Takeuchi, Y.
Osaka J. Math.
12 (1975), 23-31

ON GALOIS OBJECTS WHICH ARE STRONGLY RADICIAL OVER ITS BASIC RING

Dedicated to Professor M. Takahashi on his 60 th birthday

YASUJI TAKEUCHI

(Received March 7, 1974)

In [3], Chase and Sweedler introduced a notion of Galois object and extended, in this case, the fundamental theorem of Galois theory for fields. Furthermore, they showed that it contains, as a special case, the fundamental theorem of Galois theory on separable algebras developed by Chase, Harrison and Rosenberg. However they mentioned in [3] that they had, in general, no good characterization of the subalgebras which arised in the Galois correspondence. A purpose of this paper is to show what those subalgebras are in the case of strongly radicial extensions. On the other hand, it is well-known that for a finite purely inseparable extension K of a field k, there exists a chain of subfields of K: $K=K_0\supset K_1\supset K_2\supset\cdots\supset K_r=k$ such that K_i is of exponent one over K_{i+1} for $i=0, 1, 2, \cdots, r-1$. We shall study this analogy in the case of Galois objects over a field which are strongly radicial over their basic field.

Let H be a finite cocommutative split[1] Hopf algebra over a commutative ring A and C a Galois H^*[2]-object over A which is strongly radicial over A.

In our first section, we shall study a coalgebra structure of H. Moreover we shall show that there exists a bijection between the set of admissible[3] Hopf subalgebras of H and the set of distinguished[4] intermediate rings between A and C.

In our second section, we shall exhibit an existence of a sequence of subrings of C

$$C=C_0\supset C_1\supset\cdots\supset C_i\supset\cdots\supset C_n=A$$

satisfying the followings for each $i=0, 1, \cdots, n-1$:

(1) $C\#K_i\cong Hom_{C_i}(C, C)$ via a canonical map where K_i is a Hopf subalgebra of H.

(2) $d(C_i)\subseteq C_i$ for $d\in H$.

(3) $C_i[\mathcal{D}er_1(C_i/C_{i+1})]=Hom_{C_{i+1}}(C_i, C_i)$ for $i=0, 1, \cdots, n-1$.

1) For the definition, see §1.
2) H^* denotes a dual Hopf algebra of H.
3) For the definition, see [3, Def. 7.1].
4) For the definition, see a following part of the proof of Proposition 3 below.

(4) C_i is finitely generated projective as a C_{i+1}-module.

Throughout the following discussion, all rings are commutative with an identity, and all homomorphisms 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 a common identity. In this paper, A will denote a commutative ring such that $A/\mathfrak{p}$ is of characteristic non-zero for each $\mathfrak{p}\in Spec(A)$. We will use the definitions and terminology in [6] with respect to coalgebras and Hopf algebras, and in [4] and [7] with respect to high order derivations and strongly radicial extensions, respectively. The author likes to express his thanks to the referee for comments on Proposition 4.

1. Galois correspondence theorem

Let C be a commutative algebra over a ring A. Let H be a finite[5] commutative Hopf-algebra over A. Then C is called a *Galois H-object* if C is a finitely generated and faithfull projective A-module and there is a map $\alpha : H^*\otimes C\to C$ which measures C to C such that a map $\varphi : C\# H^*\to Hom_A(C, C)$ by $\varphi(x\# u)(y)=x\alpha(u\otimes y)$ is an algebra-isomorphism (c.f. 3].

Let (H, Δ, ε) be a coalgebra over a commutative ring A where Δ is its diagonal map and ε is its augmentation map. For $g\in H$, g is called a *grouplike element* in H if $\Delta(g)=g\otimes g$ and $\varepsilon(g)=1$. Let $\mathcal{G}(H)$ be denoted the set of grouplike elements in H. H is called a *split coalgebra* in case $H=\bigoplus_{g\in\mathcal{G}(H)} U_g$ as A-modules where each U_g is a subcoalgebra of H in which g is an only grouplike element and $U_g=Ag+(U_g\cap Ker\ \varepsilon)$.

Lemma 1. *Let C be a strongly radicial extension of a ring A. Then so is $C\otimes C$*

Proof. It is obvious from the definition

Lemma 2. *Let H be a finite commutative Hopf-algebra over a local ring A such that there is a Galois H-object C over A which is strongly radicial over A. Then H is a local ring.*

Proof. From Lemma 1, $C\otimes C$ is a strongly radicial extension of a local ring A and so is local [c.f., 7, Theorem 5]. On the other hand, we have $C\otimes C\simeq C\otimes H$ as algebras [c.f., 3, Theorem 9.3]. So H is local.

Proposition 3. *Let H be a finite commutative Hopf algebra over a commutative ring A, whose dual coalgebra H^* is split. Let C be a Galois H-object over A. If C is strongly radicial over A, then $H^*=A\,1\oplus Ker(\varepsilon_*)$ as A-module where ε_* is an augmentation map of H^*.*

---

5) For the definition, see [3, Def. 7.1].

Proof. Since H^* is split, H^* has a decomposition $H^*=U_1\oplus(\bigoplus_{g(\neq 1)\in \mathcal{G}(H)} U_g)$ where each U_g is a subcoalgebra of H^* in which g is an only grouplike element. We need to show that U_g vanishes if $g\neq 1$. Put $\bar{A}=A(\mathfrak{p})$[6], $\bar{C}=\bar{A}\otimes C$ and $\bar{H}=\bar{A}\otimes H$ for $\mathfrak{p}\in Spec(A)$. Then $\bar{C}$ is a Galois $\bar{H}$-object. Since $\bar{C}$ is strongly radicial over $\bar{A}$. $\bar{H}$ is local. So $(\bar{H})^*$ is irreducible. Then we have $\bar{A}\otimes U_g=0$ for any $\mathfrak{p}\in Spec(A)$ and so $U_g=0$.

For a coalgebra H, let H^+ denote $Ker(\varepsilon)$ where ε is an augmentation map of H. Moreover, assume H is a finite cocommutative split Hopf algebra over a ring A and C a Galois H^*-object over A which is strongly radicial over A. Then H may be considered to be a subalgebra of $Hom_A(C, C)$. For an intermediate ring B between A and C over which C is projective, $\mathfrak{Der}(C/B)$ is a C-module direct summand of $\mathfrak{Der}(C/A)$ [7, Prop. 12]. Now we shall say such intermediate ring B is distinguished if there is a C-module direct summand M of $\mathfrak{Der}(C/A)$ with $\mathfrak{Der}(C/A)=\mathfrak{Der}(C/B)\oplus M$ satisfying $C\otimes Proj_M(H^+)=C.Proj_M(H^+)$ for the projection $Proj_M$: $\mathfrak{Der}(C/A)\to M$. In this case, $Proj_M(H^+)$ is A-projective, because $C.Proj_M(H^+)(=M)$ is C-projective and A is a direct summand of C.

Proposition 4. *Let A, C, H be as above. Let B be a distinguished intermediate ring between A and C. Then there exists a subbialgebra U of H such that U is an A-module direct summand of H and $C\otimes U\cong Hom_B(C, C)$ via a canonical map.*

Proof. Set $K_0=Proj_M(H^+)$ for a projection above $Proj_M$. Then we have a split exact sequence of A-module $0\to U^+\to H^+\to K_0\to 0$ where $U^+=Ker(Proj_M|H^+)$ and the third arrow denotes $Proj_M$. So, $H^+=U^+\oplus K$ where K is an A-submodule of H^+ which is isomorphic to K_0. Now we shall show that $C\otimes U^+$ can be identified with $\mathfrak{Der}(C/B)$. Since U^+ is obviously contained in $\mathfrak{Der}(C/B)$, $C\otimes U^+$ may be regarded to be contained in $\mathfrak{Der}(C/B)$. For any $\mathfrak{p}\in Spec(A)$, put $\bar{A}=A(\mathfrak{p})$ and $\bar{C}=\bar{A}\otimes C$. Then we have $dim_{\bar{A}}[\bar{C}\otimes U^+]=dim_{\bar{A}}[\bar{C}\otimes H^+]-dim_{\bar{A}}[\bar{C}\otimes K]=dim_{\bar{A}}[\bar{A}\otimes\mathfrak{Der}(C/A)]-dim_{\bar{A}}[\bar{A}\otimes M]=dim_{\bar{A}}[\bar{A}\otimes\mathfrak{Der}(C/B)]$, because $\bar{C}\otimes K\cong\bar{C}\otimes K_0\cong\bar{A}\otimes M$. So $C\otimes U^+=\mathfrak{Der}(C/B)$, using Nakayama's lemma. Put $U=A1+U^+$. Then we shall show that $\Delta(d)$ belongs to $U\otimes U$ for $d\in U^+$. We can assume, without loss of generality, that A is local. Let $\{u_1, u_2, \cdots, u_n\}$ and $\{v_1, v_2, \cdots, v_m\}$ be A-module bases for U^+, K, respectively. Since $H^+\otimes H^+=U^+\otimes U^++U^+\otimes K+K\otimes U^++K\otimes K$, we have $\Delta(d)-1\otimes d-d\otimes 1=X+\sum a_{i,j}u_i\otimes v_j+\sum b_{i,j}v_i\otimes u_j+\sum c_{i,j}v_i\otimes v_j$ for $X\in U^+\otimes U^+$, $a_{i,j}$, $b_{i,j}$, $c_{i,j}\in A$. Since $[D, x]$[7] belongs to $\mathfrak{Der}(C/B)\subset Hom_B(C, C)$ for $D\in\mathfrak{Der}(C/B)$, $x\in C$, we obtain $\mu(X(x\otimes by))+\sum a_{i,j}u_j(x)v_j(by)+\sum b_{i,j}v_j(x)u_j(by)+\sum c_{i,j}v_i(x)v_j(by)=b\mu(X(x\otimes y))+b\sum a_{i,j}u_i(x)v_j(y)+b\sum b_{i,j}v_i(x)u_j(y)+b\sum c_{i,j}v_i(x)v_j(y)$ for x,

6) $A(\mathfrak{p})$ denotes the residue field $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$.

7) C.f., 4, chap. 1, §1.

$y \in C$, $b \in B$ where μ is a contraction map : $C \otimes C \to C$. Using the fact that any element of U^+ commutes with each element of B, we have $\sum a_{i,j}(v_j(by) - bv_j(y))u_i - \sum c_{i,j}(v_j(by) - bv_j(y))v_i = 0$ and so $\sum_j a_{i,j}(v_j(by) - bv_j(y)) = 0$, $\sum_j c_{i,j}(v_j(by) - bv_j(y)) = 0$. Hence $\sum_j a_{i,j}v_j$ and $\sum_j c_{i,j}v_j$ belong to $\mathcal{D}er(C/B) \cap K (=0)$, showing $a_{i,j} = 0$ and $c_{i,j} = 0$ for all i, j. Moreover, we have $b_{i,j} = 0$, because H is cocommutative. This shows that U is a subcoalgebra of H. Since U is obviously a subalgebra of H, U is a subbialgebra of H. This completes the proof.

REMARK.[8] Let A, C, H be as above. Let B be an intermediate ring between A and C, over which C is projective. Then B is distinguished if and only if $C.(H^+ \cap \mathcal{D}er(C/B)) = \mathcal{D}er(C/B)$.

Proof. The "only if" part follows from the proof of Proposition 4. Since C is B-projective, we can write $\mathcal{D}er(C/A) = \mathcal{D}er(C/B) \oplus M$ for a submodule M of $\mathcal{D}er(C/A)$. Now, $C.(H^+ \cap \mathcal{D}er(C/B)) = \mathcal{D}er(C/B)$. Then we may regard $C \otimes (H^+ \cap \mathcal{D}er(C/B)) = \mathcal{D}er(C/B)$, by identification $C \otimes H^+ = \mathcal{D}er(C/A)$. So we have a canonical isomorphism : $C \otimes Proj_M(H^+) \xrightarrow{\sim} M$. This shows the "if" part.

Theorem 5. *Let H be a cocommutative split Hopf algebra over a commutative ring A. Let C be a Galois H^*-object over A which is strongly radicial over A. Then there exists a bijection between the set $\mathcal{F}$ of subbialgebras of H which are A-module direct summands of H and the set $\mathcal{G}$ of distinguished intermediate rings between A and C. Its correspondence is given by associating $U \in \mathcal{F}$ with $Ker(U^+) = \{x \in C \mid d(x) = 0$ for $d \in U^+\}$.*

Proof. For $B \in \mathcal{G}$, take U as the proposition above. Then U belongs to $\mathcal{F}$. Moreover, it is obvious that $U^+ = \{d \in H \mid d(bx) = bd(x)$ for $x \in C$, $b \in B\}$. Conversely, put $B = Ker(U^+)$ for $U \in \mathcal{F}$. Then we have $B = Ker(C \otimes U^+)$ and so $C \otimes U^+ = \mathcal{D}er(C/B)$ [c.f., 7, Theorem 15]. Hence B belongs to $\mathcal{G}$, because U^+ is an A-module direct summand of H^+. So, using again [7, Theorem 15], a correspondence : $U \to Ker(U^+)$ gives a bijection between $\mathcal{F}$ and $\mathcal{G}$.

2. Galois objects over a field which are strongly radicial over their basic field

Throughout the following discussion, we shall assume that H is a cocommutative pointed[9] Hopf algebra over a field A of characteristic $p \neq 0$ and C is a strongly radicial extension of A which is a Galois H^*-object over A. In this case, both H and $C \# H$ may be regarded to be contained in $Hom_A(C, C)$. Since H measures C to C, we have $d(1) = \varepsilon(d)1$ for $d \in H$ where ε is an augmentation map for H and 1 denotes an identity in C. So $d(1) = 0$ for $d \in H^+ = Ker(\varepsilon)$.

8) This remark was advised by the referee.
9) For the definition, see [6].

This shows $C\otimes H^{+}=\mathcal{D}er(C/A)$, because $C\# H=\mathcal{D}(C/A)$. Hence we obtain $Hom_C(\mathcal{D}er(C/A), C)\cong Hom_C(C\otimes H^{+}, C)\cong C\otimes Hom_A(H^{+}, A)\cong C\otimes (H^{+})^{*}$ and so $C\otimes(H^{+})^{*}\cong J_{C/A}$ as left C-modules where $J_{C/A}$ is a kernel of a contraction map: $C\otimes C\to C$.

Lemma 6. *$J_{C/A}\cong C\otimes(H^{+})^{*}$ as rings.*

Proof. $Hom_C(C\otimes H^{+}, C)$ forms a ring by a multiplication $F*G$: $1\otimes d\to \sum_{(d)'} F(1\otimes d_{(1)})G(1\otimes d_{(2)})$ for $F, G\in Hom_C(C\otimes H^{+}, C)$ where $\sum_{(d)'} d_{(1)}\otimes d_{(2)}=\Delta(d)-1\otimes d-d\otimes 1$ for a diagonal map Δ of H. Then $Hom_C(C\otimes H^{+}, C)$ is isomorphic to $C\otimes(H^{+})^{*}$ as rings. Thus, in order to complete the proof, it suffices to show that $J_{C/A}\cong Hom_C(C\otimes H^{+}, C)$ as rings. A C-module map α: $J_{C/A}\to Hom_C(C\otimes H^{+}, C)$ by $\alpha(1\otimes x-x\otimes 1)\ (c\otimes d)=cd(x)$ for c, $x\in C$, $d\in H^{+}$ is an isomorphism. We shall show that α is a ring-homomorphism. Since $(1\otimes x-x\otimes 1)\ (1\otimes y-y\otimes 1)=1\otimes xy-xy\otimes 1-x(1\otimes y-y\otimes 1)-y(1\otimes x-x\otimes 1)$, we have $\alpha((1\otimes x-x\otimes 1)\ (1\otimes y-y\otimes 1))\ (1\otimes d)=d(xy)-xd(y)-d(x)y=\sum_{(d)'} d_{(1)}(x) d_{(2)}(y)$. On the other hand, we obtain $\{\alpha(1\otimes x-x\otimes 1)*\alpha(1\otimes y-y\otimes 1)\}\ (1\otimes d) =\sum_{(d)'}\alpha(1\otimes x-x\otimes 1)\ (1\otimes d_{(1)})\alpha(1\otimes y-y\otimes 1)\ (1\otimes d_{(2)})=\sum_{(d)'} d_{(1)}(x)d_{(2)}(y)$, showing our requirement.

Since H is irreducible as a coalgebra, $A1$ is a coradical of H. Let $P(H)$ denote $\{d\in H\mid \Delta(d)=1\otimes d+d\otimes 1\}$. Set $H_i=\wedge^{i+1}(A1)$[10] for $i=0, 1, 2, \cdots$. Then the set $\{H_i\}_i$ gives a filtration for H satisfying the followings:

(1) $H=\bigcup_i H_i$.

(2) $H_0=A1$.

(3) $H_1^{+}=P(H)$.

(4) $\Delta(H_n)\subseteqq \sum_{i=0}^{n} H_i\otimes H_{n-i}$.

(5) $\lambda(H_i)\subseteqq H_i$ for $i=0, 1, 2, \cdots$ where λ is an antipode of H[c.f., 6, Chap. 9].

Lemma 7. *$\mathcal{D}er_i(C/A)\cong C\otimes H_i^{+}$ as left C-modules for $i=0, 1, 2, \cdots$.*

Proof. Since $(H^{+})^{*}=(H^{*})^{+}$, we have $J\cong C\otimes(H^{*})^{+}$ as rings where $J=J_{C/A}$, and so $J/J^{i+1}\cong C\otimes(H^{*})^{+}/((H^{*})^{+})^{i+1}$. Hence we obtain

$$\begin{aligned}\mathcal{D}er_i\,(C/A)&\cong Hom_C(J/J^{i+1}, C)\cong Hom_C(C\otimes(H^{*})^{+}/((H^{*})^{+})^{i+1}, C)\\ &\cong C\otimes Hom_A((H^{*})^{+}/((H^{*})^{+})^{i+1}, A)\,.\end{aligned}$$

On the other hand, we have $H_i=\wedge^{i+1}(A1)=[((A1)^{\perp})^{i+1}]^{\perp}=[((H^{*})^{+})^{i+1}]^{\perp}$. This completes the proof.

10) For the definition, see [6, §9].

Theorem 8. *Let $C_i = Ker(H_i^+)$ for $i=1, 2, 3, \cdots$. Then the followings hold*:

(1) *C is a strongly radicial extension of C_i.*

(2) $C_i = Ker(\mathcal{D}er_i(C/A))$.

(3) $C \# A[H_i] = Hom_{C_i}(C, C)$.

(4) $C_{i+1} = Ker(\mathcal{D}er_1(C_i/C_{i+1}))$.

Proof. By an identification $\mathcal{D}(C/A) = C \# H$, we have $\mathcal{D}er_i(C/A) = C \otimes H_i^+$ from Lemma 8 and so $C[\mathcal{D}er_i(C/A)] = C[C \otimes H_i^+] = C \# A[H_i^+]$. Since $\{C \# A[H_i^+]\}^+$ is a C-module direct summand of $C \# H^+$, $\{C[\mathcal{D}er_i(C/A)]\}^+$ is a C-module direct summand of $\mathcal{D}er(C/A)$ where X^+ denotes a set $\{d \in X \mid d(1)=0\}$ for a subset X of $Hom_A(C, C)$. Moreover, $\{C[\mathcal{D}er_i(C/A)]\}^+$ is closed by the the multiplication and the operator $[D, x]$ for $D \in \{C[\mathcal{D}er_i(C/A])\}^+$, $x \in C$. So (1) and (3) follow easily from [7, Theorem 15]. (2) is obvious. It remains only to show (4). It is trivial that C_{i+1} is contained in $Ker(\mathcal{D}er_1(C_i/C_{i+1}))$. Assume there is an element x in $Ker(\mathcal{D}er_1(C_i/C_{i+1}))$ with $x \notin C_{i+1}$. Then we have $d(x) \neq 0$ for some $d \in H_{i+1}^+$. Since C is a free C_i-module, there is a projection p: $C \to C_i$ with $(pd)(x) \neq 0$. Since d is an ordinary C_{i+1}-derivation: $C_i \to C$ [c.f. 4, Chap. I, §2, Prop. 7], pd can be regarded to belong to $\mathcal{D}er_1(C_i/C_{i+1})$, which is absurd.

Lemma 9. *Let $J = J_{C/A}$ under the same situation as above. Then J/J^2 is free over C.*

Proof. Since C admits a p-basis over C_1 from [8, Theorem 10], $J_{C/C_1}/(J_{C/C_1})^2$ is free over C. So it suffices to show that $J/J^2 \cong J_1/J_1^2$ as C-modules where $J_1 = J_{C/C_1}$. Now we have a C-split exact sequence of canonical maps

$$0 \to L \to J/J^2 \to J_1/J_1^2 \to 0$$

where $L = \{(C \otimes C)J_{C_1/A} + J^2\}/J^2$. We have to prove $L=0$. Since $Hom_C(J/J^2, C) \cong \mathcal{D}er_1(C/A) = \mathcal{D}er_1(C/C_1) \cong Hom_C(J_1/J_1^2, C)$, we obtain $Hom_C(L, C)=0$. This shows $L=0$. In fact, assume $L \neq 0$. Let us write $L/QL = (C/Q)\bar{v}_1 \oplus (C/Q)\bar{v}_2 \oplus \cdots \oplus (C/Q)\bar{v}_r (v_i \in L)$ for a unique maximal ideal Q in C. Then we have $L = Cv_1 + Cv_2 + \cdots + Cv_r$, because L is finitely generated as a C-module. Since $C = F \oplus Q$ as vector spaces over F where F is a subfield of C [c.f., 7], any element c in C can be written as $c^{(0)} + c^{(1)}$ for $c^{(0)} \in F$, $c^{(1)} \in Q$. Then $\{c_1^{(0)}, c_2^{(0)}, \cdots, c_r^{(0)}\}$ are uniquely determined for $c_1v_1 + c_2v_2 + \cdots + c_rv_r \in L$. For let $c_1v_1 + c_2v_2 + \cdots + c_rv_r = b_1v_1 + b_2v_2 + \cdots + b_rv_r$. Then we have $(c_1^{(0)} - b_1^{(0)})v_1 + \cdots + (c_r^{(0)} - b_r^{(0)})v_r \in QL$. Since $v_1, v_2, \cdots, v_r$ are free mod Q, we obtain $c_1^{(0)} = b_1^{(0)}$, $c_2^{(0)} = b_2^{(0)}$, $\cdots$, $c_r^{(0)} = b_r^{(0)}$. So we define a map φ: $L \to C$ by $\varphi(c_1v_1 + c_2v_2 + \cdots + c_rv_r) = (c_1^{(0)} + c_2^{(0)} + \cdots + c_r^{(0)})a$ where a ias a non-zero element in Q^{e-1} for a positive integer e with $Q^e = 0$ and $Q^{e-1} \neq 0$. Then φ is a non-zero element in $Hom_C(L, C)$, which is absurd.

Lemma 10. *Let $\{t_1, t_2, \cdots, t_n\}$ be a system of generators for an A-algebra C such that $\{\tilde{t}_1, \tilde{t}_2, \cdots, \tilde{t}_n\}$ forms a system of p-generators for $C\otimes C=C\otimes 1+J$ [c.f., 9] where $\tilde{t}_i=1\otimes t_i-t_i\otimes 1 (i=1, 2, \cdots, n)$. Then we have $C_1=A[(t_1)^p, (t_2)^p, \cdots, (t_n)^p]$.*

Proof. Since J/J^2 is free over $C\otimes 1$ and $C/Q\otimes_C J/J^2\cong J/(J+Q)J$ as C/Q-spaces where Q is a unique maximal ideal of C, the images of $\tilde{t}_1, \tilde{t}_2, \cdots, \tilde{t}_n$ by a canonical map: $J\to J/J^2$ form a $C\otimes 1$-module basis for J/J^2 [c.f., 2, Chap. II, §3, Prop. 5]. So there are $d_1, d_2, \cdots, d_n$ in $\mathcal{D}er_1(C/A)$ with $d_i(t_j)=\delta_{i,j}$ for $i, j=1, 2, \cdots, n$. Since $C=A[t_1, t_2, \cdots, t_n]$, any element x in C_1 can be written as $\sum_{(e)} a_{(e)}t_1^{e_1}t_2^{e_2}\cdots t_n^{e_n}$. Then let us write $x=\sum_{(e)} c_{(e)}t_{i_1}^{e_{i_1}}t_{i_2}^{e_{i_2}}\cdots t_{i_s}^{e_{i_s}}$ where $p>e_{i_k}(k=1, 2, \cdots, s)$ and $c_{(e)}=a_{(e)}t_{j_1}^{e_{j_1}}\cdots t_{j_t}^{e_{j_t}}$ with $p\mid e_{j_l} (l=1, 2, \cdots, t)$. Assume there is a term $c_{(e)}t_{i_1}^{e_{i_1}}\cdots t_{i_s}^{e_{i_s}}$ with $t_{i_1}^{e_{i_1}}\cdots t_{i_s}^{e_{i_s}}\neq 1$. Then $(d_{i_s}^{e_{i_s}}\cdots d_{i_1}^{e_{i_1}})(t_{i_1}^{e_{i_1}}\cdots t_{i_s}^{e_{i_s}})=\prod_{k=1}^{s}\{(e_{i_k})!\}$ is a unit in C_1. So, if $c_{(e)}t_{i_1}^{e_{i_1}}\cdots t_{i_s}^{e_{i_s}}$ is a non-zero term such that $e_{i_1}+\cdots+e_{i_s}$ is maximal, we have $(d_{i_s}^{e_{i_s}}\cdots d_{i_1}^{e_{i_1}})(x)=\prod_{k=1}\{(e_{i_k})!\}c_{(e)}\neq 0$, which is a contraction to $x\in C_1=Ker(\mathcal{D}er_1(C/A))$. This shows that x is equal to $\sum_{(e)}^{s} c_{(e)}$ belonging to $A[(t_1)^p, \cdots, (t_n)^p]$.

Lemma 11. *Let d, x be any element in H^+, C, respectively. Then $d(x^{p^t})$ belongs to $A\cdot C^{p^t}$ for $t=0, 1, 2, \cdots$.*

Proof. Let $\{d_0(=1), d_1, \cdots, d_l\})$ be an A-basis for H. Then we have $\Delta_n(d)=\sum_{(i)} a_{(i)}d_{i_1}\otimes d_{i_2}\otimes\cdots\otimes d_{i_n}$ for $a_i\in A$ where $n=p^t$, $\Delta_n=(1\otimes\cdots\otimes 1\otimes\Delta)\cdots(1\otimes\Delta)\Delta$ and $(i)=(i_1, i_2, \cdots, i_n)$ $(0\leqq i_k\leqq e)$. Since H is cocommutative, we have $a_{(i_1,i_2,\cdots,i_n)}=a_{(j_1,j_2,\cdots,j_n)}$ for any permutation $(j_1, j_2, \cdots, j_n)$ of $(i_1, i_2, \cdots, i_n)$ and

$$d(x^n)=\sum_{0\leqq k_1\leqq\cdots\leqq k_n}\frac{n!}{\alpha!\beta!\cdots\gamma!}a_{(k_1\cdots k_n)}d_{k_1}(x)\cdots d_{k_n}(x)$$

where $\alpha, \beta, \cdots, \gamma$ are cardinal numbers of equal numbers in $\{k_1, k_2, \cdots, k_n\}$. This completes the proof, since $\dfrac{n!}{\alpha!\beta!\cdots\gamma!}=0 \bmod p$ unless $k_1=k_2=\cdots=k_n$.

Theorem 12. *Let H be a cocommutative pointed Hopf algebra over a field A and C is a Galois H^*-object over A which is strongly radicial over A. Then there exists a sequence of subrings of C: $C=C_0\supset C_1\supset\cdots\supset C_n=A$ satisfying, for each $i=1, 2, \cdots, n-1$,*

(1) *C_i is finitely generated projective as a C_{i+1}-module.*

(2) *$d(C_i)\subseteq C_i$ for all $d\in H$.*

(3) *A left C_i-module $Hom_A(C_i, C_i)$ is generated by the endomorphisms of C_i induced by each element in H.*

(4) $C_i[\mathfrak{Der}_1(C_i/C_{i+1})]=Hom_{C_{i+1}}(C_i, C_i)$.

Proof. Let C_i, H_i be as above. Then (1) is obvious. (2) for $i=1$ follows from Lem. 10 and 11. Since C_1 is a C_1-module direct summand of C, $Hom_A(C_1, C_1)$ may be considered to be contained in $Hom_A(C, C)$. So any homomorphism in $Hom_A(C_1, C_1)$ is induced by an element $\sum c_i\otimes d_i$ in $C\otimes H$ for $c_i\in C$, $d_i\in H$. Let us write $C=C_1\oplus C_1'$ for a C_1-submodule C_1' of C. Let $c_i=c_i^0+c_i'$ for $c_i^0\in C_1$, $c_i'\in C_1'$. Then we have $\sum c_id_i(x)=\sum c_i^0d_i(x)+\sum c_i'd_i(x)$ for $x\in C_1$ and so $\sum c_i'd_i(x)\in C_1\cap C_1'(=0)$. Hence $\sum c_i^0\otimes d_i$ induces the same homomorphism in $Hom_A(C_1, C_1)$. This shows the statement (3) for $i=1$. It follows from Theorem 8 that $C\otimes A[H_2]=Hom_{C_2}(C, C)$. Then, by the same argument above, a C_1-module $Hom_{C_2}(C_1, C_1)$ is generated by the endomorphisms of C_1 induced by each element in $A[H_2]$. Since each element of H_2 induces an ordinary derivation on C_1, we obtain $C_1[\mathfrak{Der}_1(C_1/C_2)]=Hom_{C_2}(C_1, C_1)$ and $C_2=Ker(H_2)=Ker(\mathfrak{Der}_1(C_1/C_2))$. Hence, using again Lemma 10, we have $C_2=A[t_1^p, t_2^p, \cdots, t_r^p]$ for $t_i\in C_1$ and so $C_2=A\cdot C^{p^2}$. Repeating the argument above, we complete the proof.

Corollary. *Under the situation above, moreover, let K be a C-algebra which is finitely generated projective as a C-module. Then $H^n(K/A)=H^n(K/C)$ for $n>2$ and there is an exact sequence*

$$0\rightarrow H^2(C/A)\rightarrow H^2(K/A)\rightarrow H^2(K/C)\rightarrow 0$$

where $H^r(K/A)$ denotes a Amitsur cohomology group for a extension ring K/A.

Proof. By [5, Theorem 4.3], we have an exact sequnece

$$\cdots\rightarrow H^{n-1}(K/C)\rightarrow H^n(C/A)\rightarrow H^n(K/A)\rightarrow H^n(K/C)\rightarrow\cdots$$

So it suffices to show $H^1(K/C)=0$ and $H^n(C/A)=0$ for $n>2$. The first follows from [1, Theorem 3.8]. It follows from [10, Theorem 6] that $H^n(C_i/C_{i+1})$ vanish for $n>2$ where the C_i's are as above. Hence, using again [4, Theorem 4.3], we obtain $H^n(C/A)=0$ for $n>2$.

KOBE UNIVERSITY

References

[1] S.A. Amitsur: *Homology groups and double complexes for arbitrary fields*, J. Math. Soc. Japan **14** (1962), 73–112.

[2] N. Bourbaki: Algèble Commutative, Chap. 1. 2, Hermann, 1961.

[3] S.U. Chase and M.E. Sweedler: Hopf Algebras and Galois Theory, Lecture Notes in Mathematics, Vol. 97, Springer-Verlag, Berlin, 1969.

[4] Y. Nakai: *High order derivations* I, Osaka J. Math. **7** (1970), 1–27.

[5] A. Rosenberg and D. Zelinsky: *Amitsur's complex for inseparable fields*, Osaka Math. J. **14** (1962), 219–240.

[6] M.E. Sweedler: Hopf Algebras, W.A. Benjamin, New York, 1969.

[7] Y. Takeuchi: *On strongly radicial extensions*, to appear.

[8] S. Yuan: *Inseparable Galois theory of exponent one*, Trans. Amer. Math. Soc. **149** (1970), 163–170.

[9] ————: *Finite dimensional inseparable algebras*, Trans. Amer. Math. Soc. **150** (1970), 577–589.

[10] ————: *Central separable algebras with purely inseparable splitting rings of exponent one*, Trans. Amer. Math. Soc. **153** (1971), 427–450.