The cohomological aspect of Hopf Galois extensions over a commutative ring

Kenji Yokogawa

The cohomological aspect of Hopf Galois extensions over a commutative ring

Kenji Yokogawa

(Recieved)

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 "normal basis theorem" and combined with the theory of Galois algebras[8],[9]. But normal basis theorem heavily depends on the RG-isomorphism $\mathrm{Hom}_R(RG, R) \cong RG$. Therefore, in considering Hopf Galois extensions, the corresponding notion would be the dual normal basis theorem— an H-Hopf Galois extension is isomorphic to $H^* = \mathrm{Hom}_R(H, R)$ as H-modules — of course this does not always hold. We shall call such one a Hopf Galois extension with dual normal basis. On the other hand, A.Nakajima[12],[13] examined the 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 the H-module structure of Hopf Galois extensions and then shall establish the 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 the cohomological nature. In §1, we shall prove that an H-Hopf Galois extension A has a decom-

position $A \cong H^* \otimes_H P$ as left H-modules with a rank 1 H-projective module P satisfying some cohomological properties. In §2, we deal with the 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 the 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 $\text{Ш}^n(H)$ related to the generalized Harrison cohomology groups. Also we show that $\text{Ш}^2(H)$ is isomorphic to the group of isomorphism classes of H-Hopf Galois extensins of R using the results of previous sections.

Througout this paper, R will denote a commutative ring with identity and H will be a finite co-commutative Hopf algebra over R. ε (resp. Δ resp. S) will denote the augumentation (resp. diagonalization resp. antipode) of H. Unadorned $\otimes$ and Hom will mean $\otimes_R$ and Hom_R. We shall denote by $-^*$ the functor $\mathrm{Hom}_R(-, R)$. We shall deal with the various H-modules, H-H -bimodules, etc., so to indicate the module structure, we shall use the index notation. For instance, ${}_{H_1}\mathrm{Hom}({}_{H_2}H_{H_1}, R)_{H_2} \otimes_{H_2} {}_{H_2}P$ means that $\mathrm{Hom}(H, R)$ is an H_1-$H_2 = H$-H -bimodule by $(h_1 f h_2)(x) = f(h_2 x h_1)$, $h_1, h_2, x \in H$, $f \in \mathrm{Hom}(H, R)$ and the tensor product is taken with the right $H_2 = H$ -module $\mathrm{Hom}(H, R)$ and the left $H_2 = H$ -module P over $H_2 = H$. 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].

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 ρ : $H \otimes A \longrightarrow A$ with the properties;

$\rho(h \otimes ab) = \sum_{(h)} \rho(h_{(1)} \otimes a)\rho(h_{(2)} \otimes b)$

$\rho(h \otimes 1) = \varepsilon(h)$, ε is an augumentation (if A has an identity)

$\rho(gh \otimes a) = \rho(g \otimes \rho(h \otimes a))$, $g,h \in H$, $a,b \in A$.

$\rho(h \otimes a)$ is denoted by $h \cdot a$ or simply by ha.

A is called an H-Hopf Galois extension of R if $A^H = \{ a \in A \mid h \cdot a = \varepsilon(h)a$ for any $h \in H \}$ is equal to R and the homomorphism $\phi : A \otimes A \longrightarrow \mathrm{Hom}(H, A)$ 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 ϕ 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 ${}_H\mathrm{Hom}({}_H H, R)$ (resp. $\mathrm{Hom}(H_H, R)_H$)), the isomorphism ${}_H H^* \cong I \otimes {}_H H$ (resp. $H^*_H \cong I' \otimes H_H$) 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.

$$(\#)\begin{cases} H^* = {}_{H_1}\mathrm{Hom}({}_{H_2}H_{H_1}, R)_{H_2} \cong I \otimes {}_{H_1}H_{H_2} & \text{as } H_1\text{-}H_2 = \\ H\text{-}H \text{ -bimodules with } \overset{(a)}{\text{rank}} 1 \text{ R-projective module } I. \end{cases}$$

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 ${}_{H_1}H^*_{H_2} \otimes_{H_2} {}_{H_2}P$ as left H_1= H-modules.

Proof. Let Ω be $\mathrm{Hom}_{H_1}({}H^*_{H_1}, {}H^*_{H_1})$, then Ω is isomorphic to H by homothety. And by this isomorphism ${}_{\Omega}H^*$ coincides with the original ${}_{H}H^*$. Since H^* is a right H-progenerator, we get by Morita theory ${}_{H_1}A \cong {}_{H_1}H^*_{H_2} \otimes_{H_2} \mathrm{Hom}_{H_3}({}_{H_3}H^*_{H_2}, {}_{H_3}A)$ and $\mathrm{Hom}_{H_3}({}_{H_3}H^*_{H_2}, {}_{H_3}A) = P$ 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 ${}_{H_1}A \cong {}_{H_1}H^*_{H_2} \otimes_{H_2} {}_{H_2}P$ of Proposition 1.1, P is a finitely generated faithful projective H-module.

Proof. Since the Hopf Galois extension A of R is a left H-progenerator ([15] Cor.1.4.), $P = {}_{H_1}\mathrm{Hom}_{H_2}({}_{H_2}H^*_{H_1}, {}_{H_2}A)$ 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

$$\phi : A \otimes A \cong \mathrm{Hom}(H, A).$$

Hence the left H-module P of the decomposition $A \cong H^* \otimes_H P$

must satisfy some relations, which we next investigate.

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

$$[(g \otimes h)f](x) = \sum_{(g)} g_{(1)} \cdot f(S(g_{(2)})xh)$$

$$(g \otimes h)(p \otimes x) = \sum_{(g)} g_{(1)}p \otimes hxS(g_{(2)})$$

$g,h,x \in H$, $f \in \mathrm{Hom}(H, A)$, $p \in P$, S is an antipode of H. Then ${}_{H_1}A \otimes {}_{H_2}A$ is $H \otimes H$-isomorphic to $\mathrm{Hom}(H, A)$, 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, $\mathrm{Hom}(H, A)$ is $H \otimes H$-isomorphic to $I \otimes I \otimes P \otimes H$ through the isomorphisms $\mathrm{Hom}(H, A) \cong \mathrm{Hom}(H, H^* \otimes_H P) \cong (H^* \otimes_H P) \otimes H^* \cong ((I \otimes H) \otimes_H P) \otimes (I \otimes H) \cong I \otimes I \otimes P \otimes H$. Thus $A \otimes A \cong \mathrm{Hom}(H, A)$, 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 $\mathrm{Hom}(H, A)$ in Proposition 1.3 is the one induced from that of $A \otimes A$ through the fundamental isomorphism ϕ. As to that of $P \otimes H$, we have

Proposition 1.4. $P \otimes H$ with the given $H \otimes H$-module structure in Proposition 1.3 is $H \otimes H$-isomorphic to $({}_{H_1}H \otimes {}_{H_2}H) \otimes_H P$,

where we consider $H \otimes H$ as a right H-module by the diagonalization $\Delta : H \longrightarrow H \otimes H$.

Proof. We consider the homomorphisms $\alpha, \beta : P \otimes H \underset{\beta}{\overset{\alpha}{\rightleftarrows}} (H \otimes H) \otimes_H P$ defined by $\alpha(p \otimes h) = (1 \otimes h) \otimes p$, $\beta((g \otimes h) \otimes p) = \sum_{(g)} g_{(1)}p \otimes hS(g_{(2)})$, $g,h \in H, p \in P$. As easily checked, α and β 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 $(H \otimes H) \overset{\Delta}{\otimes}_H P$. Also if Q is a left H-module and $H \otimes H$ is regarded as a right H-module via $\Delta : H \longrightarrow H \otimes H$, then the tensor product $Q \otimes_H (H \otimes H)$ will be denoted as $Q \overset{\Delta}{\otimes}_H (H \otimes H)$. 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 $A \cong H^* \otimes_H P$ and there exists the $H \otimes H$-isomorphism $\tilde{\phi}: P \otimes P \cong (H \otimes H) \overset{\Delta}{\otimes}_H P$. 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 $P \otimes P \cong (H \otimes H) \overset{\Delta}{\otimes}_H P$ 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 $m: A \otimes A \longrightarrow A$ is a left H-homomorphism (regarding $A \otimes A$ as a left H-module via Δ) and $A \cong H^*$, passing to dual we get the right H-homomorphism $m^* : H \longrightarrow H \otimes H$. m^* is uniquely determined by $m^*(1) \in H \otimes H$, hence A is determined by $m^*(1)$. Conversely, from $v = \sum_i v_{1_i} \otimes v_{2_i} \in H \otimes H$, 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 $(f \cdot g)(x) = \sum_{i,(x)} f(v_{1_i} x_{(1)}) g(v_{2_i} x_{(2)})$, $f,g \in H^*$, $x \in H$. As easily proved, $H^*(v)$ is an H-module algebra. Thus $A = H^*(m^*(1))$ in this sense.

Since A is an assoiative algebra, the following diagram commutes.

(2.1)
$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{m \otimes 1} & A \otimes A \\ \downarrow{\scriptstyle 1 \otimes m} & & \downarrow{\scriptstyle m} \\ A \otimes A & \xrightarrow{\quad m \quad} & A \end{array}$$

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

(2.2)
$$\begin{array}{ccc} H \otimes H \otimes H & \xleftarrow{m^* \otimes 1} & H \otimes H \\ \uparrow{\scriptstyle 1 \otimes m^*} & & \uparrow{\scriptstyle m^*} \\ H \otimes H & \xleftarrow{\quad m^* \quad} & H \end{array}$$

Now we define the algebra homomorphisms $\Delta_i^2 : H \otimes H \longrightarrow H \otimes H \otimes H$ ($i = 0,1,2,3$) by $\Delta_0^2(v) = 1 \otimes v$, $\Delta_1^2(v) = (\Delta \otimes 1)(v)$ $\Delta_2^2(v) = (1 \otimes \Delta)(v)$, $\Delta_3^2(v) = v \otimes 1$, $v \in H \otimes H$.

Then the commutativity of (2,2) means $\Delta_0^2(m^*(1))\Delta_2^2(m^*(1)) = \Delta_3^2(m^*(1))\Delta_1^2(m^*(1))$. 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 $\Delta_0^2(v)\Delta_2^2(v) = \Delta_3^2(v)\Delta_1^2(v)$.

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 $v = \sum_i v_{1_i} \otimes v_{2_i} \in H \otimes H$, the following diagram is commutative.

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

where $H \otimes H$ is regarded as a left H-module via Δ, and the homomorphisms are defined by $[[\phi'(f \otimes g)](x \otimes y)](z) = \sum_{i,(z)} f(v_{1_i} z_{(1)} x)g(v_{2_i} z_{(2)} y)$, $[\theta(\tau)](x \otimes (y \otimes z)) = [\tau(y \otimes z)](x)$, $[v^*(f \otimes g)](x \otimes y) = \sum_i f(v_{1_i} x)g(v_{2_i} y)$, $f,g \in H^*(v) = H^*$, $\tau \in \mathrm{Hom}_H(H \otimes H, H^*(v))$, $x,y,z, \in H$, 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, $\Delta_0^2(v)\Delta_2^2(v) =$

$\Delta_3^2(v)\Delta_1^2(v)$ and v is a unit of $H \otimes H$.

Proof. Let α, β be the homomorphisms $\mathrm{Hom}_H(H \otimes H, H^*(v)) \underset{\beta}{\overset{\alpha}{\rightleftarrows}} \mathrm{Hom}(H, H^*(v))$ defined by $[\alpha(g)](x) = g(1 \otimes x)$, $[\beta(f)](x \otimes y) = \sum_{(x)} x_{(1)} f(S(x_{(2)})y)$, $g \in \mathrm{Hom}_H(H \otimes H, H^*(v))$, $f \in \mathrm{Hom}(H, H^*(v))$, $x, y \in H$. α and β are well-defined homomorphisms and are inverse to each other. The commutativity of the following diagram is easily proved.

$$\begin{array}{ccc} H^*(v) \otimes H^*(v) & \xrightarrow{\quad\phi'\quad} & \mathrm{Hom}_H(H \otimes H, H^*(v)) \\ & {\scriptstyle\phi}\searrow \quad \swarrow{\scriptstyle\beta} \; {\scriptstyle\alpha}\swarrow & \\ & \mathrm{Hom}(H, H^*(v)) & \end{array}$$

where ϕ' is the homomorphism (defined) in Lemma 2.2 and ϕ is the fundamental homomorphism of the H-module algebra $H^*(v)$. Thus, if $A = H^*(v)$ is an H-Hopf Galois extension of R, then ϕ, so ϕ' is an isomorphism. By Lemma 2.2, this claims that v^* is an isomorphism, hence that v is a unit. Conversely we assume that $v = \sum_i v_{1_i} \otimes v_{2_i}$ is a unit and $\Delta_0^2(v)\Delta_2^2(v) = \Delta_3^2(v)\Delta_1^2(v)$. Then $H^*(v)$ is an associative H-module algebra and by the above arguments, ϕ 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 $1 \otimes \varepsilon \otimes 1$ on the both sides of $\Delta_0^2(v)\Delta_2^2(v) = \Delta_3^2(v)\Delta_1^2(v)$ and then cancel v. We get $\sum_i 1 \otimes \varepsilon(v_{1_i})v_{2_i} = \sum_i v_{1_i} \otimes \varepsilon(v_{2_i})$. Further applying $1 \otimes \varepsilon$ and $\varepsilon \otimes 1$ on both sides, we get

$$(2.3) \quad \sum_i \varepsilon(v_{1_i} v_{2_i}) = \sum_i v_{1_i} \varepsilon(v_{2_i})$$

$$(2.4) \quad \sum_i \varepsilon(v_{1_i})v_{2_i} = \sum_i \varepsilon(v_{1_i} v_{2_i})$$

We shall put $e = \varepsilon((\sum_i v_{1_i} v_{2_i})^{-1})\varepsilon \in H^* = H^*(v)$. Then for any $f \in H^*(v)$ and for any $x \in H$, we have

$$
\begin{aligned}
(f \cdot e)(x) &= \sum_{(x),j} f(v_{1_j} x_{(1)}) e(v_{2_j} x_{(2)}) \\
&= \sum_{(x),i,j} f(v_{1_j} x_{(1)}) \varepsilon((\sum_i v_{1_i} v_{2_i})^{-1}) \varepsilon(v_{2_j} x_{(2)}) \\
&= \sum_j f(v_{1_j} \varepsilon(v_{2_j}) \varepsilon((\sum_i v_{1_i} v_{2_i})^{-1}) x),
\end{aligned}
$$

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 $x \in H$, $xe = \varepsilon(x)e$ 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

$$\begin{array}{ccc} H^*(v) \otimes H^*(v) & \xrightarrow{\eta \otimes \eta} & H^*(v') \otimes H^*(v') \\ \downarrow \text{multi.} & & \downarrow \text{multi.} \\ H^*(v) & \xrightarrow{\eta} & H^*(v') \end{array} \tag{2.5}$$

is equivalent to the commutativity of the diagram

$$\begin{array}{ccc} (H^*(v))^* \otimes (H^*(v))^* & \xrightarrow{\eta^* \otimes \eta^*} & (H^*(v'))^* \otimes (H^*(v'))^* \\ \downarrow \ell(v) & & \downarrow \ell(v') \\ H = (H^*(v))^* & \xrightarrow{\eta^*} & (H^*(v'))^* = H \end{array} \tag{2.6}$$

where $[\ell(v)](x) = v\Delta(x)$, $[\ell(v')](x) = v'\Delta(x)$, $x \in H$. Since $[\ell(v)\eta^*](1) = v\Delta(w)$ and $[\eta^* \otimes \eta^* \ell(v')](1) = (w \otimes w)v'$, 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 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 $\phi : P \otimes P \cong (H \otimes H) \overset{\Delta}{\otimes}_H P$. If H is commutative such (P,ϕ) is a Pic-valued 1-cocycle. By abuse the language, we shall call such (P,ϕ) a Pic-valued 1-cocycle even if H is not commutative.

Let (P,ϕ) be a Pic-valued 1-cocycle. Then we have a chain of isomorphisms ; $P \otimes P \otimes P \overset{1\otimes\phi}{\cong} P \otimes ((H \otimes H) \overset{\Delta}{\otimes}_H P)$ $= H^3\, 1 \overset{\Delta}{\underset{H^2}{\otimes}} (P \otimes P) \overset{1\otimes\phi}{\cong} H^3\, 1 \overset{\Delta}{\underset{H^2}{\otimes}} ((H \otimes H) \overset{\Delta}{\otimes}_H P) =$ $H^3 (1 \overset{\Delta}{\otimes}_H)\Delta P = H^3 (\Delta \overset{1}{\otimes}_H)\Delta P \overset{1\otimes\phi^{-1}}{\cong} H^3\, \Delta \overset{1}{\underset{H^2}{\otimes}} (P \otimes P)$ $= ((H \otimes H) \overset{\Delta}{\otimes}_H P) \otimes P \overset{\phi^{-1}\otimes 1}{\cong} P \otimes P \otimes P.$

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, ϕ) and a unit v of H^2, 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,ϕ) be a Pic-valued 1-cocycle , then $A = H^* \otimes_H P$ 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 ϕ be the fundamental isomorphism $A \otimes A \cong \mathrm{Hom}(H, A)$. Then we have the H^2-isomorphism $\tilde{\phi}' : P \otimes P \cong H^2 \overset{\Delta}{\otimes}_H P$ by Theorem 1.5. $\tilde{\phi}'$ may differ from the given $\tilde{\phi}$, but Lemma 3.1 ensures that the differnce between $u(P, \tilde{\phi}')$ and $u(P, \tilde{\phi})$ is a 3-coboundary. So we may assume $\tilde{\phi}' = \tilde{\phi}$ and we have the following commutative diagram.

(3.1)
$$\begin{array}{ccc}
A \otimes A & \xrightarrow{\quad\phi\quad} & \mathrm{Hom}(H, A) \\
\| & & \| \text{ can.} \\
 & & (H^* \otimes_H P) \otimes H^* \\
(H^* \otimes_H P) \otimes (H^* \otimes_H P) & & \| \text{ can.} \\
\| \text{ can.} & & I \otimes I \otimes P \otimes H \\
 & & \| \text{ by Prop. 1.4.} \\
I \otimes I \otimes P \otimes P & \xrightarrow{1 \otimes 1 \otimes \tilde{\phi}} & I \otimes I \otimes (H^2 \overset{\Delta}{\otimes}_H P)
\end{array}$$

We shall show that $u(P, \tilde{\phi}) = 1 \otimes 1 \otimes 1 \in H^3$. 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) ;

(3.2)
$$\begin{array}{ccc}
(He \otimes_H P) \otimes (He \otimes_H P) & \xrightarrow{\quad\phi\quad} & \mathrm{Hom}(H, He \otimes_H P) \\
\| & & \uparrow \alpha \\
(He \otimes He) \otimes_{H^2} (P \otimes P) & \xrightarrow{1 \otimes \tilde{\phi}} & (He \otimes He) \overset{\Delta}{\otimes}_H P
\end{array}$$

(3.3)
$$\begin{array}{ccccc}
(He \otimes He \otimes He) \otimes_{H^3} (P \otimes P \otimes P) & = & (He \otimes_H P) \otimes (He \otimes_H P) \otimes (He \otimes_H P) & & \\
\downarrow 1 \otimes (1 \otimes \tilde{\phi}) & & & \downarrow \gamma & \\
(He \otimes_H P) \otimes ((He \otimes He) \overset{\Delta}{\otimes}_H P) & & & \mathrm{Hom}(H \otimes H, He \otimes_H P) & \\
\| & & & \uparrow \beta & \\
(He \otimes He \otimes He) \underset{H^2}{\otimes} (P \otimes P) & \xrightarrow{1 \otimes \tilde{\phi}} & (He \otimes He \otimes He) & & (1 \otimes \Delta)\Delta \underset{H}{\otimes} P
\end{array}$$

$$
\begin{array}{ccc}
(He \otimes He \otimes He) \otimes_{H^3} (P \otimes P \otimes P) & = & (He \otimes_H P) \otimes (He \otimes_H P) \otimes (He \otimes_H P) \\
\downarrow 1 \otimes (\tilde{\phi} \otimes 1) & & \downarrow \gamma \\
((He \otimes He) \overset{\Delta}{\otimes}_H P) \otimes (He \otimes_H P) & & Hom(H \otimes H, He \otimes_H P) \\
\| & & \uparrow \beta \\
(He \otimes He \otimes He) \underset{H^2}{\otimes} (P \otimes P) & \xrightarrow{\Delta \otimes 1 \quad 1 \otimes \tilde{\phi}} & (He \otimes He \otimes He) \underset{H}{\otimes} (\Delta \otimes 1)\Delta P
\end{array}
\tag{3.4}
$$

where α is defined by $[\alpha((xe \otimes ye) \otimes p)](h) = \sum_{(x)} e \otimes e(hyS(x_{(2)}))x_{(1)}p$, β is defined by $\beta[(xe \otimes ye \otimes ze) \otimes p](g \otimes h) = \sum_{(x),(y)} e \otimes e(gy_{(1)}S(x_{(2)}))e(hzS(y_{(2)}))x_{(1)}p$, γ is defined by $[\gamma((e \otimes p_1) \otimes (e \otimes p_2) \otimes (e \otimes p_3))](g \otimes h) = (e \otimes p_1) \cdot g((e \otimes p_2) \cdot h(e \otimes p_3))$ (product in $He \otimes_H P = H^* \otimes_H P$), $p, p_1, p_2, p_3 \in P$, $x, y, z, g, h \in H$.

(3.2) is a localized diagram of (3.1) and by the similar methods to Proposition 1.3, 1.4, β is a well-defined isomorphism. We shall compute $\beta \cdot (1 \otimes \tilde{\phi}) \cdot (1 \otimes (1 \otimes \tilde{\phi}))$. For $(e \otimes p_1) \otimes (e \otimes p_2) \otimes (e \otimes p_3) \in (He \otimes_H P) \otimes (He \otimes_H P) \otimes (He \otimes_H P)$, we shall put $\tilde{\phi}(p_2 \otimes p_3) = \sum_i (1 \otimes p'_{2_i}) \otimes p'_{3_i} \in H^2 \overset{\Delta}{\otimes}_H P$ (we may assume that the first term of H^2 is 1 by Proposition 1.4) and we shall put $\tilde{\phi}(p_1 \otimes p'_{3_i}) = \sum_j (1 \otimes p'_{1_j}) \otimes p''_{3_{ij}} \in H^2 \overset{\Delta}{\otimes}_H P$. Then from the commutativity of (3.2), we get

$$(e \otimes p_2) \cdot (e \otimes hp_3) = \sum_i e \otimes e(hp'_{2_i})p'_{3_i}, \quad h \in H. \tag{3.5}$$

$$(e \otimes p_1) \cdot (e \otimes hp'_{3_i}) = \sum_j e \otimes e(hp'_{1_j})p''_{3_{ij}}, \quad h \in H. \tag{3.6}$$

Since $\tilde{\phi}$ is an H^2-isomorphism, $\tilde{\phi}(\sum_{(g)} g_{(1)}p_2 \otimes g_{(2)}hp_3) = \sum_{(g),i} (g_{(1)} \otimes g_{(2)}hp'_{2_i}) \otimes p'_{3_i}$, which is equal to $\sum_{(g),i} (1 \otimes g_{(1)}hp'_{2_i}S(g_{(2)})) \otimes g_{(3)}p'_{3_i}$, $g \in H$. e is a basis of H^* as an H-H -bimodule , so $e(gh) = (eg)(h) = (ge)(h) = e(hg)$ for any $g, h \in H$. Thus we get for $g \in H$, $r \in R$;

$$(3.5)' \quad \sum_{(g)} (e \otimes g_{(1)}p_2)\cdot(e \otimes g_{(2)}hp_3) = \sum_{i,(g)} e \otimes e(g_{(1)}hp'_{2_i}S(g_{(2)}))g_{(3)}p'_{3_i} = \sum_i e \otimes e(hp'_{2_i})gp'_{3_i}.$$

$$(3.6)' \quad (e \otimes p_1)\cdot(e \otimes hrp'_{3_i}) = \sum_j e \otimes re(hp'_{1_j})p''_{3_{ij}}.$$

Thus $[(\beta\cdot(1 \otimes \phi)\cdot(1 \otimes (1 \otimes \phi)))((e \otimes p_1)\otimes(e \otimes p_2)\otimes(e \otimes p_3))](g \otimes h)$

$$= [\beta(\sum_{i,j,(p'_{1_j})} (1 \otimes p'_{1_{j(1)}} \otimes p'_{2_i}p'_{1_{j(2)}}) \otimes p''_{3_{ij}})](g \otimes h)$$

$$= \sum_{i,j,(p'_{1_j})} e \otimes e(gp'_{1_{j(1)}})e(hp'_{2_i}p'_{1_{j(2)}}S(p'_{1_{j(3)}}))p''_{3_{ij}}$$

$$= \sum_{i,j} e \otimes e(gp'_{1_j})e(hp'_{2_i})p''_{3_{ij}}.$$

By (3.5)' and (3.6)', this is equal to

$$\sum_i (e \otimes p_1)\cdot(e \otimes e(hp'_{2_i})gp'_{3_i})$$

$$= (e \otimes p_1)\cdot(\sum_{(g)} (e \otimes g_{(1)}p_2)\cdot(e \otimes g_{(2)}hp_3)$$

$$= (e \otimes p_1)\cdot(g((e \otimes p_2)\cdot h(e \otimes p_3))).$$

Similarly, $[(\beta\cdot(1 \otimes \phi)\cdot(1 \otimes (\phi \otimes 1)))((e \otimes p_1) \otimes (e \otimes p_2) \otimes (e \otimes p_3))](g \otimes h) = \sum_{(g)} ((e \otimes p_1)\cdot(e \otimes g_{(1)}p_2))\cdot(e \otimes g_{(2)}hp_3)$.

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, ϕ) be a Pic-valued 1-cocycle and assume that $u(P, \phi)$ is a unit-valued 3-coboundary. We may alter ϕ 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 $A = H^* \otimes_H P$, $H^* = I \otimes H$. From ϕ, we make $\phi : A \otimes A \cong \mathrm{Hom}(H, A)$ 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 ϕ. Only the existence of identity is not yet valid. We make the 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 $a \# g \cdot b \# h = \sum_{(g)} ag_{(1)}b \# g_{(2)}h$, $a,b \in A$, $g,h \in H$) and consider the homomorphism $\mu : A \# H \to \mathrm{Hom}(A, A)$ defined by $[\mu(a \# h)](b) = ah \cdot b$. Locally A is an associative H-module algebra with $\overset{a}{)}$dual normal basis, hence by Proposition 2.1 $A = H^*(v)$. From the proof of Theorem 2.3, that ϕ 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 μ is an isomorphism locally (c.f.[15] Theorem 1.1), so globally. Let $\mu(\sum_i a_i \# h_i)$ be an identity of $\mathrm{Hom}(A, A)$. 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, ϕ) be a Pic-valued 1-cocycle. From the above proof, if $A = H^* \otimes_H P$ has a structure of an H-Hopf Galois extension of R, then we can chose the cocycle condition isomorphism ϕ 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 $A = H^* \otimes_H P$ 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 ϕ : $A \otimes A \cong \mathrm{Hom}(H, A)$. 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 $A = H^* \otimes_H P$ be an H-Hopf Galois extension of R. Then we can chose an H^2-isomorphism $\tilde{\phi} : (H \otimes H) \overset{\Delta}{\otimes}_H P$ to satisfy that $u(P, \tilde{\phi})$ is an identity automorphism of $P \otimes P \otimes P$. Conversely, let $(P, \tilde{\phi})$ be a Pic-valued 1-cocycle and assume that $u(P, \tilde{\phi})$ is an identity automorphism of $P \otimes P \otimes P$. Then $A = H^* \otimes_H P$ has a structure of an H-Hopf Galois extension of R.

Proof. Only the existence of an identity of $A = H^* \otimes_H P$ should be proved. We make the smash product $A \# H$ and consider the homomorphism $\mu : A \# H \to \mathrm{Hom}(A, A)$ as the proof of Theorem 3.2. We shall show that μ 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 $\mathrm{Hom}(A, A)$ are finitely generated projective R-modules. From $\tilde{\phi}$, we have the isomorphism ϕ: $(He \otimes_H P) \otimes (He \otimes_H P) \cong \mathrm{Hom}(H, He \otimes_H P)$, where e is a basis of H^*. We shall regard $(He \otimes_H P) \otimes (He \otimes_H P)$ as a left H-module via the second term and regard $\mathrm{Hom}(H, He \otimes_H P)$ as a left H-module by ${}_H\mathrm{Hom}({}_HH, He \otimes_H P)$. Then ϕ is a left H-homomorphism. As left H-modules, the former is a direct sum of $\dim_R P$ -copies of P and the latter is a direct sum of

$\dim_R P$ -copies of H^*, which is isomorphic to the direct sum of $\dim_R P$ -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 μ is an isomorphism.

Thus μ is an isomorphism for a general commutative ring R. let $\mu(a)$ be an identity of $\mathrm{Hom}(A, A)$. 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 $\eta : H = RG \cong H^* = \mathrm{Hom}(RG, R)$ defined by $[\eta(\sigma)](\tau) = \delta_{\sigma^{-1},\tau}$ (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, $A = H^* \otimes_H P$, $B = H^* \otimes_H Q$ ($P \otimes P \overset{\tilde{\phi}_A}{\cong} H^2 \overset{\Delta}{\otimes}_H P$, $Q \otimes Q \overset{\tilde{\phi}_B}{\cong} H^2 \overset{\Delta}{\otimes}_H Q$, $u(P, \tilde{\phi}_A) = u(Q, \tilde{\phi}_B) = 1 \otimes 1 \otimes 1 \in H^3$) are isomorphic. By Proposition 1.1, if A and B are isomorphic then $P \cong Q$ (we shall identify P and Q). Let ξ be the isomorphism $A = H^* \otimes_H P \overset{\xi}{\cong} B = H^* \otimes_H P$, then ξ induces an

automorphism of P, which we shall denote by $w(\xi)$ and we sometimes regard $w(\xi)$ as a unit of H by homothety. ξ commutes with the multiplications of A and B, so $w(\xi)$ commutes with ϕ_A and ϕ_B. That is the following diagram is commutative.

$$\begin{array}{ccc} P \otimes P & \xrightarrow{\phi_A} & (H \otimes H) \overset{\Delta}{\otimes}_H P \\ \downarrow{\scriptstyle w(\xi) \otimes w(\xi)} & & \downarrow{\scriptstyle 1 \otimes w(\xi)} \\ P \otimes P & \xrightarrow{\phi_B} & (H \otimes H) \overset{\Delta}{\otimes}_H P \end{array} \tag{3.7}$$

Since ϕ_A and ϕ_B are H^2-isomorphisms and the isomorphism $1 \otimes w(\xi)$ is a left homothety by $\Delta(w(\xi))$, the commutativity of (3.7) claims that $\phi_A\phi_B^{-1} = \Delta(w(\xi))^{-1}(w(\xi) \otimes w(\xi))$ or equivalently $\phi_A\phi_B^{-1} = d(w(\xi))$, d is a coboundary operator. Conversely, if such $w(\xi)$ exists, we can easily make the isomorphism $\xi : H^* \otimes_H P \cong H^* \otimes_H P$. 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 $\phi_A : P \otimes P \cong H^2 \overset{\Delta}{\otimes}_H P$ and $\phi_B : Q \otimes Q \cong H^2 \overset{\Delta}{\otimes}_H Q$, $u(P, \phi_A) = u(P, \phi_B) = 1 \otimes 1 \otimes 1$. Then A is isomorphic to B, if and only if, $P \cong Q$ 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 $P \cong H$. By Theorem 3.2, there exists $\phi : H \otimes H \cong H^2 \overset{\Delta}{\otimes}_H H = H \otimes H$ with $u(H, \phi)$

$= 1 \otimes 1 \otimes 1$. $\tilde{\phi}$ is a homothety by a unit v of H^2. $u(H, v)$ $= (v^{-1} \otimes 1) \cdot ((\Delta \otimes 1)(v^{-1})) \cdot ((1 \otimes \Delta)(v)) \cdot (1 \otimes v)$. Thus $u(H, \tilde{\phi})$ $= 1 \otimes 1 \otimes 1$ 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 $\mathrm{Hom}_G(H, A)$ is an H-Hopf Galois extension of R, where the multiplication on ${}_H\mathrm{Hom}_G({}_H H, A)$ is defined by the formula;

$$(f_1 \cdot f_2)(x) = \sum_{(x)} f_1(x_{(1)}) \cdot f_2(x_{(2)}),\quad f_1, f_2 \in \mathrm{Hom}_G(H, A),\ x \in H.$$

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

$$\begin{array}{ccc} \mathrm{Hom}_G(H, A) \otimes \mathrm{Hom}_G(H, A) & \xrightarrow{\phi'} & \mathrm{Hom}(H, \mathrm{Hom}_G(H, A)) \\ \| \text{can.} & & \\ \mathrm{Hom}_{G \otimes G}(H \otimes H, A \otimes A) & & \text{can.} \ \| \\ \| \mathrm{Hom}_{G^2}(H^2, \phi) & & \\ \mathrm{Hom}_{G \otimes G}(H \otimes H, \mathrm{Hom}(G, A)) & \xrightarrow{\alpha} & \mathrm{Hom}_G({}_G H \otimes H, A) \end{array} \tag{4.1}$$

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

$$[\alpha(\tau)](x \otimes y) = \sum_{(x)} [\tau(x_{(1)} \otimes x_{(2)} y)](1),$$

$1, x, y \in H$, $\tau \in \mathrm{Hom}_{G \otimes G}(H \otimes H, \mathrm{Hom}(G, A))$. As easily checked, (4.1) is a commutative diagram. α is an isomorphism – the inverse α^{-1} is given by the formula;

$[(\alpha^{-1}(\nu))(x \otimes y)](z) = \sum_{(x)} \nu(x_{(1)} \otimes z \cdot S(x_{(2)}) \cdot y)$,
$\nu \in \mathrm{Hom}_G({}_G H \otimes H, A)$, $x,y \in H$, $z \in G$. Thus ϕ' is an isomorphism. So $\mathrm{Hom}_G(H, A)$ 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 $m : H \otimes H \longrightarrow H$ is a homomorphism of Hopf algebras. Let A,B be an H-Hopf Galois extension of R, we shall define

$$A \cdot B = \mathrm{Hom}_{H \otimes H}(H, A \otimes B)$$

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 $A \cdot B = \mathrm{Hom}_{H \otimes H}(H, A \otimes B)$ is isomorphic to $\{\sum a_i \otimes b_i \in A \otimes B \mid \sum_i ha_i \otimes b_i = \sum_i a_i \otimes hb_i$ for any $h \in H\}$.

We shall denote $\{\sum_i a_i \otimes b_i \in A \otimes B \mid \sum_i ha_i \otimes b_i = \sum_i a_i \otimes hb_i$ 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 left H-modules. We define the homomorphisms $\alpha, \beta : (H^*(v) \otimes H^*(v'))^H \underset{\beta}{\overset{\alpha}{\rightleftarrows}} H^*(vv')$ 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 α and β are well-defined left H-homomorphisms and are inverse to each other. That α gives an isomorphism of H-module algebras can be proved by straitforward 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, ϕ_P), (Q, ϕ_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·B is an H-Hopf Galois extension of R induced from a Pic-valued 1-cocycle $(P \otimes_H Q, \phi_P \otimes_{H^2} \phi_Q)$.
Especially, the isomorphism classes of H-Hopf Galois extensions of R E(H) forms an abelian group.

Proof. We shall define the homomorphisms $\alpha', \beta' : (A \otimes B)^H \rightleftarrows H^* \otimes_H (P \otimes_H Q)$ by the formula;

$\alpha'((f_1 \otimes p) \otimes (f_2 \otimes q)) = \alpha(f_1 \otimes f_2) \otimes (p \otimes q)$

$\beta'(f \otimes (p \otimes q)) = \sum_i (f_{1_i} \otimes p) \otimes (f_{2_i} \otimes q)$ if $\beta(f) = \sum_i f_{1_i} \otimes f$

where α, β is the homomorphism in Proposition 4.4, $f_1, f_2, f_{1_i}, f_{2_i} \in H^*$, $p \in P$, $q \in Q$. As easily checked, α' and β' are well-defined left H-homomorphisms and are inverse to each other. To see that α' is an isomorphism of H-module algebras, we may localize (it). Then Proposition 4.4 ensures that α' 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

$$\Delta_0^n, \Delta_i^n \ (i=1,2,\cdots,n), \Delta_{n+1}^n : H^n \longrightarrow H^{n+1} \quad (n \geq 0)$$

be the algebra homomorphism defined by the formulas;

$$\Delta_0^n(x_1 \otimes \cdots \otimes x_n) = 1 \otimes x_1 \otimes \cdots \otimes x_n$$

$$\Delta_i^n(x_1 \otimes \cdots \otimes x_n) = x_1 \otimes \cdots \otimes x_{i-1} \otimes \Delta(x_i) \otimes x_{i+1} \otimes \cdots \otimes x_n$$

$$\Delta_{n+1}^n(x_1 \otimes \cdots \otimes x_n) = x_1 \otimes \cdots \otimes x_n \otimes 1, \quad x_i \in H.$$

H^0 means R and we note that Δ_0^0, Δ_1^0 coincides with the unit map $R \to H$.

Let U denote the unit functor and Pic denote the Picard group functor. Δ_i^n $(i=0,1,\cdots,n+1)$ yields functors $U(H^n) \longrightarrow U(H^{n+1})$, $Pic(H^n) \longrightarrow Pic(H^{n+1})$, which we shall denote by the same letter Δ_i^n. We shall define

$$d_n : U(H^n) \longrightarrow U(H^{n+1}), \quad d_n : Pic(H^n) \longrightarrow Pic(H^{n+1})$$

as the alternate sum of Δ_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 $C(H, U) = \{ U(H^n), d_n \}_{n \geq 0}$ and $C(H, Pic) = \{ Pic(H^n), d_n \}_{n \geq 0}$. The n-th cohomology group $Ker(d_n)/Im(d_{n-1})$ $(n \geq 1)$ of $C(H, U)$, $C(H, Pic)$ is denoted by $H^n(H, U)$, $H^n(H, Pic)$ respectively, and will be called the unit-valued (resp. Pic-

valued) generalized Harrison cohomology group. The 0-th cohomology group is defined as $H^0(H, U) = \mathrm{Ker}(d_0) = U(R)$, $H^0(H, Pic) = \mathrm{Ker}(d_0) = Pic(R)$.

Next, we proceed toward the definition of groups $\mathbf{H}^n(H)$ parallel with Hattori [6],[7]. Let $\mathcal{P}ic(H^n)$ be the category of projective H^n-modules of rank 1 $(n=0,1,\cdots)$. This is a category with product $\otimes_{H^n}$. In this Appendix, P* denotes the H^n-dual module of $P \in \mathcal{P}ic(H^n)$ unless otherwise stated. Hence $P^* \in \mathcal{P}ic(H^n)$.

Similar to the case of Pic-valued cohomology groups, $\Delta_i^n : H^n \longrightarrow H^{n+1}$ yields the functor $\Delta_i^n : \mathcal{P}ic(H^n) \longrightarrow \mathcal{P}ic(H^{n+1})$. Hence we also define $d_n : \mathcal{P}ic(H^n) \longrightarrow \mathcal{P}ic(H^{n+1})$ as the alternate sum of Δ_i^n. Let $f : P \cong Q$ be an isomorphism in $\mathcal{P}ic(H^n)$ and let $\Delta_i^n f : \Delta_i^n P \cong \Delta_i^n Q$, $\Delta_i^n f^* : \Delta_i^n P^* \cong \Delta_i^n Q^*$ be the canonical isomorphism induced from f, then $d_n f$ is defined as $\Delta_0^n f \otimes \Delta_1^n f^* \otimes \cdots : d_n P \cong d_n Q$.

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^2H^n with H^{n+2} through the composite of the canonical isomorphisms $d^2H^n \overset{dI_{n+1}}{\cong} dH^{n+1} \overset{I_{n+2}}{\cong} H^{n+2}$.

For any $P \in \mathcal{P}ic(H^n)$, we have a canonical isomorphism $d^2P \cong H^{n+2}$ given by contracting all dual pairs appearing in the expression of d^2P. This isomorphism $d^2P \cong H^{n+2}$ will be written as c_P in the sequal. For $f : P \cong Q$, the following diagram is commutative:

$$\begin{array}{ccc} d^2P & \xrightarrow{\quad c_P \quad} & H^{n+2} \\ \downarrow{\scriptstyle d^2f} & & \| \\ d^2Q & \xrightarrow{\quad c_Q \quad} & H^{n+2} \end{array}$$

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

Let $n \geq 1$, (P, p) denotes a pair of a module $P \in Pic(H^{n-1})$ such that $|P|$ is a 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:

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

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

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

The set of isomorphism classes $|(P, p)|$ of $(P, p) \in P^n(H)$ forms an abelian group, which we shall write $\mathbb{P}^n(H)$. We shall denote by $\mathbb{Z}^n(H)$ the subgroup of $\mathbb{P}^n(H)$ consisting of all $|(P, p)|$ satisfying $dp = c_P$, and by $\mathbb{B}^n(H)$ the set of all $|(dP, c_P)|$ $(P \in Pic(H^{n-2}))$. For $n = 1$, we shall put $\mathbb{B}^1(H) = \{|(R, I_1)|\}$. Since $dc_P = c_{dP}$, $\mathbb{B}^n(H)$

is a subgroup of $\mathbb{Z}^n(H)$ and we have the groups

$$\mathbb{H}^n(H) = \mathbb{Z}^n(H)/\mathbb{B}^n(H)$$

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

Every $u \in U(H^n)$ determines a pair (H^{n-1}, u) where $u : dH^{n-1} = H^n \longrightarrow H^n$ and $|(H^{n-1}, u)| \in \mathbb{Z}^n(H)$ 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 $(n \geq 1)$,

$$\alpha^n : H^n(H, U) \longrightarrow \mathbb{H}^n(H);\ cl(u) \longmapsto cl|(H^{n-1}, u)|.$$

For $n = 0$, α^0 is defined to the identity map $H^0(H, U) = \mathbb{H}^0(H)$.

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

$$\beta^n : \mathbb{H}^n(H) \longrightarrow H^{n-1}(H, \mathrm{Pic});\ cl|(P, p)| \longmapsto cl|P|.$$

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

$$\begin{array}{ccc} d^2P & \xrightarrow{\ c_P\ } & H^{n+1} \\ \| & & \downarrow u \\ d^2P & \xrightarrow{\ dp\ } & H^{n+1} \end{array}$$

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

$$c_Q : dP = d^2Q \cong H^n$$

as a cocycle condition isomorphism. Then $dc_Q = c_{dQ}$ claims

that $u = 1$. Hence we have the following homomorphism.

$$\gamma^n : H^{n-1}(H, Pic) \longrightarrow H^{n+1}(H, U); \ cl|(P,p)| \longmapsto cl(u).$$

Theorem A.1. The following sequence is exact:

$$0 \longrightarrow H^1(H, U) \xrightarrow{\alpha^1} \mathbb{H}^1(H) \xrightarrow{\beta^1} H^0(H, Pic) \xrightarrow{\gamma^1} \cdots$$

$$\cdots \xrightarrow{\gamma^{n-1}} H^n(H, U) \xrightarrow{\alpha^n} \mathbb{H}^n(H) \xrightarrow{\beta^n} H^{n-1}(H, Pic) \xrightarrow{\gamma^n} \cdots$$

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

$$(dQ, p) = (dQ, c_Q) \cdot (H^n, u), \quad (dQ, c_Q) \in B^n(H),$$

$$cl|(P, p)| = cl|(dQ, p)| \in Im(\alpha^n).$$

If $cl|P| \in Ker(\gamma^n)$, we have $dp = c_p$ with a suitably chosen $p : dP \cong H^n$. This means that $cl|P| \in Im(\beta^n)$.

If $cl(u) \in Ker(\alpha^{n+1})$, there exists $P \in Pic(H^{n-1})$ such that $(H^n, u) \cong (dP, c_p)$. This means that there exists $p : dP \cong H^n$ satisfying $c_p = udp$. Hence $u^{-1} \in Im(\gamma^n)$, and therefore $u \in Im(\gamma^n)$.

The definitions of $\mathbb{H}^1(H)$ and $H^0(H, Pic)$ 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 $\mathbb{H}^n(H)$, $H^n(H, U)$ and $H^n(H, Pic)$ represent are different

from Hattori's by their own characters. For example, $\mathbb{H}^0(H) = H^1(H, U) = U(R)$, $H^0(H, Pic) = Pic(R)$, $H^1(H, U) = \{ u \in U(H) \mid \Delta(u) = u \otimes u \}$ 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, β^1 is an epimorphism. Thus we get

Corollary A.2. The following sequences are exact;

$$0 \longrightarrow H^1(H, U) \xrightarrow{\alpha^1} \mathbb{H}^1(H) \xrightarrow{\beta^1} Pic(R) \longrightarrow 0 ,$$

$$0 \longrightarrow H^2(H, U) \xrightarrow{\alpha^2} \mathbb{H}^2(H) \xrightarrow{\beta^2} H^1(H, Pic) \xrightarrow{\gamma^2} H^3(H, U) \xrightarrow{\alpha^3} \cdots$$

Let $cl|(P, p)| \in \mathbb{H}^2(H)$, this means that P is a rank 1-projective H-module and that $dP = (P \otimes P) \otimes_{H^2} (H \otimes H) \overset{\Delta}{\otimes}_H P^* \overset{p}{=\!=} H^2$ satisfying $c_p = dp$. From p we make $\phi_P : P \otimes P \cong H^2 \overset{\Delta}{\otimes}_H P$ naturally, then $c_p = dp$ means $u(P, \phi_P) = 1 \otimes 1 \otimes 1 \in H^3$. And $(P, p) \cong (P', p')$ means that there exists a unit $w \in H$ which makes the following diagram commutative;

$$\begin{array}{ccc} dP & \xrightarrow{\quad p \quad} & H^n \\ \Big\downarrow{\scriptstyle dw} & & \Big\| \\ dP' & \xrightarrow{\quad p' \quad} & H^n \end{array}$$

Thus $(P, p) \cong (P', p')$ means $u(P, \phi_p) = dw \cdot u(P', \phi_{p'})$. 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.

Nara Women's University

References

[1] M.Auslander and O.Goldman: The Brauer group of a commutative ring, Trans. Amer. Soc.,97(1960), 367-409.

[2] S.U.Chase and A.Rosenberg: A theorem of Harrison, Kummer theory, and Galois algebras, Nagoya Math. J.,27(1966), 663-685.

[3] S.U.Chase and M.E.Sweedler: Hopf algebras and Galois theory, Lect. Note in Math. 97, Springer, 1969.

[4] D.K.Harrison: Abelian extension of arbitrary fields, Trans. Amer. Math. Soc.,97(1960), 230-235.

[5] A.Hattori: Semisimple algebras over a commutative ring, J. Math. Soc. Japan, 15(1963), 404-419.

[6] A.Hattori: On groups $H^n(S,G)$ and the Brauer group of commutative rings, Sic. Pap. Coll. Gen. Educ. Univ. Tokyo, 28(1978), 1-20.

[7] A.Hattori: On groups $\mathbb{H}^n(S/R)$ related to the Amitsur cohomology and the Brauer group of commutative rings, Osaka J. Math., 16(1979), 357-382.

[8] T.Kanzaki: On Galois algebra over a commutative ring, Osaka J. Math., 2(1965), 309-317.

[9] T.Kanzaki: A note on abelian Galois algebra over a commutative ring, Osaka J. Math.,3(1966), 1-6.

[10] H.F.Kreimer and P.M.Cook II: Galois theories and normal bases, J. Algebra, 43(1976), 115-121.

[11] R.Larson and M.E.Sweedler: An associative orthogonal bilinear form for Hopf algebras, Amer. J. Math., 91(1967), 75-94.

[12] A.Nakajima: On generalized Harrison cohomology and Galois object, Math. J. Okayama Univ., 17(1975), 135-149.

[13] A.Nakajima: Galois objects as modules over a Hopf algebra, Math. J. Okayama Univ., 18(1976), 159-169.

[14] M.E.Sweedler: Hopf algebras, Benjamin, New York, 1969.

[15] K.Yokogawa: Non-commutative Hopf Galois extensions, to appear.