THE COHOMOLOGICAL ASPECTS OF HOPF GALOIS EXTENSIONS OVER A COMMUTATIVE RING

KENJI YOKOGAWA

(Received October 12, 1979)

Introduction. Let $R$ be a commutative ring with identity, $H$ a finite co-commutative Hopf algebra over $R$ and $A$ an $H$-Hopf Galois extension of $R$ in the sense of [15]. When $R$ is a field and $H$ is a group ring $RG$, $H$-module structure is simply stated as "the normal basis theorem" and combined with the theory of Galois algebras [8], [9]. But the normal basis theorem heavily depends on the $RG$-isomorphism $\text{Hom}_R(RG, R) \cong RG$. Therefore, in considering Hopf Galois extensions, the corresponding notion would be the dual normal basis theorem - an $H$-Hopf Galois extension of $R$ is isomorphic to $H^* = \text{Hom}_R(H, R)$ as $H$-modules - of course this does not always hold. We shall call such one a Hopf Galois extension with a dual normal basis. On the other hand, A. Nakajima [12], [13] examined an $H$-module structure under rather strong assumption $H^* \cong H$ and obtained information concerning the relation between the generalized Harrison cohomology groups and Hopf Galois extensions.

In this paper, we shall examine an $H$-module structure of Hopf Galois extensions and then shall establish an exact sequence involving the isomorphism classes of Hopf Galois extensions, unit-valued Harrison cohomology groups and Pic-valued Harrison cohomology groups, but unfortunately we must essentially assume that $H$ is commutative for a cohomological nature. In §1, we shall prove that an $H$-Hopf Galois extension $A$ has a decomposition $A \cong H^* \otimes_H P$ as $H$-modules with a rank 1 $H$-projective module $P$ satisfying some cohomological properties. In §2, we deal with Hopf Galois extensions with a dual normal basis. In §3, we shall start from a rank 1 $H$-projective module $P$ with further cohomological properties and then construct a Hopf Galois extension of $R$ from $P$. Finally in §4, using the results of §1, §2 and §3, we shall show that the isomorphism classes of Hopf Galois extensions of $R$ forms an abelian group. In Appendix, we shall define the generalized Harrison cohomology groups (c.f. [12]) and then, following the idea of A. Hattori [6], [7] we construct the cohomology groups $H^n(H)$ related to the generalized Harrison cohomology groups. Also we show that $H^2(H)$ is isomorphic to the group of isomorphism classes of $H$-Hopf Galois extensions of $R$ using the results of
previous sections.

Throughout this paper, \( R \) will denote a commutative ring with identity and \( H \) will be a finite co-commutative Hopf algebra over \( R \). \( \varepsilon \) (resp. \( \Delta \), resp. \( S \)) will denote the augmentation (resp. diagonalization, resp. antipode) of \( H \). Unadorned \( \otimes \) and \( \text{Hom} \) will mean \( \otimes_R \) and \( \text{Hom}_R \). We shall denote by \(-^* \) the functor \( \text{Hom}_R(\_, R) \). We shall deal with various \( H \)-modules, \( H-H \)-bimodules, etc., so to indicate the module structure, we shall use the index notation. For instance, \( \text{Hom}(H, R) \) means that \( \text{Hom}(H, R) \) is an \( H-H \)-bimodule by \( (h_1 \otimes h_2)(x) = f(h_1 x h_2) \), \( h_1, h_2, x \in H \), \( f \in \text{Hom}(H, R) \) and the tensor product is taken with the right \( H \)-module \( \text{Hom}(H, R) \) and the left \( H \)-module \( P \) over \( H \). Repeated tensor products of \( H \) will be denoted by exponents, \( H^n = H \otimes \cdots \otimes H \) with \( n \)-factors. For other notations and terminologies we shall refer to [3], [14] and [15].

Recently the author found that T.E. Early and H.F. Kreimer [16] had investigated this subject in different ways.

1. Decomposition of Hopf Galois extensions

First we shall review the definition of \( H \)-Hopf Galois extensions. Let an \( R \)-algebra \( A \) be a faithful finitely generated projective \( R \)-module which \( H \) measures and makes \( A \) an \( H \)-module algebra, that is there exists an \( R \)-homomorphism \( \rho: H \otimes A \to A \) with the properties;

\[
\rho(h \otimes ab) = \sum \rho(h_1 \otimes a) \rho(h_2 \otimes b) \\
\rho(h \otimes 1) = \varepsilon(h), \varepsilon \text{ is an augmentation (if } A \text{ has an identity)} \\
\rho(g h \otimes a) = \rho(g \otimes \rho(h \otimes a)), g, h \in H, a, b \in A.
\]

\( \rho(h \otimes a) \) is denoted by \( h \cdot a \) or simply by \( ha \). \( A \) is called an \( H \)-Hopf Galois extension of \( R \) if \( A^H = \{ a \in A | h \cdot a = \varepsilon(h) a \text{ for any } h \in H \} \) is equal to \( R \) and the homomorphism \( \phi: A \otimes A \to \text{Hom}(H, A) \) defined by \( [\phi(a \otimes b)](h) = ah \cdot b \), \( a, b \in A, h \in H \) is an isomorphism. We shall call this homomorphism \( \phi \) a fundamental homomorphism or a fundamental isomorphism if this homomorphism is an isomorphism. We know that \( H^* \) is an \( H \)-Hopf Galois extension of \( R \) (c.f. [3], [15]). As to \( H^* \) (with its canonical left (resp. right) \( H \)-module structure \( \_ \text{Hom}(H, R) \) (resp. \( \text{Hom}(H, R) \)) \), the isomorphism \( H^* \cong I \otimes H \) (resp. \( H^* \cong I' \otimes H \)) with rank 1 \( R \)-projective module \( I \) (resp. \( I' \)) is well-known [3], [11]. But unfortunately, these isomorphisms are not necessarily \( H-H \)-bimodule isomorphisms. Hence we consider the following condition (\#), which is automatically satisfied if \( H \) is a group ring or \( H \) is commutative.

\[
\begin{align*}
H^* &= \_ \text{Hom}(H, R) \cong I \otimes H \\
H^* &= H-H \text{-bimodules with a rank 1 } R \text{-projective module } I
\end{align*}
\]
Proposition 1.1. If \( H \) satisfies the condition (\#), then for any left \( H \)-module \( A \), there exists the unique (up to \( H \)-isomorphisms) left \( H \)-module \( P \) such that \( H_1 A \) is isomorphic to \( H_1^* H_2 \otimes H_2 P \) as left \( H \)-modules.

Proof. Let \( \Omega \) be \( \text{Hom}_{H_1}(H^*_A, H^*_A) \), then \( \Omega \) is isomorphic to \( H \) by homothety. And by this isomorphism \( _H^* H \) coincides with the original \( _H^* H \).
Since \( H^* \) is a right \( H \)-progenerator, we get by Morita theory \( _H A \cong _H^* H_2 \otimes H_2 \text{Hom}_{H_3}(H_3^* H_2, H_2 A) \) and \( \text{Hom}_{H_3}(H_3^* H_2, H_2 A) \Rightarrow P \) is uniquely determined up to \( H \)-isomorphisms. This verifies the assertion.

Corollary 1.2. Under the condition (\#), let \( A \) be an \( H \)-Hopf Galois extension of \( R \), then in the decomposition \( H_1 A \cong H_1^* H_2 \otimes H_2 P \) of Proposition 1.1, \( P \) is a finitely generated faithful protective \( H \)-module.

Proof. Since a Hopf Galois extension \( A \) of \( R \) is a left \( H \)-progenerator ([15] Cor. 1.4.), \( P = _H^* \text{Hom}_{H_2}(H_1^* H_2, A) \) is a finitely generated faithful projective \( H \)-module by the condition (\#). This verifies the assertion.

Now, for an \( H \)-Hopf Galois extension \( A \) of \( R \), we have the fundamental isomorphism
\[
\phi: A \otimes A \cong \text{Hom}(H, A).
\]
Hence the left \( H \)-module \( P \) of the decomposition \( A \cong H^* \otimes H \) must satisfy some relations, which we next investigate.

Proposition 1.3. Under the assumption (\#), let \( P \) be a left \( H \)-module and \( H_1 A = H_1^* H_2 \otimes H_2 P \). We consider \( \text{Hom}(A, A) \) and \( P \otimes H ) \) as left \( H \otimes H \)-modules by the formulas:

\[
[(g \otimes h)f](x) = \sum (g_1) f(S(g_2)xh)
\]
\[
(g \otimes h)(p \otimes x) = \sum (g_1)p \otimes hxS(g_2)
\]
\( g, h, x \in H, f \in \text{Hom}(H, A), p \in P, S \) is an antipode of \( H \). Then \( H_1 A \otimes H_2 P \) is \( H \otimes H \)-isomorphic to \( \text{Hom}(H, A) \), if and only if, \( H_1 P \otimes H_2 P \) is \( H \otimes H \)-isomorphic to \( P \otimes H \).

Proof. By the condition (\#), \( A \otimes A \) is \( H \otimes H \)-isomorphic to \( (I \otimes P) \otimes (I \otimes P) \) and with the given \( H \otimes H \)-module structures, \( \text{Hom}(H, A) \) is \( H \otimes H \)-isomorphic to \( I \otimes I \otimes P \otimes H \) through the isomorphisms \( \text{Hom}(H, A) \cong \text{Hom}(H, H^* \otimes H_2 P) \cong (H^* \otimes H_2 P) \otimes H^* \cong ((I \otimes H) \otimes H_2 P) \otimes (I \otimes H) \cong I \otimes I \otimes P \otimes H \). Thus \( A \otimes A \cong \text{Hom}(H, A) \), if and only if, \( I \otimes I \otimes P \otimes P \cong I \otimes I \otimes P \otimes H \). The later is equivalent to \( P \otimes P \cong P \otimes H \) since \( I \) is a rank 1 \( R \)-projective module. This verifies the assertion.

When \( A \) is an \( H \)-Hopf Galois extension of \( R \), the \( H \otimes H \)-module structure
of $\text{Hom}(H,A)$ in Proposition 1.3 is the one induced from that of $A \otimes A$ through the fundamental isomorphism $\phi$. As to that of $P \otimes H$, we have

**Proposition 1.4.** $P \otimes H$ with the $H \otimes H$-module structure given in Proposition 1.3 is $H \otimes H$-isomorphic to $(H \otimes H) \otimes H P$, where we consider $H \otimes H$ as a right $H$-module by the diagonalization $\Delta: H \rightarrow H \otimes H$.

Proof. We consider the homomorphisms $\alpha, \beta: P \otimes H \rightarrow (H \otimes H) \otimes H P$ defined by $\alpha(p \otimes h) = (1 \otimes h) \otimes p$, $\beta((g \otimes h) \otimes p) = \sum g_{(1)} p \otimes h s(g_{(2)}), g, h \in H, p \in P$. As easily checked, $\alpha$ and $\beta$ are well-defined $H \otimes H$-homomorphisms and are inverse to each other. This verifies the assertion.

$(H \otimes H) \otimes H P$ in the above Proposition will be denoted as $(H \otimes H) \otimes H P$. Also if $Q$ is a left $H$-module and $H \otimes H$ is regarded as a right $H$-module via $\Delta: H \rightarrow H \otimes H$, then the tensor product $Q \otimes H (H \otimes H)$ will be denoted as $Q \otimes_H (H \otimes H)$. These notations will be used frequently in the sequel.

In the next theorem, we use the terms of the generalized Harrison cohomology. As to them, we refer to [12] or Appendix of this paper. From now, the term cohomology will mean the generalized Harrison cohomology and cocycle, coboundary, etc. will mean that of the generalized Harrison cohomology.

**Theorem 1.5.** Under the assumption $(\#)$, an $H$-Hopf Galois extension $A$ of $R$ has a decomposition $A \simeq H^* \otimes_H P$ and there exists the $H \otimes H$-isomorphism $\phi: P \otimes P \simeq (H \otimes H) \otimes_H P$. If $H$ is commutative, above $P$ is a Pic-valued $1$-cocycle.

Proof. For commutative $H$, we shall show that $P$ is a rank $1$ $H$-projective module, then all will be settled. We localize the relation $P \otimes P \simeq (H \otimes H) \otimes_H P$ and count the rank of $P$, then we get that $P$ is rank $1$ over $H$. This completes the proof.

2. Hopf Galois extensions with a dual normal basis

Let $A$ be a left $H$-module algebra which is isomorphic to $H^*$ as left $H$-modules. Since the multiplication $m: A \otimes A \rightarrow A$ is a left $H$-homomorphism (regarding $A \otimes A$ as a left $H$-module via $\Delta$) and $A \simeq H^*$, passing to dual we get a right $H$-homomorphism $m^*: H \rightarrow H \otimes H$. $m^*$ is uniquely determined by $m^*(1) \in H \otimes H$, hence $A$ is determined by $m^*(1)$. Conversely, from $v = \sum_i v_i \otimes v_i \in H \otimes H$, we can form an $H$-module algebra $H^*(v)$ (not necessarily associative) as follows; $H^*(v) = H^*$ as a left $H$-module, the multiplication is given by $(f \cdot g)(x) = \sum_{i(\in)} f(v_i x_{(1)}) g(v_{i(2)x_{(2)}}, f, g \in H^*, x \in H$. As easily proved, $H^*(v)$ is
an $H$-module algebra. Thus $A=H^*(m^*(1))$ in this sense. Since $A$ is an associative algebra, the following diagram commutes.

$$
\begin{array}{ccc}
A \otimes A \otimes A & \xrightarrow{m \otimes 1} & A \otimes A \\
\downarrow 1 \otimes m & & \downarrow m \\
A \otimes A & \xrightarrow{m} & A
\end{array}
$$

(2.1)

Passing to dual, the commutativity of the above diagram (2.1) is equivalent to the commutativity of the following diagram.

$$
\begin{array}{ccc}
H \otimes H \otimes H & \xleftarrow{m^* \otimes 1} & H \otimes H \\
\uparrow 1 \otimes m^* & & \uparrow m^* \\
H \otimes H & \xleftarrow{m^*} & H
\end{array}
$$

(2.2)

Now we define the algebra homomorphisms $\Delta_i: H \otimes H \to H \otimes H \otimes H$ ($i=0,1,2,3$) by $\Delta_0(v)=1 \otimes v$, $\Delta_1(v)=(\Delta \otimes 1)(v)$, $\Delta_2(v)=(1 \otimes \Delta)(v)$, $\Delta_3(v)=v \otimes 1$, $v \in H \otimes H$. Then the commutativity of (2.2) means $\Delta_0(m^*(1))\Delta_0(m^*(1))=\Delta_3(m^*(1))\Delta_3(m^*(1))$. Thus we get the following

**Proposition 2.1.** $A$ is an associative $H$-module algebra (not necessarily with identity) which is isomorphic to $H^*$ as left $H$-modules, if and only if, $A=H^*(v)$ with $v \in H \otimes H$ satisfying $\Delta_0(v)\Delta_2(v)=\Delta_3(v)\Delta_3(v)$.

Next we shall consider the condition of $v$ which guarantees that $H^*(v)$ is an $H$-Hopf Galois extension of $R$.

**Lemma 2.2.** For $v=\sum_i v_i \otimes v_i \in H \otimes H$, the following diagram is commutative.

$$
\begin{array}{ccc}
H^*(v) \otimes H^*(v) & \xrightarrow{\phi'} & \text{Hom}_H(H \otimes H, H^*(v)) \\
\downarrow v^* & & \downarrow \theta \\
(H \otimes H)^* \xrightarrow{\text{can.}} (H \otimes_H (H \otimes H))^*
\end{array}
$$

where $H \otimes H$ is regarded as a left $H$-module via $\Delta$, and the homomorphisms are defined by $[[\phi'(f \otimes g)](x \otimes y)](z) = \sum_{i,j} f(v_{1_i} x_{(1)} g(v_{2_j} z_{(2)} y), [\theta(\tau)](x \otimes (y \otimes z)) = \tau(y \otimes z))(x)$, $[v^*(f \otimes g)](x \otimes y) = \sum f(v_{1} x) g(v_{2} y)$, $f,g \in H^*(v) = H^*$, $\tau \in \text{Hom}_H(H \otimes H, H^*(v))$, $x,y,z \in H$, can. is the usual canonical isomorphism.

*Proof.* This is an easy computation.

**Theorem 2.3.** $A=H^*(v)$, $v \in H \otimes H$ is an $H$-Hopf Galois extension of $R$, if and only if, $\Delta_0(v)\Delta_3(v)=\Delta_3(v)\Delta_3(v)$ and $v$ is a unit of $H \otimes H$. 
Proof. Let \( \alpha, \beta \) be the homomorphisms \( \text{Hom}_H(H \otimes H, H^*(v)) \) defined by
\[
\alpha(g)(x \otimes y) = g(1 \otimes x), \quad \beta(f)(x \otimes y) = \sum_{i,j} x_i f(S(x_{i,j}) y),
\]
g \in \text{Hom}_H(H \otimes H, H^*(v)), f \in \text{Hom}_H(H, H^*(v)), x, y \in H. \ \alpha \text{ and } \beta \text{ are well-defined homomorphisms and are inverse to each other. The commutativity of the following diagram is easily proved.}

\[
\begin{array}{ccc}
H^*(v) \otimes H^*(v) & \xrightarrow{\phi'} & \text{Hom}_H(H \otimes H, H^*(v)) \\
\downarrow{\phi} & & \downarrow{\alpha, \beta} \\
\text{Hom}(H, H^*(v)) & & \text{Hom}(H, H^*(v))
\end{array}
\]

where \( \phi' \) is the homomorphism defined in Lemma 2.2 and \( \phi \) is the fundamental homomorphism of an \( H \)-module algebra \( H^*(v) \). Thus, if \( A = H^*(v) \) is an \( H \)-Hopf Galois extension of \( R \), then \( \phi \) is a homomorphism, so \( \phi' \) is an isomorphism. By Lemma 2.2, this claims that \( v^* \) is an isomorphism, hence that \( v \) is a unit. Conversely we assume that \( v = \sum_i v_i \otimes v_{i^2} \) is a unit and \( \Delta_3(v) \Delta_2^2(v) = \Delta_2(v) \Delta_3^2(v) \). Then \( H^*(v) \) is an associative \( H \)-module algebra and by the above arguments, \( \phi \) is an isomorphism. We shall show that \( H^*(v) \) has an identity, then \( A^H \) is automatically equal to \( R \) (c.f. [15] Prop. 1.2). Thus \( A = H^*(v) \) is an \( H \)-Hopf Galois extension of \( R \). Applying \( 1 \otimes \epsilon \otimes 1 \) on both sides of \( \Delta_3^2(v) \Delta_2(v) = \Delta_2(v) \Delta_3^2(v) \) and then cancel \( v \). We get
\[
\sum_i 1 \otimes \epsilon(v_i) v_{i^2} = \sum_i v_i \otimes \epsilon(v_{i^2}).
\]
Further applying \( 1 \otimes \epsilon \) and \( \epsilon \otimes 1 \) on both sides, we get
\[
\begin{align}
\sum_i \epsilon(v_i) v_{i^2} &= \sum_i v_i \epsilon(v_{i^2}) \\
\sum_i \epsilon(v_i) v_{i^2} &= \sum_i \epsilon(v_{i^2}) v_i
\end{align}
\]
We shall put \( e = (\sum_i v_i \epsilon(v_{i^2}))^{-1} \epsilon = H^* = H^*(v) \). Then for any \( f \in H^*(v) \) and for any \( x \in H \), we have
\[
(f \cdot e)(x) = \sum_{i,j} f(v_i x_{i,j}) \epsilon(v_{i^2} x_{i^2})
\]
\[
= \sum_{i,j} f(v_i x_{i,j}) \epsilon((\sum_i v_i v_{i^2})^{-1}) \epsilon(v_{i^2} x_{i^2})
\]
\[
= \sum_i f(v_i \epsilon(v_{i^2})) \epsilon((\sum_i v_i v_{i^2})^{-1}) v_i,
\]
which is equal to \( f(x) \) by (2.3). Similarly, we get \( (e \cdot f)(x) = f(x) \) by (2.4). Thus \( e \) is an identity of \( H^*(v) \) and for \( x \in H \), \( x e = \epsilon(x) e \) follows readily. This completes the proof.

Let \( A, B \) be an \( H \)-module algebra, then \( A \cong B \) means that there exists an
algebra isomorphism $A \cong B$ which preserves $H$-actions.

**Theorem 2.4.** Two $H$-Hopf Galois extensions of $R$ with a dual normal basis $H^*(v), H^*(v')$ are isomorphic, if and only if, there exists a unit $w \in H$ such that $v \Delta(w) = (w \otimes w)v'$.

Thus, if $H$ is commutative, the isomorphism classes of $H$-Hopf Galois extensions of $R$ with a dual normal basis is set theoretically isomorphic to the unit-valued 2-cohomology group.

Proof. The existence of the left $H$-isomorphism $\eta: H^*(v) \cong H^*(v')$ is equivalent to the existence of the right $H$-isomorphism $\eta^*: H = (H^*(v'))^* \cong (H^*(v))^* = H$. The later is uniquely determined by the unit $w = \eta^*(1) \in H$.

The commutativity of the diagram

$$
\begin{array}{ccc}
H^*(v) \otimes H^*(v) & \xrightarrow{\eta \otimes \eta} & H^*(v') \otimes H^*(v') \\
\downarrow \text{multi.} & & \downarrow \text{multi.} \\
H^*(v) & \xrightarrow{\eta} & H^*(v')
\end{array}
$$

is equivalent to the commutativity of the diagram

$$
\begin{array}{ccc}
(H^*(v))^* \otimes (H^*(v))^* & \xrightarrow{\eta^* \otimes \eta^*} & (H^*(v'))^* \otimes (H^*(v'))^* \\
\downarrow l(v) & & \downarrow l(v') \\
H = (H^*(v))^* & \xrightarrow{\eta^*} & (H^*(v'))^* = H
\end{array}
$$

where $[l(v)](x) = v \Delta(x)$, $[l(v')](x) = v' \Delta(x)$, $x \in H$. Since $[l(v)\eta^*](1) = v \Delta(w)$ and $[\eta^* \otimes \eta^* l(v')](1) = (w \otimes w)v'$, the commutativity of (2.6) is equivalent to $v \Delta(w) = (w \otimes w)v'$. From Proposition 2.3 and the definition of cohomology, the assertion about cohomology follows readily. This completes the proof.

**Remark.** In §4, we shall define the product on the isomorphism classes of $H$-Hopf Galois extensions of $R$, and then we shall show that the isomorphism of Theorem 2.4 is a group isomorphism.

**3. General Hopf Galois extensions**

Let $P$ be a finitely generated faithful projective $H$-module with an $H^2$-isomorphism $\delta: P \otimes P \cong (H \otimes H) \otimes P$. If $H$ is commutative such $(P, \delta)$ is a $Pic$-valued 1-cocycle. By abuse the language, we shall call such $(P, \delta)$ a $Pic$-valued 1-cocycle even if $H$ is not commutative.
Let \((P, \phi)\) be a Pic-valued 1-cocycle. Then we have a chain of isomorphisms:

\[
P \otimes P \otimes P \cong P \otimes ((H \otimes H) \otimes \mu P) \cong H^2 \otimes \mu^2 (P \otimes P) \cong H^3 \otimes \mu (P \otimes P) \cong P \otimes P \otimes P.
\]

Composing these isomorphisms, we get an automorphism of \(P \otimes P \otimes P\), which we shall denote by \(u(P, \phi)\). When \(H\) is commutative, \(u(P, \phi)\) is an \(H^3\)-automorphism of \(P \otimes P \otimes P\) and we shall regard \(u(P, \phi)\) as a unit of \(H^3\) by homothety.

**Lemma 3.1.** If \(H\) is commutative, then for a Pic-valued 1-cocycle \((P, \phi)\) and a unit \(v\) of \(H^3\), we have \(u(P, v\phi) = d(v)u(P, \phi)\) (\(d\) is a coboundary operator) and \(u(P, \phi)\) is a unit-valued 3-cocycle.

**Proof.** The assertion follows by easy computations and usual localization technique.

**Theorem 3.2.** Let \(H\) be commutative and \((P, \phi)\) be a Pic-valued 1-cocycle, then \(A = H^* \otimes \mu P\) has a structure of an \(H\)-Hopf Galois extension of \(R\), if and only if, \(u(P, \phi)\) is a 3-coboundary.

**Proof.** First we shall prove only if part. Let \(\phi\) be the fundamental isomorphism \(A \otimes A \cong \text{Hom}(H, A)\). Then we have the \(H^2\)-isomorphism \(\phi'\);

\[
P \otimes P \cong H^2 \otimes \mu P\]

by Theorem 1.5. \(\phi'\) may differ from the given \(\phi\), but Lemma 3.1 ensures that the difference between \(u(P, \phi')\) and \(u(P, \phi)\) is a 3-coboundary. So we may assume \(\phi' = \phi\) and we have the following commutative diagram:

\[
\begin{array}{ccc}
A \otimes A & \xrightarrow{\phi} & \text{Hom}(H, A) \\
\parallel & & \parallel \text{can.} \\
(H^* \otimes P) \otimes H^* & \parallel & I \otimes I \otimes P \otimes H \\
\parallel \text{can.} & & \parallel \text{by Prop. 1.4} \\
I \otimes I \otimes P \otimes P & \xrightarrow{1 \otimes 1 \otimes \phi} & I \otimes I \otimes (H^2 \otimes \mu P)
\end{array}
\]

We shall show that \(u(P, \phi) = 1 \otimes 1 \otimes 1 \in H^3\). For this purpose, we may assume that \(R\) is a local ring, hence \(H^* = eH = He\), \(e\) is a free basis as an \(H\)-\(H\)-bimodule. We consider the following diagrams (they are commutative but the commutativity is unnecessary);
\[
(He \otimes_H P) \otimes (He \otimes_H P) \xrightarrow{\phi} \text{Hom}(H, He \otimes_H P)
\]
(3.2)

\[
(He \otimes H) \otimes_H (P \otimes P) \xrightarrow{\alpha \Delta} \text{Hom}(H, He \otimes_H P) \otimes (He \otimes_H P)
\]
(3.3)

where \(\alpha\) is defined by \([\alpha((xe \otimes ye) \otimes p)](h) = \sum (e \otimes e(hyS(x_{(2)})))x_{(2)}p\). \(\beta\) is defined by \(\beta((xe \otimes ye \otimes ze) \otimes p)(g \otimes h) = \sum (e \otimes e(gy)S(x_{(2)}))e(hzS(y_{(2)})))x_{(2)}p\). \(\gamma\) is defined by \([\gamma((e \otimes p_1) \otimes (e \otimes p_2) \otimes (e \otimes p_3))(g \otimes h) = (e \otimes p')(g((e \otimes p_2) \cdot h(e \otimes p_3)))\) (product in \(He \otimes H = H^* \otimes_H P\)), \(p, p_1, p_2, p_3 \in P, x, y, z, g, h \in H\).

(3.2) is a localized diagram of (3.1) and by the similar methods to Proposition 1.3, 1.4, \(\beta\) is a well-defined isomorphism. We shall compute \(\beta \cdot (1 \otimes \phi) \cdot (1 \otimes (1 \otimes \phi))\). For \((e \otimes p_1, e \otimes p_2, e \otimes p_3) \in (He \otimes_H P) \otimes (He \otimes_H P) \otimes (He \otimes_H P)\), we shall put \(\bar{\phi}(p_1, p_2, p_3) = \sum (1 \otimes p_1') \otimes p_2' \in H^2 \otimes_H P\) (we may assume that the first term of \(H^2\) is 1 by Proposition 1.4) and we shall put \(\bar{\phi}(p_i, p'_i) = \sum (1 \otimes p_1') \otimes p_2' \in H^2 \otimes_H P\). Then from the commutativity of (3.2), we get

\[
(3.5') \quad \sum (e \otimes g_1(p_2) \cdot (e \otimes g_2)h p_3) = \sum (e \otimes (e h p_2)S(g_2))g_3 p_i
\]

Since \(\bar{\phi}\) is an \(H^2\)-isomorphism, \(\bar{\phi}(\sum (g_1(p_2) \otimes g_2)h p_3) = \sum (g_1 \otimes g_2)h p_2' \otimes p_3',\) which is equal to \(\sum (1 \otimes g_1)h p_2' g_2(p_3) \otimes g_3 p_i,\) and \(e\) is a basis of \(H^*\) as an \(H-H\)-bimodule, so \(e(g h) = (e g)(h) = (e h)(g) = e(h g)\) for any \(g, h \in H\). Thus we get for \(g \in H, r \in R\);

\[
(3.5) \quad \sum (e \otimes g_1(p_2) \cdot (e \otimes g_2)h p_3) = \sum (e \otimes (e h p_2)S(g_2))g_3 p_i
\]

\[
(3.6) \quad (e \otimes p_1) \cdot (e \otimes h p_3) = \sum (e \otimes e(h p_1') p_2'), h \in H.
\]
Thus 
\[ [(\beta \cdot (1 \otimes \phi)) \cdot (1 \otimes (1 \otimes \phi))) ((e \otimes p_1) \otimes (e \otimes p_2) \otimes (e \otimes p_3))] (g \otimes h) \]
\[ = [\beta (\sum_{i,j \in F_p} (1 \otimes p_{ij}^i \otimes p_{ij}^j \otimes p_{ij}^k))(g \otimes h) \]
\[ = \sum_{i,j \in F_p} e \otimes e(g p_{ij}^i)(e(h p_{ij}^j) g p_{ij}^k) p_{ij}^k, \]
\[ = \sum_{i,j \in F_p} e \otimes e(g p_{ij}^i) e(h p_{ij}^j) p_{ij}^k. \]

By (3.5)' and (3.6)', this is equal to
\[ \sum_{i} (e \otimes p_1) \cdot (e \otimes e(h p_{ij}^i) g p_{ij}^k) \]
\[ = (e \otimes p_1) \cdot (\sum_{i,j} (e \otimes g_{ij}^i) p_2) \cdot (e \otimes g_{ij}^i) h p_3) \]
\[ = (e \otimes p_1) \cdot (g(e \otimes p_2) \cdot h(e \otimes p_3)). \]

Similarly,
\[ [(\beta \cdot (1 \otimes \phi)) \cdot (1 \otimes (1 \otimes \phi))) ((e \otimes p_1) \otimes (e \otimes p_2) \otimes (e \otimes P_3))] (g \otimes h) \]
\[ = \sum_{(i,j)} ((e \otimes p_1) \cdot (e \otimes g_{ij}^i) p_2) \cdot (e \otimes g_{ij}^i) h p_3). \]

Since \( A \) is an associative algebra, \( \beta \cdot (1 \otimes \phi) \cdot (1 \otimes (1 \otimes \phi)) = \beta \cdot (1 \otimes \phi) \cdot (1 \otimes (\phi \otimes 1)) \), which claims that \( u(P, \phi) = 1 \otimes 1 \otimes 1 \in H^3 \) as desired.

Conversely, let \((P, \phi)\) be a \(Pic\)-valued 1-cocycle and assume that \( u(P, \phi) \) is a unit-valued 3-coboundary. We may alter \( \phi \) by \( v \phi \) with the suitable unit \( v \in H^2 \). Hence we may assume \( u(P, \phi) = 1 \otimes 1 \otimes 1 \in H^3 \). We shall put \( A = H^* \otimes_P P, H^* = \iota \otimes H \). From \( \phi \), we make \( \phi: A \otimes A \approx \text{Hom}(H, A) \) such that the diagram (3.1) commutes. We define the product of \( A \) by \( a \cdot b = [\phi(a \otimes b)](1), 1 \in H, a, b \in A \). By the above arguments, \( u(P, \phi) = 1 \otimes 1 \otimes 1 \) claims that this product is associative and makes \( A \) an \( H \)-module algebras with the fundamental isomorphism \( \phi \). Only the existence of identity is not yet valid. We make a smash product \( A \# H(A \# H = A \otimes H) \) as an \( R \)-module we write \( a \# h \) rather than \( a \otimes h \), the product is defined by \( a \# g \cdot b \# h = \sum_{(i,j)} a g_{ij}^i b g_{ij}^j h, a, b \in A, g, h \in H \) and consider the homomorphism \( \mu: A \# H \to \text{Hom}(A, A) \) defined by \( [\mu(a \# h)](b) = ah \cdot b \). Locally \( A \) is an associative \( H \)-module algebra with a dual normal basis, hence by Proposition 2.1 \( A = H^*(v) \). From the proof of Theorem 2.3, that \( \phi \) is an isomorphism claims that \( v \) is a unit and \( A \) has an identity. Thus locally \( A \) is an \( H \)-Hopf Galois extension with identity. Hence \( \mu \) is an isomorphism locally (c.f. [15] Theorem 1.1), so globally. Let \( \mu(\sum_i a_i \# h_i) \) be an identity of \( \text{Hom}(A, A) \). Since \( \sum_i a_i \# h_i \) is contained in \( A \) locally, \( \sum_i a_i \# h_i \) is contained in \( A \) globally and \( \sum_i a_i \# h_i \) is a left identity of \( A \). By localization, \( \sum_i a_i \# h_i \) is a right identity of \( A \). This completes the proof.
Let $H$ be merely a finite Hopf algebra satisfying the condition $(\#)$ and $(P, \phi)$ be a Pic-valued 1-cocycle. From the above proof, if $A = H^* \otimes_R P$ has a structure of an $H$-Hopf Galois extension of $R$, then we can chose the cocycle condition isomorphism $\phi$ to satisfy that $u(P, \phi)$ is an identity automorphism of $P \otimes P \otimes P$. Conversely if $u(P, \phi)$ is an identity automorphism of $P \otimes P \otimes P$, then we can make $A = H^* \otimes_R P$ an associative $H$-module algebra (it may not have an identity — the commutativity of $H$ is used only to ensure the existence of an identity of $A$) with the fundamental isomorphism $\phi: A \otimes A \cong \text{Hom}(H, A)$. Instead of localization techniques, passing to the residue class field, we can prove the existence of an identity as follows;

**Theorem 3.3.** Let $H$ be a finite (of course co-commutative) Hopf algebra which satisfies the condition $(\#)$ and let $A = H^* \otimes_R P$ be an $H$-Hopf Galois extension $\Delta$ of $R$. Then we can choose an $H^2$-isomorphism $\phi: P \otimes P \cong (H \otimes H) \otimes_R P$ to satisfy that $u(P, \phi)$ is an identity automorphism of $P \otimes P \otimes P$. Conversely, let $(P, \phi)$ be a Pic-valued 1-cocycle and assume that $u(P, \phi)$ is an identity automorphism of $P \otimes P \otimes P$. Then $A = H^* \otimes_R P$ has a structure of an $H$-Hopf Galois extension of $R$.

**Proof.** Only the existence of an identity of $A = H^* \otimes_R P$ should be proved. We make a smash product $A \# H$ and consider the homomorphism $\mu: A \# H \to \text{Hom}(A, A)$ as the proof of Theorem 3.2. We shall show that $\mu$ is an isomorphism. For this purpose, we may assume that $R$ is a local ring, further by Nakayama’s lemma we may assume that $R$ is a field since $A \# H$ and $\text{Hom}(A, A)$ are finitely generated projective $R$-modules. From $\phi$, we have the isomorphism $\phi: (He \otimes_R P) \otimes (He \otimes_R P) \cong \text{Hom}(H, He \otimes_R P)$, where $e$ is a basis of $H^*$. We shall regard $(He \otimes_R P) \otimes (He \otimes_R P)$ as a left $H$-module via the second term and regard $\text{Hom}(H, He \otimes_R P)$ as a left $H$-module by $\mu \text{Hom}(H, He \otimes_R P)$. Then $\phi$ is a left $H$-homomorphism. As left $H$-modules, the former is $\nu$ direct sum of $\text{dim}_R P$-copies of $P$ and the latter is a direct sum of $\text{dim}_R P$-copies of $H^*$, which is isomorphic to the direct sum of $\text{dim}_R P$-copies of $H$. Since $H$ is a finite dimensional algebra over a field $R$ we get $P \cong H$ as left $H$-modules by Krull-Schmidt theorem. This means that $A$ has a dual normal basis, hence $A$ has an identity by Theorem 2.3 and $\mu$ is an isomorphism. Thus $\mu$ is an isomorphism for a general commutative ring $R$. Let $\mu(a)$ be an identity of $\text{Hom}(A, A)$. Then by Nakayama’s lemma, $a$ is contained in $A$ and $a$ is a left identity of $A$. Again by Nakayama’s lemma, $a$ is a right identity of $A$. Thus $A$ has an identity element. This completes the proof.

**Corollary 3.4.** If $H$ is a group ring $RG$ over a field $R$. Then any $RG$-Hopf Galois extension $A$ of $R$ (hence the usual Galois extension with the Galois group $G$) has a dual normal basis, therefore $A$ has a normal basis.
Proof. That $A$ has a dual normal basis is proved in the proof of Theorem 3.3. Considering the $H$-$H$-bimodule isomorphism $\gamma: H_RG \simeq H^* = \text{Hom}(RG, R)$ defined by $[\gamma(\sigma)](\tau) = \delta_{\sigma^{-1}, \tau}$ (Kronecker delta) $\sigma, \tau \in G$, the assertion follows.

Now, we shall assume that $H$ is commutative and shall investigate when two $H$-Hopf Galois extensions of $R$, $A = H^* \otimes_H P$, $B = H^* \otimes_H Q$ ($P \otimes P \simeq H^2 \otimes_H P$, $Q \otimes Q \simeq H^2 \otimes_H Q$, $u(P, \phi_A) = u(Q, \phi_B) = 1 \otimes 1 \otimes 1 \in H^3$) are isomorphic. By Proposition 1.1, if $A$ and $B$ are isomorphic then $P \simeq Q$ (we shall identify $P$ and $Q$). Let $\xi$ be the isomorphism $A = H^* \otimes_H P \simeq B = H^* \otimes_H P$, then $\xi$ induces an automorphism of $P$, which we shall denote by $\omega(\xi)$ and we sometimes regard $\omega(\xi)$ as a unit of $H$ by homothety. $\xi$ commutes with the multiplications of $A$ and $B$, so $\omega(\xi)$ commutes with $\phi_A$ and $\phi_B$. That is the following diagram is commutative.

\[
P \otimes P \xrightarrow{\phi_A} (H \otimes H) \otimes_H P \quad \xrightarrow{\Delta} \quad (H \otimes H) \otimes_H P
\]

\[
P \otimes P \xrightarrow{\phi_B} (H \otimes H) \otimes_H P \quad \xrightarrow{\Delta} \quad (H \otimes H) \otimes_H P
\]

Since $\phi_A$ and $\phi_B$ are $H^2$-isomorphisms and the isomorphism $1 \otimes \omega(\xi)$ is a left homothety by $\Delta(\omega(\xi))$, the commutativity of (3.7) claims that $\phi_A \phi_B^{-1} = \Delta(\omega(\xi))^{-1}$ ($\omega(\xi) \otimes \omega(\xi))$ or equivalently $\phi_A \phi_B^{-1} = d(\omega(\xi))$, $d$ is a coboundary operator. Conversely, if such $\omega(\xi)$ exists, we can easily make the isomorphism $\xi: H^* \otimes_H P \simeq H^* \otimes_H P$. Thus we get

**Theorem 3.5.** Let $H$ be a commutative Hopf algebra, $A = H^* \otimes_H P$ and $B = H^* \otimes_H Q$ be $H$-Hopf Galois extensions of $R$ with $\phi_A: P \otimes P \simeq H^2 \otimes_H P$ and $\phi_B: Q \otimes Q \simeq H^2 \otimes_H Q$, $u(P, \phi_A) = u(Q, \phi_B) = 1 \otimes 1 \otimes 1$. Then $A$ is isomorphic to $B$, if and only if, $P \simeq Q$ and $\phi_A \phi_B^{-1}$ is a unit-valued 2-coboundary.

Here we can review the results of §2. We assume that $H$ is commutative. Let $A = H^* \otimes_H P$ be an $H$-Hopf Galois extension of $R$ with a dual normal basis, so $P \simeq H$. By Theorem 3.2, there exists $\phi: H \otimes H \simeq H^2 \otimes_H H = H \otimes H$ with $u(H, \phi) = 1 \otimes 1 \otimes 1$. $\phi$ is a homothety by a unit $v$ of $H^3$. $u(H, v) = (v^{-1} \otimes 1) \cdot ((\Delta \otimes 1)(v^{-1})) \cdot ((1 \otimes \Delta)(v)) \cdot (1 \otimes v)$. Thus $u(H, \phi) = 1 \otimes 1 \otimes 1$ claims that $v$ is a unit valued 2-cocycle. As easily proved, the product of $A = H^* \otimes_H H$ defined by Theorem 3.2 is same as that of $H^*(v)$. Similarly Theorem 3.5
deduces Theorem 2.4 when \( P \cong H \).

4. The isomorphism classes of Hopf Galois extensions

Throughout this section, we assume that \( H \) is commutative.

First we shall prove two Lemmas, and then we shall prove that the isomorphism classes of \( H \)-Hopf Galois extensions of \( R \)-which we shall denote by \( E(H) \)-forms an abelian group.

Lemma 4.1 (c.f. [13] Lemma 2.5). Let \( m: G \to H \) be a homomorphism of finite Hopf algebras and let \( A \) be a \( G \)-Hopf Galois extension of \( R \). Then \( \text{Hom}_G(H, A) \) is an \( H \)-Hopf Galois extension of \( R \), where the multiplication on \( \text{Hom}_G(H, A) \) is defined by the formula;

\[
(f_1 \cdot f_2)(x) = \sum_{\omega} f_1(x \omega \omega) \cdot f_2(x \omega), \quad f_1, f_2 \in \text{Hom}_G(H, A), \quad x \in H.
\]

Proof. \( \epsilon \) is an identity of \( \text{Hom}_G(H, A) \) and \( \text{Hom}_G(H, A) \) is an associative \( H \)-module algebra. We shall consider the following diagram.

\[
\begin{array}{ccc}
\text{Hom}_G(H, A) \otimes \text{Hom}_G(H, A) & \overset{\phi'}{\longrightarrow} & \text{Hom}(H, \text{Hom}_G(H, A)) \\
\text{can.} & & \text{can.} \\
\text{Hom}_{G \otimes G}(H \otimes H, A \otimes A) & \overset{\alpha}{\longrightarrow} & \text{Hom}_G(H \otimes H, \text{Hom}(G, A)) \\
\text{can.} & & \text{can.}
\end{array}
\]

(4.1)

where \( \phi \) is the fundamental isomorphism \( A \otimes A \cong \text{Hom}(G, A) \) and \( \phi' \) is the fundamental homomorphism of an \( H \)-module algebra \( \text{Hom}_G(H, A) \). \( \alpha \) is defined by

\[
[\alpha(\tau)](x \otimes y) = \sum_{\omega} [\tau(x \omega \omega) x \omega y], \quad 1, x, y \in H, \quad \tau \in \text{Hom}_{G \otimes G}(H \otimes H, \text{Hom}(G, A)).
\]

As easily checked, (4.1) is a commutative diagram. \( \alpha \) is an isomorphism - the inverse \( \alpha^{-1} \) is given by the formula;

\[
[[\alpha^{-1}(\nu)](x \otimes y)](z) = \sum_{\omega} \nu(x \omega y \omega \omega) z \omega x \omega y,
\]

\( \nu \in \text{Hom}_G(H \otimes H, A), \quad x, y, z \in H, \quad z \in G \). Thus \( \phi' \) is an isomorphism. So \( \text{Hom}_G(H, A) \) is an \( H \)-Hopf Galois extension of \( R \) as desired.

Lemma 4.2. Let \( A_i \) be an \( H_i \)-Hopf Galois extension of \( R \) \((i=1,2)\), then \( A_1 \otimes A_2 \) is an \( H_1 \otimes H_2 \)-Hopf Galois extension of \( R \).

Proof. The tensor product of the fundamental isomorphisms of \( A_1 \) and
$A_2$ will give the fundamental isomorphism of $A_1 \otimes A_2$.

Well, the multiplication $m: H \otimes H \rightarrow H$ is a homomorphism of Hopf algebras. Let $A, B$ be an $H$-Hopf Galois extension of $R$, we shall define

$$A \cdot B = \text{Hom}_R(H, A \otimes B)$$

which is an $H$-Hopf Galois extension of $R$ by Lemma 4.1 and 4.2.

By the image of $1 \in H$, $A \cdot B$ is characterized as follows;

**Lemma 4.3.** Let $A, B$ be an $H$-Hopf Galois extension of $R$, then $A \cdot B = \text{Hom}_R(H, A \otimes B)$ is isomorphic to \{\(\sum a_i \otimes b_i \in A \otimes B | \sum h a_i \otimes b_i = \sum a_i \otimes h b_i \) for any $h \in H}\}.

We shall denote \{\(\sum a_i \otimes b_i \in A \otimes B | \sum h a_i \otimes b_i = \sum a_i \otimes h b_i \) for any $h \in H}\} by $(A \otimes B)^H$. In the sequel, we will pass freely between $A \cdot B$ and $(A \otimes B)^H$.

By this product, $E(H)$ forms an abelian semi-group.

**Proposition 4.4.** Let $A = H^*(v)$, $B = H^*(v')$ be an $H$-Hopf Galois extension of $R$ with dual normal basis. Then

$$H^*(v) \cdot H^*(v') \cong H^*(vv')$$

Proof. First we shall show that $H^*(v) \cdot H^*(v')$ is isomorphic to $H^*(vv')$ as $H$-modules. We define the homomorphisms $\alpha, \beta: (H^*(v) \otimes H^*(v'))^H \rightarrow H^*(vv')$ by the formulas

$$[\alpha(f_1 \otimes f_2)](x) = f_1(x)f_2(1)$$
$$[\beta(f)](x \otimes y) = f(xy)$$

$f_1 \otimes f_2 \in (H^*(v) \otimes H^*(v'))^H$, $f \in H^*(vv')$, $1, x, y \in H$. It is easily checked that $\alpha$ and $\beta$ are well-defined left $H$-homomorphisms and are inverse to each other. That $\alpha$ gives an isomorphism of $H$-module algebras can be proved by straightforward but laborious calculations. This completes the proof.

From Proposition 4.4 and Theorem 2.4, we get

**Corollary 4.5.** The group of the isomorphism classes of $H$-Hopf Galois extensions of $R$ with dual normal basis is isomorphic to the unit-valued 2-cohomology group as abelian groups.

**Theorem 4.6.** Let $(P, \phi_P)$, $(Q, \phi_Q)$ be a Pic-valued 1-cocycle with $u(P, \phi_P) = u(Q, \phi_Q) = 1 \otimes 1 \otimes 1$, and let $A = H^* \otimes_H P$, $B = H^* \otimes_H Q$ be an $H$-Hopf Galois extension of $R$ induced from $P$, $Q$ respectively. Then $A \cdot B$ is an $H$-Hopf
Galois extension of \( R \) induced from a Pic-valued 1-cocycle \( (P \otimes_R Q, \Phi_P \otimes_R \Phi_Q) \).
Especially, the isomorphism classes of \( H \)-Hopf Galois extensions of \( R \), \( E(H) \) forms an abelian group.

Proof. We shall define the homomorphisms \( \alpha', \beta' : (A \otimes B) \rightarrow H^* \otimes_H (P \otimes_R Q) \) by the formula;
\[
\alpha'((f_1 \otimes p) \otimes (f_2 \otimes q)) = \alpha(f_1 \otimes f_2) \otimes (p \otimes q)
\]
\[
\beta'(f \otimes (p \otimes q)) = \sum (f_i \otimes p) \otimes (f_j \otimes q) \text{ if } \beta(f) = \sum f_i \otimes f_j
\]
where \( \alpha, \beta \) is the homomorphism in Proposition 4.1, \( f, p, q \in P, q \in Q \).
As easily checked, \( \alpha' \) and \( \beta' \) are well-defined left \( H \)-homomorphisms and are inverse to each other. To see that \( \alpha' \) is an isomorphism of \( H \)-module algebras, we may localize it. Then Proposition 4.4 ensures that \( \alpha' \) is an isomorphism of \( H \)-module algebras. Now, that \( E(H) \) forms an abelian group with identity \( H^* \) follows readily. This verifies the assertion.

Appendix

Throughout we assume that \( H \) is commutative.

First we shall define the generalized Harrison cohomology. Let
\[
\Delta^n, \Delta_i^n (i = 1, 2, \ldots, n), \Delta_{n+1}^n : H^* \rightarrow H^{*+1} (n \geq 0)
\]
be the algebra homomorphism defined by the formulas;
\[
\Delta^n(x_1 \otimes \cdots \otimes x_n) = 1 \otimes x_1 \otimes \cdots \otimes x_n
\]
\[
\Delta_i^n(x_1 \otimes \cdots \otimes x_n) = x_1 \otimes \cdots \otimes x_{i-1} \otimes \Delta(x_i) \otimes x_{i+1} \otimes \cdots \otimes x_n
\]
\[
\Delta_{n+1}^n(x_1 \otimes \cdots \otimes x_n) = x_1 \otimes \cdots \otimes x_n \otimes 1, x_i \in H.
\]
\( H^0 \) means \( R \) and we note that \( \Delta_0^n, \Delta_1^n \) coincides with the unit map \( R \rightarrow H \). Let \( U \) denote the unit functor and \( \text{Pic} \) denote the Picard group functor. \( \Delta_i^n (i=0, 1, \ldots, n+1) \) yields functors \( U(H^*) \rightarrow U(H^{*+1}), \text{Pic}(H^*) \rightarrow \text{Pic}(H^{*+1}) \), which we shall denote by the same letter \( \Delta_i^n \). We shall define
\[
d_n : U(H^*) \rightarrow U(H^{*+1}), d_n : \text{Pic}(H^*) \rightarrow \text{Pic}(H^{*+1})
\]
as the alternate sum of \( \Delta_i^n \) (we use the same letter \( d_n \) or simply \( d \), it would not make confusions). We remark that \( d_0 \) is a zero homomorphism.
Since \( d^2 = d_{n+1}d_n = 0 \), we can define cochain complexes \( C(H, U) = \{ U(H^*) \}, d_n \}_{n \geq 0} \) and \( C(H, \text{Pic}) = \{ \text{Pic}(H^*) \}, d_n \}_{n \geq 0} \). The \( n \)-th cohomology group \( \text{Ker}(d_n)/\text{Im}(d_{n-1}) (n \geq 1) \) of \( C(H, U), C(H, \text{Pic}) \) is denoted by \( H^n(H, U), H^n(H, \text{Pic}) \) respectively, and will be called the unit-valued (resp. Pic-valued) generalized Harrison cohomology group. The 0-th cohomology group is defined as \( H^0(H, U) = \text{Ker}(d_0) = U(R), H^0(H, \text{Pic}) = \text{Ker}(d_0) = \text{Pic}(R) \).
Next, we proceed toward the definition of groups $H^n(H)$ parallel with Hattori [6],[7]. Let $\text{Pic}(H^n)$ be the category of projective $H^n$-modules of rank $1(n=0,1,\cdots)$. This is a category with product $\otimes_H$. In this Appendix, $P^*$ denotes the $H^n$-dual module of $P \in \text{Pic}(H^n)$ unless otherwise stated. Hence $P^* \in \text{Pic}(H^n)$.

Similar to the case of $\text{Pic}$-valued cohomology groups, $\Delta^i: H^n \to H^{n+1}$ yields the functor $\Delta^i: \text{Pic}(H^n) \to \text{Pic}(H^{n+1})$. Hence we also define $d_\ast: \text{Pic}(H^n) \to \text{Pic}(H^{n+1})$ as the alternate sum of $\Delta^i$. Let $f: P \cong Q$ be an isomorphism in $\text{Pic}(H^n)$ and let $\Delta^i f: \Delta^i P \cong \Delta^i Q$, $\Delta^i f^*: \Delta^i P^* \cong \Delta^i Q^*$ be the canonical isomorphism induced from $f$, then $d_\ast f$ is defined as $\Delta^i f \otimes \Delta^i f^* \otimes \cdots$.

There exists a canonical isomorphism $I_{n+1}: dH^n \cong H^{n+1}$, through which we identify $dH^n$ with $H^{n+1}$. We also identify $d^2 H^n$ with $H^{n+2}$ through the composite of the canonical isomorphisms $d^2 H^n \cong dH^{n+1} \cong H^{n+2}$. For any $P \in \text{Pic}(H^n)$, we have a canonical isomorphism $d^2 P \cong H^{n+2}$ given by contracting all dual pairs appearing in the expression of $d^2 P$. This isomorphism $d^2 P \cong H^{n+2}$ will be written as $c_P$ in the sequel. For $f: P \cong Q$, the following diagram is commutative:

$$
\begin{array}{ccc}
\text{d}^2 P & \xrightarrow{c_P} & H^{n+2} \\
\text{d}^2 f & \downarrow & \downarrow \\
\text{d}^2 Q & \xrightarrow{c_Q} & H^{n+2} \\
\text{d}I_{n+1} & \xrightarrow{I_{n+2}} & I_{n+2}
\end{array}
$$

In particular, the composite $d^2 H^n \cong dH^{n+1} \cong H^{n+2}$ (through which we identified $d^2 H^n$ with $H^{n+2}$) coincides with $c_H$: $d^2 H^n \cong H^{n+2}$. An automorphism of $P \in \text{Pic}(H^n)$ is given by a unit $u \in H^n$ by homothety, which we shall denote by the same letter $u$. For $P \in \text{Pic}(H^n)$, we shall denote the isomorphism class of $P$ by $\lvert P \rvert \in \text{Pic}(H^n)$.

Let $\lvert P \rvert \geq 1$, $(P, p)$ denotes a pair of a module $P \in \text{Pic}(H^{n+1})$ such that $\lvert P \rvert$ is a $\text{Pic}$-valued $n$-1-cocycle and a cocycle condition isomorphism $p: dP \cong H^n$. An isomorphism $(P, p) \cong (P', p')$ is an isomorphism $f: P \cong P'$ such that the following diagram commutes:

$$
\begin{array}{ccc}
dP & \xrightarrow{\text{p}} & H^n \\
\text{df} & \downarrow & \downarrow \\
dP' & \xrightarrow{\text{p'}} & H^n
\end{array}
$$

We shall denote the category of these pairs and isomorphisms $P^u(H)$. This is a category with product defined naturally by

$$(P, p) \cdot (Q, q) = (P \otimes_H H^{-1} Q, p \otimes_H q)$$

The set of isomorphism classes $\lvert (P, p) \rvert$ of $(P, p) \in P^u(H)$ forms an abelian
THE COHOMOLOGICAL ASPECTS OF HOPF GALOIS EXTENSIONS

91

group, which we shall write \( P^n(H) \). We shall denote by \( Z^n(H) \) the subgroup of \( P^n(H) \) consisting of all \(|(P, p)| \) satisfying \( dp = c_p \), and by \( B^n(H) \) the set of all \(|(dP, c_p)| \) \((P \in \text{Pic}(H^n))\). For \( n = 1 \), we shall put \( B^1(H) = \{|(R, I)|\} \).

Since \( dc_p = c_{dP} \), \( B^n(H) \) is a subgroup of \( Z^n(H) \) and we have the groups

\[
H^n(H) = Z^n(H)/B^n(H)
\]

for \( n = 0 \), we put \( Z^0(H) = \{u \in U(R) | d_0 u = 1\} \), and \( B^0(H) = \{1\} \). Since \( d_0 \) is a zero-homomorphism, this means \( H^0(H) = H^0(H, U) = U(R) \).

Every \( u \in U(H^n) \) determines a pair \((H^{n-1}, u)\) where \( u: dH^{n-1} = H^n \to H^n \) and \(|(H^{n-1}, u)| \in Z^n(H) \) if and only if \( u \) is a unit-valued \( n \)-cocycle. If \( u \) is a coboundary, \((H^{n-1}, u) \cong (H^{n-1}, 1)\). Thus we have a homomorphism \((n \geq 1)\),

\[
\alpha^n: H^n(H, U) \to H^n(H); cl(u) \mapsto cl|(H^{n-1}, u)|.
\]

For \( n = 0 \), \( \alpha^0 \) is defined to the identity map \( H^0(H, U) = H^0(H) \).

The definability of the following map is clear \((n \geq 1)\),

\[
\beta^n: H^*(H) \to H^{*+1}(H, \text{Pic}); cl|(P, p)| \mapsto cl|P|.
\]

Let \(|P|\) be a Pic-valued \( n \)-1-cocycle and take any cocycle condition isomorphism \( p: dP \cong H^* \). There exists a unit \( u \in H^{n+1} \) such that the following diagram is commutative.

\[
\begin{array}{ccc}
d^2P & \xrightarrow{c_p} & H^{n+1} \\
\downarrow & & \downarrow u \\
d^2P & \xrightarrow{dp} & H^{n+1}
\end{array}
\]

And we see easily that \( u \) is a unit-valued \( n + 1 \)-cocycle. The cohomology class of \( u \) does not change, even if we change \( P \) to an isomorphic module \( P' \) or \( p \) to another cocycle condition isomorphism \( p' \). If \(|P|\) is a coboundary \(|dQ|\), taking \( c_0: dP = d^2Q \cong H^* \)
as a cocycle condition isomorphism. Then \( dc_0 = c_{dP} \) claims that \( u = 1 \). Hence we have the following homomorphism.

\[
\gamma^n: H^{n-1}(H, \text{Pic}) \to H^{n+1}(H, U); cl|(P, p)| \mapsto cl(u).
\]

**Theorem A.1.** The following sequence is exact:

\[
0 \to H^1(H, U) \xrightarrow{\alpha^1} H^1(H) \xrightarrow{\beta^1} H^0(H, \text{Pic}) \xrightarrow{\gamma^1} \cdots \to H^n(H, U) \xrightarrow{\alpha^n} H^n(H) \xrightarrow{\beta^n} H^{n-1}(H, \text{Pic}) \xrightarrow{\gamma^n} \cdots
\]

**Proof.** Let \( n > 1 \), it is easily verified from the definition of maps that the
composite of any consecutive maps reduces to 0. Let \( cl(P, p) \in \text{Ker}(\beta^n) \). We may assume that \( P=dQ \) with some \( Q \in \text{Pic}(H^{n-2}) \). Then there exists \( u \in U(H^n) \) such that \( p=uc_0 \) and it must satisfy \( du=1 \). Since we have

\[
(dQ, p) = (dQ, c_0) \cdot (H^n, u), \quad (dQ, c_0) \in B^n(H),
\]

\[
cl(P, p) = cl((dQ, p)) \in \text{Im}(\alpha^n).
\]

If \( cl(P) \in \text{Ker}(\gamma^n) \), we have \( dp=c_P \) with a suitably chosen \( p : dP \cong H^n \). This means that \( cl(P) \in \text{Im}(\beta^n) \). If \( cl(u) \in \text{Ker}(\alpha^{n+1}) \), there exists \( P \in \text{Pic}(H^{n-1}) \) such that \((H^n, u) \cong (dP, c_P)\). This means that there exists \( p : dP \cong H^n \) satisfying \( c_P = udp \). Hence \( u^{-1} \in \text{Im}(\gamma^n) \), and therefore \( u \in \text{Im}(\gamma^n) \).

The definitions of \( H^1(H) \) and \( H^0(H, \text{Pic}) \) are slightly different to the case of \( n>1 \). But the above arguments will give the proof of the case \( n=1 \), if we are careful. This completes the proof.

Well, in our case of Harrison cohomology, those which \( H^0(H), H^*(H, U) \) and \( H^*(H, \text{Pic}) \) represent are different from Hattori's by their own characters. For example, \( H^0(R)=H^1(H, U)=U(R), \ H^0(H, \text{Pic})=\text{Pic}(R), \ H^1(H, U)=\{u \in U(H) | \delta(u)=u \otimes u\} \) is the group of group-like units of \( H \), by Corollary 4.5 \( H^2(H, U) \) represents the group of isomorphism classes of \( H \)-Hopf Galois extensions of \( R \) with a dual normal basis. Further as is easily verified, \( \beta^1 \) is an epimorphism. Thus we get

**Corollary A.2.** The following sequences are exact;

\[
0 \to H^1(H, U) \xrightarrow{\alpha^1} H^1(H) \xrightarrow{\beta^1} \text{Pic}(R) \to 0, \\
0 \to H^2(H, U) \xrightarrow{\alpha^2} H^2(H) \xrightarrow{\beta^2} H^1(H, \text{Pic}) \xrightarrow{\gamma^2} H^3(H, U) \xrightarrow{\alpha^3} \ldots
\]

Let \( cl((P, p)) \in H^3(H) \), this means that \( P \) is a rank 1-projective \( H \)-module and that \( dP=(P \otimes P) \otimes_H (H \otimes H) \otimes_H P^* \cong H^2 \) satisfying \( c_P = dp \). From \( p \) we make \( \bar{p} : P \otimes P \cong H^2 \otimes_P P \) naturally, then \( c_P = dp \) means \( u(P, \bar{p}) = 1 \otimes 1 \otimes 1 \in H^3 \). And \((P, p) \equiv (P', p') \) means that there exists a unit \( w \in H \) which makes the following diagram commutative;

\[
\begin{array}{ccc}
dP & \xrightarrow{p} & H^* \\
\downarrow{dw} & & \downarrow \\
dP' & \xrightarrow{p'} & H^*
\end{array}
\]

Thus \((P, p) \equiv (P', p') \) means \( u(P, \bar{p}) = dw \cdot \bar{p} \cdot u(P', \bar{p}') \). From Theorem 3.2, 3.5, we get

**Theorem A.3.** \( H^2(H) \) represents the group of isomorphism classes of \( H-\)}
Hopf Galois extensions of \( R \).

References


Department of Mathematics
Faculty of Science
Nara Women's University
Nara 630, Japan