NOTE ON THE ISOMORPHISM CLASS GROUPS OF HOPF GALOIS EXTENSIONS

HIROAKI KOMATSU and ATSUSHI NAKAJIMA

Let $R$ be a commutative ring with identity and let $H$ be a finite Hopf algebra over $R$. For a commutative ring extension $S/R$, the notion of Galois $H$-object $S$ over $R$ was introduced by S. U. Chase and M. E. Sweedler in [1], and $H$ is called a Galois Hopf algebra of $S/R$. This is a generalization of a separable Galois extension and a purely inseparable extension. If a field $K$ is a Galois extension of a subfield $k$ with Galois group $G$, then $G$ is uniquely determined. On the other hand, A. Hattori pointed out in [3] that the purely inseparable field extension $K = k[X]/(X^p - r)$ of $k$ of characteristic $p$ has two essentially distinct Galois Hopf algebras $H(0, p)$ and $H(1, p)$ defined below in the sense of Chase and Sweedler [1]. In this note we show that the group of isomorphism classes of Galois objects $\text{Gal}(k, H(0, p))$ and $\text{Gal}(k, H(1, p))$ are isomorphic and give some results with related topics.

In the following, all algebras, morphisms and tensor products are taken over a fixed commutative ring $R$ unless otherwise stated. $H$ is a Hopf algebra which is a finitely generated projective $R$-module.

Now for the convenience of readers, we review the definitions of Galois objects and related notations according to [1]. A commutative algebra $S$ is called an $H$-comodule algebra if there exists an algebra morphism $\rho_S : S \to S \otimes H$ such that $(\rho_S \otimes I)\rho_S = (I \otimes \Delta)\rho_S$ and $(I \otimes \varepsilon)\rho_S = I$, where $I$ is the identity morphism and $\Delta, \varepsilon$ are coalgebra structure morphisms of $H$. For $H$-comodule algebras $S$ and $T$ with structure morphisms $\rho_S$ and $\rho_T$ respectively, a morphism $\phi : S \to T$ is called an $H$-comodule algebra morphism if $\phi$ is an algebra morphism such that $\rho_T \phi = (\phi \otimes I)\rho_S$. $S$ is called a Galois $H$-object over $R$ if $R = S_0 = \{ s \in S | \rho_S(s) = s \otimes 1 \}$, the invariant subalgebra of $S$ under $\rho_S$. $S$ is a faithfully flat $R$-module and the morphism $\gamma : S \otimes S \to S \otimes H$ defined by $\gamma(x \otimes y) = (x \otimes 1)\rho_S(y)$ is an isomorphism. Two Galois $H$-objects $S$ and $T$ are called isomorphic if there exists an $H$-comodule algebra isomorphism $\phi$ from $S$ to $T$. Let $S$ and $T$ be Galois $H$-objects with structure morphisms $\rho_S$ and $\rho_T$ respectively. Consider the morphism

$$(I \otimes \tau)(\rho_S \otimes I) - I \otimes \rho_T : S \otimes T \to S \otimes T \otimes H,$$

where $\tau$ is the twist morphism $x \otimes y \to y \otimes x$. Then the subalgebra $S \cdot T = \ker[(I \otimes \tau)(\rho_S \otimes I) - I \otimes \rho_T]$ of $S \otimes T$ is a Galois $H$-object and the $H$-
comodule structure on $S \cdot T$ is given by $I \otimes \rho_T = (I \otimes \tau)(\rho_S \otimes I)$. Then in the set of isomorphism classes of Galois $H$-objects $\mathrm{Gal}(R, H)$, we can define the product

$$[S][T] = [S \cdot T] \in \mathrm{Gal}(R, H),$$

where $[X]$ is the isomorphism class of Galois $H$-objects which are isomorphic to $X$, and $\mathrm{Gal}(R, H)$ is an abelian group with identity element $[H]$. These notions are also defined by usual action (cf. [1, 5]).

In the following $R$ is a commutative algebra over the prime field $GF(p)$ ($p \neq 0$). For an element $u$ in $R$, we denote by $H(u, p^n)$, the free Hopf algebra over $R$ with basis $\{1, \delta, \ldots, \delta^{p^n-1}\}$ whose Hopf algebra structure is defined as follows:

- algebra structure: $\delta^{p^n} = 0$,
- coalgebra structure: $\Delta(\delta) = \delta \otimes 1 + 1 \otimes \delta + u(\delta \otimes \delta)$, $\varepsilon(\delta) = 0$,
- antipode: $\lambda(\delta) = \sum_{i=1}^{p^n-1} (-1)^i u^{p^n-i-1} \delta^i$.

Then in $H(1, p^n)$, if we put $\sigma = \delta + 1$, then $\langle \sigma \rangle$ is a cyclic group of order $p^n$ and $H(1, p^n) = R\langle \sigma \rangle$, where $R\langle \sigma \rangle$ is the group algebra of $\langle \sigma \rangle$. On the other hand, $H(0, p^n)$ is the algebra which is generated by derivation $\delta$ of nilpotency index $p^n$. In general $H(1, p^n)$ and $H(0, p^n)$ are non-isomorphic Hopf algebras.

For an $R$-algebra $S = R[X]/(X^p - s) = R[x] (s \in R)$, we define a morphism $\rho_S: S \to S \otimes H(0, p)$ by $\rho_S(x) = x \otimes 1 + 1 \otimes \delta$. Then it is easy to check that $\rho_S$ gives an $H(0, p)$-comodule algebra structure on $S$ and $S$ is a Galois $H(0, p)$-object over $R$ (cf. [1, p. 35, Example 4.11]). We set the above type of Galois $H(0, p)$-object by $[x; s]$. Then we have the following which was proved in [5, Lemma 2.1 and Th. 2.2].

**Theorem 1.** Let $S = [x; s]$ and $T = [y; t]$ be Galois $H(0, p)$-objects defined as above.

1. Let $\phi: S \to T$ be a morphism of Galois $H(0, p)$-object. Then $\phi$ is an isomorphism if and only if there exists an element $r$ in $R$ such that $s - t = r^p$. When this is the case, $\phi$ is defined by $\phi(x) = y + r$.

2. $S \cdot T = [x; s + t]$.

**Proof.** (1) By $\rho_T \phi = (\phi \otimes I) \rho_S$, we have $\phi(x) = y + r$ for some $r$ in $R$. Since $\phi$ is an algebra morphism, $s - t = r^p$ is clear.

(2) By the definition of the product $S \cdot T$, the subalgebra $A$ of $S \otimes T$
generated by the element \( z = x \otimes 1 + 1 \otimes y \) over \( R \) is contained in \( S \cdot T \) and \( z^p = s + t \). Since \( A \) is a Galois \( H(0, p) \)-object in \( S \cdot T \), \( A \) is equal to \( S \cdot T \) by [1, Th. 1.12].

Since \( R \) is an algebra over \( GF(p) \), \( R^p = |r^p| r \in R \) is an additive subgroup of the additive group \( R \), and by [5, Th. 1.4], if \( S \) is a Galois \( H(0, p) \)-object over \( R \), then \( S \) is isomorphic to \([x : s] \) for some \( s \) in \( R \). Thus we have the following

**Corollary 2.** \( \text{Gal}(R, H(0, p)) \) is isomorphic to \( R/R^p \) as groups.

Next we consider a Galois \( H(1, p) \)-object. For \( S = R[X]/(X^p - s) = R[x] \), we define an \( H(1, p) \)-comodule structure on \( R[x] \) by \( \rho(x) = x \otimes \sigma \). Then by [1, pp. 36–39], \( R[x] \) is a Galois \( H(1, p) \)-object if and only if \( x^p \) is invertible in \( R \). We set this type of Galois \( H(1, p) \)-object by \( \langle x : s \rangle \). Let \( \text{gal}(R, H(1, p)) \) be the set of isomorphism classes of Galois \( H(1, p) \)-objects \( \langle x : s \rangle \). Then we have the following which is similar to Th. 1 and Cor. 2.

**Theorem 3.** Let \( S = \langle x : s \rangle \) and \( T = \langle y : t \rangle \) be Galois \( H(1, p) \)-objects defined as above.

1. Let \( \phi: S \to T \) be a morphism of Galois \( H(1, p) \)-object. Then \( \phi \) is an isomorphism if and only if there exists an invertible element \( r \) in \( R \) such that \( s = r^p t \). When this is the case \( \phi \) is defined by \( \phi(x) = ry \).
2. \( S \cdot T = \langle z : st \rangle \).

**Proof.** (1) By \( \rho_r \phi = (\phi \otimes I) \rho_s \), we have \( \phi(x) = ry \) for some \( r \) in \( R \). Since \( \phi \) is an algebra isomorphism, \( r \) is invertible and \( s = r^p t \).

(2) It is easy to see that the element \( x \otimes y \) in \( S \cdot T \) generates a subalgebra \( A \) which is a Galois \( H(1, p) \)-object. Then by [1, Th. 1.12], \( A \) is equal to \( S \cdot T \).

**Corollary 4.** \( \text{gal}(R, H(1, p)) \) is a subgroup of \( \text{Gal}(R, H(1, p)) \) and \( \text{gal}(R, H(1, p)) \) is isomorphic to \( U(R)/U(R)^p \), where \( U(R) \) is the unit group of \( R \).

In [1, Example 4.16], S. U. Chase proved the following theorem. Let \( R \) be an arbitrary commutative ring and let \( G \) be a cyclic group of order \( n \). Then there exists a one-to-one correspondence between Galois \( RG \)-objects and pairs \((I, \beta)\), where \( I \) is an invertible \( R \)-module and \( \beta: I \otimes I \otimes \cdots \otimes I \) (\( n \)-times) \( \to R \) is an \( R \)-module isomorphism. Therefore, \( \text{gal}(R, H(1, p)) \)
does not equal \( \text{Gal}(R, H(1, p)) \) for a certain ring \( R \) and if \( R \) is a field, \( \text{gal}(R, H(1, p)) \) equals \( \text{Gal}(R, H(1, p)) \).

By Cor. 2 and Cor. 4, we have the following

**Corollary 5.** Let \( k \) be a field of characteristic \( p \). Then the following conditions are equivalent:

1. \( k \) is a perfect field.
2. \( \text{Gal}(k, H(0, p)) = 0. \)
3. \( \text{Gal}(k, H(1, p)) = 1. \)

In general, we have the following

**Theorem 6.** If \( k \) is a field of characteristic \( p \), then \( \text{Gal}(k, H(0, p)) \) is isomorphic to \( \text{Gal}(k, H(1, p)) \) as groups.

**Proof.** Let \( k \) be an infinite field and let \( K \) be an extension field of \( k \). First we show that \( \#k \leq \#(U(K)/U(k)) \) where \( \#X \) is the cardinality of \( X \). Let \( x \) be an element in \( K \) which does not contained in \( k \). For elements \( a, b \) in \( k \), we assume that \( U(k) \langle x + a \rangle = U(k) \langle x + b \rangle \). Then there exists an element \( c \) in \( U(k) \) such that \( x + a = c(x + b) \) and so \((1 - c)x + (a - cb) = 0. \)

Since \( 1 - c \) and \( a - cb \) are contained in \( k \), we have \( c = 1 \) and \( a = cb \). Therefore \( a = b \) and thus \( \#k \leq \#(U(K)/U(k)) \). Now in the proof of the theorem, we may assume that \( k \neq k^p \). Since \( k/k^p \) and \( U(k)/U(k)^p \) are elementary abelian \( p \)-groups, it suffices to show that \( \#(k/k^p) = \#(U(k)/U(k)^p) \).

As vector spaces over \( k^p \), we have \( \#k^p \leq \#(k/k^p) \leq \#k \). But since \( k \) is isomorphic to \( k^p \) and the fact we have just shown above, \( \#k = \#(k/k^p) = \#(U(k)/U(k)^p) \).

For a separable field extension, we have the following example which was given in [5, Remark 2].

**Example 7.** Let \( k \) be the prime field \( GF(2) \). Then the polynomial \( X^4 + X + 1 \) is separable irreducible in \( k[X] \) and so \( K = k[X]/(X^4 + X + 1) \) is a cyclic \( 2^2 \)-extension of \( k \) with Galois group \( \langle \sigma \rangle \) of order 4. Thus \( K \) is a Galois \( k \langle \sigma \rangle \)-object over \( k \), where \( k \langle \sigma \rangle \) is the dual Hopf algebra of the group algebra \( k \langle \sigma \rangle \). On the other hand, let \( H \) be a free \( k \)-module with basis \( \{1, D, D^2, D^3\} \). The Hopf algebra structure of \( H \) is defined by \( D^4 = D \), \( \Delta(D) = D \otimes 1 + 1 \otimes D \), \( \varepsilon(D) = 0 \) and \( \lambda(D) = -D \). Then by [5, Th. 1.3], \( K \) is a Galois \( H \)-object of \( k \) and we can see that \( z^2 = 0 \) or
\[ z^2 = 1 \] for any \( z \in H^* \). Thus \( k\langle \sigma \rangle \) is not isomorphic to \( H^* \) as Hopf algebras. This shows that \( K = k[X]/(X^* + X + 1) \) has two non-isomorphic Galois Hopf algebras \( k\langle \sigma \rangle^* \) and \( H \).

For the above Hopf algebras \( R\langle \sigma \rangle^* \) and \( H \), the isomorphism class groups \( \text{Gal}(R, R\langle \sigma \rangle^*) \) and \( \text{Gal}(R, H) \) were also computed for an arbitrary commutative algebra \( R \) over \( GF(2) \). Since \( R\langle \sigma \rangle = H(1, 2^1) \), then by [4, Th. 3.2.4], there is a group isomorphism

\[ \text{Gal}(R, R\langle \sigma \rangle^*) \cong R^+_1/ M_1, \]

where \( R^+_1 = R \times R \), the cartesian product of \( R \) with addition defined by

\[ (s_1, t_1) + (s_2, t_2) = (s_1 + s_2, s_1s_2 + t_1 + t_2) \]

and \( M_1 = |(r^2 + r, r(r^2 + r) + s(1 + s))|, s \in R \). On the other hand, by [5, Th. 2.2], there is a group isomorphism

\[ \text{Gal}(R, H) \cong R/ \{ r^4 + r | r \in R \}. \]

If we take \( R = GF(2) \), then \( M_1 = (0, 0) \) and \( |r^4 + r | r \in R | = 0 \) and so \( \text{Gal}(GF(2), GF(2) \langle \sigma \rangle^*) \cong GF(2) \times GF(2) \) which is a cyclic group of order 4 by definition of addition, and \( \text{Gal}(GF(2), H) \cong GF(2) \). Therefore

**Theorem 7.** Under the above notations, \( \text{Gal}(GF(2), GF(2) \langle \sigma \rangle^*) \) is not isomorphic to \( \text{Gal}(GF(2), H) \).

For a separable field extension with characteristic 0, the similar example was obtained in [2, Example 2.3] and they showed that for the rational number field \( Q \), the field extension \( Q[\sqrt{2}] / Q \) has two different type of Galois Hopf algebras \( H_1 \) and \( H_2 \). But it is not known that the isomorphism class groups \( \text{Gal}(Q, H_1) \) and \( \text{Gal}(Q, H_2) \) are isomorphic or not.

**References**


Department of Mathematics
Graduate School of Natural Science and Technology
Okayama University, Okayama 700, Japan

Department of Mathematics
College of Liberal Arts and Sciences
Okayama University, Okayama 700, Japan

(Received February 13, 1991)