Mathematical Journal of Okayama University

Volume 23, *Issue* 2 1981 *Article* 11

DECEMBER 1981

Free algebras and Galois objects of rank 2

Atsushi Nakajima*

*Okayama University

Math. J. Okayama Univ. 23 (1981), 181—187

FREE ALGEBRAS AND GALOIS OBJECTS OF RANK 2

ATSUSHI NAKAJIMA

Throughout the present note, R will represent a commutative algebra over $GF(2)$, and $U(R)$ the group of all invertible elements in R. Unadorned $\otimes$ means $\otimes_R$, every module is R-module and every map is R-linear. Given an element u in R, we denote by H_u the free Hopf algebra over R with basis $\{1, d\}$ whose Hopf algebra structure is given by

$$d^2 = ud, \ \Delta(d) = d\otimes 1 + 1\otimes d, \ \varepsilon(d) = 0 \text{ and } \lambda(d) = d,$$

where Δ, ε and λ are the comultiplication, counit and antipode of H_u, respectively. As for other notations and terminologies used here, we follow [2] and [6].

In this note we study on Galois H_u-objects and purely inseparable R-algebras in the sense of [7] and compute the group of Galois H_u-objects of R.

1. Galois H_u-objects and purely inseparable algebras of rank 2.

An R-algebra A is called a *free* (resp. *projective*) *R-algebra* if A is a free (resp. projective) R-module and R is an R-direct summand of A. An R-algebra A is called an *H_u-comodule algebra* if A is an H_u-comodule such that the H_u-coaction map $\rho: A \longrightarrow A\otimes H_u$ is an R-algebra homomorphism. An H_u-comodule algebra is called a *free* (resp. *projective*) *H_u-comodule algebra* if it is a free (resp. projective) R-algebra.

Let F be a free H_u-comodule algebra with basis $\{1, x\}$. First, we determine the H_u-comodule algebra structure of F. Let $\rho: F \longrightarrow F\otimes H_u$ be an H_u-comodule structure map of F, and set

$$\rho(x) = t_0 + t_1(x\otimes 1) + t_2(1\otimes d) + t_3(x\otimes d) \ (t_i \in R).$$

Then, in view of $(1\otimes\varepsilon)\rho(x) = x$ and $(1\otimes\Delta)\rho(x) = (\rho\otimes 1)\rho(x)$, we have

$$t_0 = 0, \ t_1 = 1 \text{ and } t_2 t_3 = t_3^2 = 0.$$

Moreover, if we set $x^2 = rx + s (r, s \in R)$, then $\rho(rx+s) = \rho(x^2) = \rho(x)^2$ yields $t_3^2 u = t_2 r$ and $t_3 r = 0$. Thus we obtain the following

Lemma 1.1. *Let F be a free R-algebra with basis* $\{1, x\}$, and $x^2 = rx + s$ $(r, s \in R)$. *If F is an H_u-comodule algebra then there exist $r_1, s_1 \in R$ such*

Mathematical Journal of Okayama University, Vol. 23 [1981], Iss. 2, Art. 11

that

(1.1) $$rs_1 = r_1 s_1 = s_1^2 = 0 \quad and \quad r_1^2 u = r_1 r,$$

and the H_u-comodule structure of F is given by

(1.2) $$\rho(x) = x \otimes 1 + r_1(1 \otimes d) + s_1(x \otimes d).$$

Conversely, if there exist r_1, $s_1 \in R$ which satisfies (1.1), *then the map ρ defined by* (1.2) *gives the H_u-comodule structure of F.*

A projective H_u-comodule algebra A is called a *Galois H_u-object* if $\gamma: A \otimes A \longrightarrow A \otimes H_u$ defined by $\gamma(a_1 \otimes a_2) = (a_1 \otimes 1)\rho(a_2)$ is an isomorphism, where ρ is the H_u-comodule structure map of A.

Proposition 1.2. *Let F be a free R-algebra as in* Lemma 1.1. *If F is a Galois H_u-object then there exists $v \in U(R)$ such that $vu = r$, and the H_u-comodule structure of F is given by*

(1.3) $$\rho(x) = x \otimes 1 + v(1 \otimes d).$$

Conversely, if there exists $v \in U(R)$ such that $vu = r$, then F is a Galois H_u-object with the H_u-comodule structure map ρ defined by (1.3)

Proof. If F is a Galois H_u-object, then γ is an isomorphism. Since F and H_u are free R-modules of rank 2 and γ is an F-algebra map, γ is an isomorphism if and only if there exists $k \in F \otimes F$ such that $\gamma(k) = 1 \otimes d$. We set $k = t_0 + t_1(x \otimes 1) + t_2(1 \otimes x) + t_3(x \otimes x)$ $(t_i \in R)$. Then by $\gamma(k) = 1 \otimes d$ and Lemma 1.1, we have

$$s_1 = 0, \quad r_1 t_2 = 1 \quad \text{and} \quad r_1 u = r.$$

Thus we may take $v = r_1$.

Conversely, if $vu = r$ for some $v \in U(R)$, then ρ defined by (1.3) gives an H_u-comodule algebra structure on F (Lemma 1.1) and $\gamma(v^{-1}(x \otimes 1 + 1 \otimes x)) = 1 \otimes d$. Thus F is a Galois H_u-object.

Definition 1.3 ([7, Def.1 and Lemma 1 (a)]). An R-algebra A is called *purely inseparable* if the kernel of the map $\mu: A \otimes A^o \longrightarrow A$ defined by $a \otimes b^o \longrightarrow ab$ is contained in the radical $J(A \otimes A^o)$ of $A \otimes A^o$, where A^o denotes the opposite algebra to A.

Now, we shall prove the following

Theorem 1.4. *Let F be a free R-algebra with basis* $\{1, x\}$, *and* $x^2 = ux + s$ $(s \in R)$.

(1) *F is a Galois H_u-object with the H_u-comodule structure map ρ defined by $\rho(x)=x\otimes 1+1\otimes d$.*

(2) *If u is in $U(R)$ then F is a Galois extension of R, and conversely.*

(3) *If u is in the radical $J(R)$ of R then F is a purely inseparable algebra over R, and conversely.*

Proof. (1) is a direct consequence of Prop.1.2. (2) is already known (cf. [5]), so we prove (3). Let $\mu: F\otimes F \longrightarrow F$ be the multiplication map of F. Then $\mathrm{Ker}(\mu)$ is generated by $a\otimes 1+1\otimes a$ ($a\in F$), so $y=x\otimes 1+1\otimes x$ is a generator of $\mathrm{Ker}(\mu)$. Assume that F is purely inseparable. Since $\mathrm{Ker}(\mu)$ is contained in $J(F\otimes F)$, $1+cy$ is invertible in $F\otimes F$ for any $c\in R$. Let $z=t_0+t_1(x\otimes 1)+t_2(1\otimes x)+t_3(x\otimes x)$ be the inverse element of $1+cy$ ($t_i\in R$). Then, from $(1+cy)z=1$ we obtain

$$\begin{bmatrix} 1 & cs & cs & 0 \\ c & 1+cu & 0 & cs \\ c & 0 & 1+cu & cs \\ 0 & c & c & 0 \end{bmatrix} \begin{bmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

As is easily seen

$$(1+cu)^2 \begin{bmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \end{bmatrix} = (1+cu) \begin{bmatrix} 1+cu \\ c \\ c \\ 0 \end{bmatrix}$$

Then, by the uniqueness of the inverse of $1+cy$, the matrix of the coefficients of t_i is invertible, and so the determinant of it is a nonzero divisor ([4, p.161, Cor.]). We have thus the following:

(1.4) For any $c\in R$, there exists $t\in R$ such that $(1+cu)t=c$.

If $u\notin J(R)$, then there exists a maximal ideal M in R such that $u\notin M$, so that $R=Ru+M$. Put $1=r_0u+m$ ($r_0\in R$, $m\in M$). Then, by (1.4), there exists $t\in R$ such that $(1+r_0u)t=r_0$. Thus $r_0=(1+r_0u)t=mt\in M$. But this implies a contradiction $1=r_0u+m\in M$. Hence $u\in J(R)$.

Conversely, if $u\in J(R)$ then $u\in J(F\otimes F)$, since $F\otimes F$ is integral over R. Thus $y^2=uy\in J(F\otimes F)$, whence it follows that $y\in J(F\otimes F)$.

We denote by (u, s) the Galois H_u-object in Th.1.4(1).

Now, let A be an H_u-comodule algebra. Then A has an H_u^*-module structure ([2, §7, p.56]). The dual Hopf algebra $H_u^*=\mathrm{Hom}_R(H_u, R)$ is a free R-module with basis $\{\varepsilon, \delta\}$, where $\delta(1)=0$ and $\delta(d)=1$, and the Hopf algebra stucture is given by

$$\delta^2 = 0,\ \tilde{\Delta}(\delta) = \delta\otimes\varepsilon + \varepsilon\otimes\delta + u(\delta\otimes\delta),\ \tilde{\varepsilon}(\delta) = 0 \text{ and } \tilde{\lambda}(\delta) = \delta,$$

where Δ, $\tilde{\varepsilon}$ and $\tilde{\lambda}$ are the structure maps of H_u^*. Thus the H_u^*-action on A is given by

$$\varepsilon(a_1) = a_1 \text{ and } \delta(a_1a_2) = \delta(a_1)a_2 + a_1\delta(a_2) + u\delta(a_1)\delta(a_2)\ (a_i \in A).$$

In case $u = 0$, δ is obviously an R-derivation on A. Next, we consider the case that u is invertible. If we put $\sigma = \varepsilon + u\delta$, then $\sigma^2 = \varepsilon$ and $\tilde{\Delta}(\sigma) = \sigma\otimes\sigma$, so σ is an R-algebra automorphism of A.

Theorem 1.5. *If A is a Galois H_u-object then A is isomorphic to a free Galois H_u-object (u, s) for some $s \in R$.*

Proof. By [2, Ths.9.3 and 9.6], $R = \{a \in A | \delta(a) = 0\}$ and the sequence of R-modules

$$0 \longrightarrow R \xrightarrow{i} A \xrightarrow{\delta} \delta(A) \longrightarrow 0$$

is exact and split, where i is the canonical injection. Thus $\delta(A)$ is projective and of rank 1. We show that $\delta(A) = R$. Let $Q = \{w \in D | (1\#\delta)w = 0\}$, where $D = A\#H_u^*$, the smash product of A and H_u^*([2, Def.9.2, Def. and Remarks 9.4.]). Then it is easy to see that w is in Q if and only if $w = \delta(a)\#1 + a\#\delta$ $(a \in A)$. Since $a\#\delta = \delta(a)\#1 + (1\#\delta)(a\#1 + u\delta(a)\#1)$, $w = (1\#\delta)\,(b\#1)$ for some $b \in A$. Moreover by Th.9.6, the map $[\ ,\ ]$: $Q\otimes_D A \longrightarrow R$ defined by $[w,a] = w(a)$ is an epimorphism, and so there exists $y \in A$ such that $\delta(y) = 1$. Thus $R \subseteq \delta(A)$, and $\delta(A) \subseteq R$ is clear because $\delta^2 = 0$. Hence A is a free algebra with basis $\{1, y\}$, and $y^2 = ry + t$ $(r,\ t \in R)$. Then, by Prop.1.2, there exists $v \in U(R)$ such that $vu = r$, and the H_u-comodule structure of A is given by $\rho(y) = y\otimes 1 + v(1\otimes d)$. Therefore, we have $A \cong (u,\ v^{-2}t)$ (as Galois H_u-object).

Corollary 1.6. *Let A be a projective H_u-comodule algebra of rank 2. Then the following conditions are equivalent.*

(1) *A is a Galois H_u-object.*

(2) *A contains an element x such that $\delta(x) \in U(R)$.*

(3) $\delta(A) = R$.

Proof. By the proof of Th.1.5, (1)$\Longrightarrow$(2) is clear and (2)$\Longleftrightarrow$(3) is immediate by $\delta(A) \subseteq R$, so we prove (2)$\Longrightarrow$(1). If $t_0 + t_1x = 0 (t_i \in R)$, then $0 = \delta(t_0 + t_1x) = t_1\delta(x)$, and thus $t_0 = t_1 = 0$. Since A is of rank 2, $\{1, x\}$ is a free basis of A. Then by Lemma 1.1, the H_u-comodule structure of A is given by (1.2). Since $\delta(x) = x\delta(1) + r_1\delta(d) + s_1x\delta(d) = r_1 +$

$s_1x\in U(R)$, we have $s_1=0$ and $r_1\in U(R)$. Hence, by Lemma 1.1 and Prop.1.2, A is a Galois H_u-object.

2. Group of Galois H_u-objects. *Let* A and B be H_u-comodule algebras with structure maps ρ_A and ρ_B, respectively. We set $\tau_{A,B}=(1\otimes t)(\rho_A\otimes 1)-(1\otimes\rho_B): A\otimes B\longrightarrow A\otimes B\otimes H_u$ and $AB=\mathrm{Ker}(\tau_{A,B})$, where t is the twist map $a\otimes b\longrightarrow b\otimes a$. Then it is easy to see that the map $\rho_{AB}: AB\longrightarrow AB\otimes H_u$ defined by $\rho_{AB}=(1\otimes t)(\rho_A\otimes 1)\ (=1\otimes\rho_B)$ is an H_u-comodule algebra structure map of AB. Moreover, if A and B are Galois H_u-objects then AB is a Galois H_u-object by [1, p.689]. In our case the converse holds.

Theorem 2.1. *Let A and B be free H_u-comodule algebras of rank* 2. *If AB is a Galois H_u-object, then A and B are Galois H_u-objects.*

Proof. Let $\{1, x\}$ and $\{1, y\}$ be free bases of A and B, respectively. Since AB is a Galois H_u-object, AB has a free basis $\{1, z\}$ and $\rho_{AB}(z)=z\otimes 1+1\otimes 1\otimes d$. We set $\rho_A(x)=x\otimes 1+r_1(1\otimes d)+s_1(x\otimes d)$ and $z=t_0+t_1(x\otimes 1)+t_2(1\otimes y)+t_3(x\otimes y)$ $(r_1, s_1, t_i\in R)$. Then by $\rho_{AB}(z)=(1\otimes t)(\rho_A\otimes 1)(z)$, we have $t_1r_1=1$ and $t_1s_1=t_3r_1=t_3s_1=0$. Thus r_1 is invertible and $s_1=0$. Then, by Prop.1.2, A is a Galois H_u-object. Also, similarly, B is a Galois H_u-object.

Proposition 2.2. *Let $A_i=(u, s_i)$ $(i=1, 2)$ be Galois H_u-objects. Then $A_1A_2=(u, s_1+s_2)$.*

Proof. Let $\{1, x_i\}$ be free bases of A_i. Then, by the definition of A_1A_2,

$$A_1A_2=\{t_0+t_1(x_1\otimes 1+1\otimes x_2)\mid t_i\in R\}$$

and $\{1, y=x_1\otimes 1+1\otimes x_2\}$ is a free basis of A_1A_2. Moreover, $y^2=uy+s_1+s_2$ and $\rho(y)=y\otimes 1+1\otimes 1\otimes d$. Thus $A_1A_2=(u, s_1+s_2)$.

Now, let $\mathrm{Gal}(R, H_u)$ be the group of isomorphism classes of Galois H_u-objects in the sense of [1, p.686]. If $C\in\mathrm{Gal}(R, H_u)$ and $A\in C$ then we write $C=[A]$. Moreover, by M_u, we denote the subgroup $\{\beta^2+u\beta\mid\beta\in R\}$ of the additive group $(R, +)$. Under this situation, we shall prove the following

Theorem 2.3. $\mathrm{Gal}(R, H_u)$ *is group isomorphic to the factor group $(R, +)/M_u$, which is abelian and of exponent* 2.

Mathematical Journal of Okayama University, Vol. 23 [1981], Iss. 2, Art. 11

Proof. By Th.1.4, there exists a map $\phi : (R, +) \longrightarrow \mathrm{Gal}(R, H_u)$ where $\phi(t) = [(u, t)]$. In verture of the results of Th.1.5 and Prop. 2.2, ϕ is a group epimorphism. Now, let $A_i = (u, s_i)$ be Galois H_u-objects with bases $\{1, x_i\}$ and H_u-comodule structure maps ρ so that $x_i^2 = ux_i + s_i$ and $\rho(x_i) = x_i \otimes 1 + 1 \otimes d$ $(i = 1, 2)$. We assume that there is an (H_u-Galois object) isomorphism $f : A_1 \longrightarrow A_2$, and set $f(x_1) = \alpha x_2 + \beta (\alpha, \beta \in R)$. Then by $\rho f(x_1) = (f \otimes 1)\rho(x_1)$, we have $\alpha = 1$. Noting $f(x_1)^2 = f(x_1^2)$, we see that $\beta^2 + u\beta = s_1 + s_2$. Thus, we obtain $\mathrm{Ker}(\phi) \subseteq M_u$. Conversely, let $\phi(\beta^2 + u\beta) = [(u, \beta^2 + u\beta)]$. Define a map $f : (u, \beta^2 + u\beta) \longrightarrow (u, 0)$ by $f(1) = 1$ and $f(x) = y + \beta$, where $\{1, x\}$ and $\{1, y\}$ are free bases of $(u, \beta^2 + u\beta)$ and $(u, 0)$, respectively. Then it is easy to see that $\rho f(x) = (f \otimes 1)\rho(x)$ and $f(x^2) = f(x)^2$. Thus f is an isomorphism as Galois H_u-object. Hence $\mathrm{Ker}(\phi) \supseteq M_u$. This proves the theorem.

Now, let Q_s be the group of the isomorphism classes of quadratic Galois extensions of R in the sense of Kitamura [3, p.16]. Then

Corollary 2.5. (1) $\mathrm{Gal}(R, H_1) \cong (R, +)/\{r^2 - r \mid r \in R\} \cong Q_s \cong \mathrm{Gal}(R, H_u)$ *for every* $u \in U(R)$.

(2) $\mathrm{Gal}(R, H_0) \cong (R, +)/\{r^2 \mid r \in R\}$.

Proof. Let $s, s' \in R$, and $u \in U(R)$. Then, the polynomial rings $R[X]$ and $R[Y]$, $R[X]/R[X](X^2 + uX + s) \cong R[Y](Y^2 + Y + u^{-2}s)$(as R-algebra), and moreover, $R[X]/R[X](X^2 + X + s) \cong R[Y]/R[Y](Y^2 + Y + s')$ if and only if $s - s' \in M_1$. Hence, it follows that $Q_s \cong (R, +)/M_1 \cong \mathrm{Gal}(R, H_1)$. Since $\beta^2 + u\beta = u^2(u^{-1}\beta)^2 + u^2(u^{-1}\beta)$ $(\beta \in R)$, we have $M_u = u^2 M_1$. Hence we obtain $\mathrm{Gal}(R, H_u) \cong (R, +)/M_u \cong (u^2 M_1 \cong (R, +)/M_1 \cong \mathrm{Gal}(R, H_1)$.

REFERENCES

[1] M. BEATTIE: A direct sum decomposition for the Brauer group of H-dimodule algebras, J. Alg. **42** (1976), 686—693.

[2] S. U. CHASE and M. S. SWEEDLER: Hopf Algebras and Galois Theory, Lecture Notes in Math. **97**, Springer-Verlag, Berlin, 1969.

[3] K. KITAMURA: On the free quadratic extensions of commutative rings, Osaka J. Math. **10** (1973), 15—20.

[4] N. H. MCCOY: Rings and Ideals, Carus Math. Monograph **8**, The Math. Ass. Amer. 1948.

[5] T. NAGAHARA: A quadratic extensions, Proc. Japan Acad. **47** (1971), 6—7.
[6] M. E. SWEEDLER: Hopf Algebra, Benjamin, New York, 1969.
[7] M. E. SWEEDLER: Purely inseparable algebras, J. Alg. **35** (1975), 342—355.

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(*Received December 15, 1980*)