$$C_\mathfrak{p} \oplus Der(C/A)_\mathfrak{p} \to \operatorname{Hom}_A(C, C)_\mathfrak{p} \to \operatorname{Hom}_{A_\mathfrak{p}}(C_\mathfrak{p}, C_\mathfrak{p}) \to C_\mathfrak{p} \oplus Der(C_\mathfrak{p}/A_\mathfrak{p}) .$$

Then we have $\varphi(Der(C/A)_\mathfrak{p}) \subseteqq Der(C_\mathfrak{p}/A_\mathfrak{p})$. We shall show φ maps $Der(C/A)_\mathfrak{p}$ onto $Der(C_\mathfrak{p}/A_\mathfrak{p})$. By the above isomorphisms any element $D_\mathfrak{p}$ of $Der(C_\mathfrak{p}/A_\mathfrak{p})$ can be identified with an element of form $(1/s)D$ in $\operatorname{Hom}_A(C, C)_\mathfrak{p}$ for $s \in A - \mathfrak{p}$, $D \in \operatorname{Hom}_A(C, C)$. If $D_\mathfrak{p}$ is of order q, we have finitely many equalities in $C_\mathfrak{p}$

$$\frac{1}{s}D(x_0x_1 \cdots x_q) = \sum_{k=1}^{q} (-1)^{k-1} \sum_{i_1<i_2<\cdots<i_k} x_{i_1}x_{i_2} \cdots x_{i_k}\left(\frac{1}{s}\right)D(x_0 \cdots \hat{x}_{i_1} \cdots \hat{x}_{i_k} \cdots x_q) ,$$

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 $A - \mathfrak{p}$ such that tD is a qth order A-derivation on C. Hence we have $(1/s)D = (1/st)\cdot tD \in Der(C/A)_\mathfrak{p}$ and $\varphi((1/s)D) = D_\mathfrak{p}$.

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 $0 \to (C \otimes C)J_{B/A} \to J_{C/A} \to J_{C/B} \to 0$. 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 $\mathfrak{p} \in \operatorname{Spec}(A)$, $A_\mathfrak{p}$ is artinian and $A(\mathfrak{p})$ 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 $\mathfrak{p} \in \operatorname{Spec}(A)$, we have $C \otimes A(\mathfrak{p}) = F_\mathfrak{p} + Q_\mathfrak{p}$ where $Q_\mathfrak{p}$ is the nil-radical of $C \otimes A(\mathfrak{p})$ and $F_\mathfrak{p}$ is a subfield of $C \otimes A(\mathfrak{p})$ which is purely inseparable over $A(\mathfrak{p})$.*

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

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & & J_{C/A} \arrow[r, dash] \arrow[d] & J_{C(\mathfrak{m})/A(\mathfrak{m})} \arrow[d] & \\
0 \arrow[r] & C \otimes C \otimes \mathfrak{m} \arrow[r] \arrow[d, "\mu \otimes 1"] & C \otimes C \arrow[r] \arrow[d, "\mu"] & C(\mathfrak{m}) \otimes C(\mathfrak{m}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & C \otimes \mathfrak{m} \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & C(\mathfrak{m}) \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

whose all the vertical and horizontal sequence are exact where μ is the multiplication map: $C \otimes C \to C$ and the other maps are also canonical. From this diagram, we obtain an exact sequence $0 \to \operatorname{Ker}(\mu \otimes 1) \to J_{C/A} \to J_{C(\mathfrak{m})/A(\mathfrak{m})}$. Since $\operatorname{Ker}(\mu \otimes 1) = J_{C/A} \otimes \mathfrak{m}$, $\operatorname{Ker}(\mu \otimes 1)$ 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 Δ be the set of C-module direct summands $\mathscr{E}$*

of Der(C/A) with $DD' \in \mathscr{E}$ and $[D, x] \in \mathscr{E}$ for all $D, D' \in \mathscr{E}$ and all $x \in C$. Let Γ be the set of intermediate rings between A and C, over which C is projective. Then correspondences $\delta\colon \Delta \to \Gamma$, $\gamma\colon \Gamma \to \Delta$ given respectively by $\delta(\mathscr{E}) = \mathrm{Ker}\,(\mathscr{E})$, $\gamma(B) = Der(C/B)$ 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 $Der(C/B)$ is a C-module direct summand of $Der(C/A)$.*

Proof. In order to show the first statement, it suffices to observe $\mathrm{Hom}_B(C, C)$ is contained in $\mathscr{D}(C/B)$. For any $f \in \mathrm{Hom}_B(C, C)$, we have $f = c + D$ for $c \in C$, $D \in Der(C/A)$. 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 $Der(C/B)$. 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 $\mathfrak{p} \in \mathrm{Spec}\,(A)$, a sequence of canonical $C_\mathfrak{p}$-module homomorphisms

$$0 \longrightarrow (C_\mathfrak{p} \otimes_{A_\mathfrak{p}} C_\mathfrak{p})J_{B_\mathfrak{p}/A_\mathfrak{p}} \longrightarrow J_{C_\mathfrak{p}/A_\mathfrak{p}} \longrightarrow J_{C_\mathfrak{p}/B_\mathfrak{p}} \longrightarrow 0$$

is exact, because both $B_\mathfrak{p}$ and $C_\mathfrak{p}$ are $A_\mathfrak{p}$-free. Hence a sequence of canonical C-module homomorphisms

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

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

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

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

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

Proof. In this case C is local by Theorem 4. Let $\mathfrak{m}$ be the maximal ideal in A and Q the maximal ideal in C. Put $\bar{A} = A/\mathfrak{m}$

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

Now we can prove Theorem 7.

Proof of Theorem 7. It follows from Lemma 8 that γ is well-defined. We have to show δ is well-defined. For any $\mathscr{E} \in \Delta$, put $B = \mathrm{Ker}\,(\mathscr{E})$. In the case of any local ring A, we shall first observe C is free over B. From the above lemma there are elements $c_1, c_2, \cdots, c_r$ in C and a C-module basis $D_1, D_2, \cdots, D_r$ for $\mathscr{E}$ with $D_i(c_j) = \delta_{i,j}$ $(i, j = 1, 2, \cdots, r)$. Then we have $D_iD_j = 0$ for $i, j, = 1, 2, \cdots, r$. In fact, we can write $D_iD_j = x_1D_1 + \cdots + x_rD_r$ for $x_i \in C$. Then we have $x_k = (\sum_{i=1}^r x_iD_i)(c_k) = D_iD_j(c_k) = 0$ for $k = 1, 2, \cdots, r$ and so $D_iD_j = 0$. Since $D(bx) = bD(x) + xD(b) + [D, x](b)$ for any $D \in \mathscr{E}$, any $b \in B$, any $x \in C$, any element of $\mathscr{E}$ 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 C not belonging to C_1. Suppose inductively that we have already found an element u_i in C not belonging to C_1 with $D_k(u_i) = 0$ for all $k \leqq i$. 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_1 and we have $D_k(u_{i+1}) = 0$ for all $k \leqq i+1$, because $D_iD_j = 0$ for $i, j = 1, 2, \cdots, r$. Repeating this construction, we can obtain an element u_r in C with $u_r \notin C_1$ and $D_i(u_r) = 0$ for $i = 1, 2, \cdots, r$. Then u_r belongs to B, which is absurd. Hence we have $C = C_1$ and so C is a free B-module when A is local. In the case of any general ring A, $\mathscr{E}_{\mathfrak{p}}$ is a $C_{\mathfrak{p}}$-module direct summand of $Der(C_{\mathfrak{p}}/A_{\mathfrak{p}})$ for each $\mathfrak{p} \in \mathrm{Spec}\,(A)$. Moreover, we have $B_{\mathfrak{p}} = \mathrm{Ker}\,(\mathscr{E}_{\mathfrak{p}})$. So, from the result above, $C_{\mathfrak{p}}$ is a free $B_{\mathfrak{p}}$-module of rank equal to $\mathrm{rank}_{C_{\mathfrak{p}}}(\mathscr{E}_{\mathfrak{p}}) + 1$. Since $\mathscr{E}$ is a finitely generated projective C-module, the map of $\mathrm{Spec}\,(A)$ into the domain of rational integers by $\mathfrak{p} \mapsto \mathrm{rank}_{C_{\mathfrak{p}}}(\mathscr{E}_{\mathfrak{p}}) + 1$ is locally constant [2, Chap. II, § 5, No 2, Theorem 1]. On the other hand, by Theorem 4, we have $\mathrm{Spec}\,(C) \cong \mathrm{Spec}\,(B) \cong \mathrm{Spec}\,(A)$ as the topological spaces and $\mathrm{rank}_{C_{\mathfrak{P}}}(\mathscr{E}_{\mathfrak{P}}) + 1 = \mathrm{rank}_{C_{\mathfrak{p}}}(\mathscr{E}_{\mathfrak{p}}) + 1$ for any $\mathfrak{P} \in \mathrm{Spec}\,(B)$, $\mathfrak{p} = \mathfrak{P} \cap A$. By [2, ibid], C is projective over B

and so δ is well-defined. Hence we have $Der(C_{\mathfrak{p}}/B_{\mathfrak{p}}) \cong \mathrm{Hom}_{C_{\mathfrak{p}}}(J_{C_{\mathfrak{p}}}/B_{\mathfrak{p}}, C_{\mathfrak{p}})$ for each $\mathfrak{p} \in \mathrm{Spec}(A)$. This shows $Der(C_{\mathfrak{p}}/B_{\mathfrak{p}})$ is generated by such a C-module basis $D_1, D_2, \cdots, D_r$ for $\mathscr{E}_{\mathfrak{p}}$ as the above augument. So we obtain $\mathscr{E}_{\mathfrak{p}} = Der(C_{\mathfrak{p}}/B_{\mathfrak{p}})$ for each $\mathfrak{p} \in \mathrm{Spec}(A)$ and so $\mathscr{E} = Der(C/B)$. This shows $\gamma\cdot\delta$ is the identity map on Λ. It is obvious that $\delta\cdot\gamma$ is the identity map on Γ. This completes the proof.

References

1. N. Bourbaki, *Algèbre*, Chap. II, 3^e ed., Actualités Sci. Indust., No. 1261, Hermann, Paris, 1958.

2. ————, *Algèbre commutative*, Chap. I, II, Actualités Sci. Indust., No. 1290, Hermann, Paris, 1961.

3. A. Hattori, *On high order derivations from the view-point of two sided modules*, Sci. Pap. Coll. Gen Ed. Univ. of Tokyo, **20** (1970), 1-11.

4. M. Nagata, *Local Rings*, Interscience Publishers, New York, 1962.

5. Y. Nakai, *High order derivations I*, Osaka J. Math., **7** (1970), 1-27.

6. Y. Nakai, K. Kosaki, and Y. Ishibashi, *High order derivations II*, J. Sci. Hiroshima Univ., Ser. A-1, **34** (1970), 17-27.

7. H. Osborn, *Modules of differentials I*, Math. Annalen, **170** (1967), 221-244.

8. Y. Takeuchi, *On quasi-Galois extensions of a commutative ring*, Revista de Union Mate. Argentina, **24** (1969), 167-175.

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

10. S. Yuan, *Differentiably simple rings of prime characteristic*, Duke Math. J., **31** (1964), 625-630.

11. ————, *Inseparable Galois theory of exponent one*, Trans. Amer. Math. Soc., **149** (1970), 163-170.

12. ————, *Finite dimensional inseparable algebras*, Trans. Amer. Math. Soc., **150** (1970), 577-587.

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

Kobe University