数理解析研究所講究録
第 438 巻 1981 年 9-14

A type of strongly radicial polynomials

Atsushi Nakajima (Okayama University)

Throughout the present note, R will represent a commutative algebra over GF(p). 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 $\underline{H}_u$ the free Hopf algebra over R with basis $\{1, \delta, \dots, \delta^{p-1}\}$ whose Hopf algebra structure is given by

$\delta^p = 0$, $\Delta(\delta) = \delta\otimes 1 + 1\otimes\delta + u(\delta\otimes\delta)$, $\Delta(\delta^j) = \Delta(\delta)^j$,

$\varepsilon(\delta) = 0$, $\varepsilon(\delta^j) = \varepsilon(\delta)^j$, $\lambda(\delta) = \sum_{i=1}^{p-1}(-1)^i u^{i-1}\delta^i$ and

$\lambda(\delta^j) = \lambda(\delta)^j$ $(1 \leqq j \leqq p-1)$,

where Δ, ε and λ are the comultiplication, counit and antipode of H_u, respectively.

In this note we study on quadratic extension and H_u-Hopf Galois extension of R.

Let A be a commutative R-algebra and $\mu: A\otimes A \longrightarrow A$ a multiplication map. A is called a <u>purely inseparable</u> algebra in the sense of Sweedler if $\mathrm{Ker}(\mu) \subseteq J(A\otimes A)$, the Jacobson radical of $A\otimes A$ ([5, Def.1 and Lemma 1 (a)]). A is called a <u>strongly radicial</u> if A is f. g. projective R-module and $\mathrm{Ker}(\mu)$ is nilpotent.

First, we have the following

Theorem 1. Let $A = R[X]/(X^2 - rX - s)$ $(r, s \in R)$. Assume $p = 2$. Then

(1) A is purely inseparable if and only if $r \in J(R)$.

(2) A is strongly radicial if and only if r is nilpotent.

Proof. Noting that $\mathrm{Ker}(\mu)$ is generated by $y = x\otimes 1 + 1\otimes x$ as A-module and $y^2 = ry$, (2) is clear. Thus we prove (1). If $r \in J(R)$ then $r \in J(A\otimes A)$, since $A\otimes A$ is integral over R. Thus $y^2 = ry \in J(A\otimes A)$, whence it follows that $y \in J(A\otimes A)$.

Let $y \in \mathrm{Ker}(\mu) \subseteq J(A\otimes A)$. Then $1 + cy$ is invertible 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 we obtain

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

As is easily seen

$$(1+cr)^2 \begin{pmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \end{pmatrix} = (1+cr) \begin{pmatrix} 1+cr \\ c \\ c \\ 0 \end{pmatrix}.$$

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 ([2, p.161, Cor.]). We have thus the following

(*) For any $c \in R$, there exists $t \in R$ such that

$$(1 + cr)t = c$$

If $r \notin J(R)$, then there exists a maximal ideal M in R such that $R = Rr + M$. Put $1 = r_0 r + m$ ($r_0 \in R$, $m \in M$). Then by (*), there exists $t \in R$ such that $(1 + r_0 r)t = r_0$. Thus $r_0 = (1 + r_0 r)t = mt \in M$. This implies a contradiction $1 \in M$. Hence $r \in J(R)$.

<u>Remark 2</u>. Let $A = R[X]/(X^2 - rX - s)$. Assume 2 is invertible in R. Then we can show the following:

(1) A is purely inseparable if and only if $r^2 + 4s \in J(R)$.

(2) A is strongly radicial if and only if $r^2 + 4s$ is nilpotnet.

Now, we consider H_u-Hopf Galois extension of R.

An R-algebra A is called a <u>projective R-algebra</u> if A is a projective R-module and R is an R-direct summand of A. An R-algebra A is called an <u>H_u-module algebra</u> if A is an H_u-module such that the followings hold: For any $a, b \in A$,

$$\delta(ab) = a\delta(b) + \delta(a)b + u\delta(a)\delta(b) \quad \text{and} \quad \delta(1) = 0.$$

For an H_u-module algebra A, the <u>smash product</u> $A \# H_u$ is equal to $A \otimes H_u$ as an R-module but with multiplication

$$(a \# h)(b \# k) = \sum_{(h)} a(h_{(1)}b) \# h_{(2)}k$$

where $\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$. In our case we have

$$(1 \# \delta)(a \# 1) = \delta(a) \# 1 + a \# \delta + u\delta(a) \# \delta.$$

A commutative R-algebra A is called an <u>H_u-Hopf Galois extension</u>

of R if A is a f. g. projective H_u-module algebra and the map $\phi: A \# H_u \longrightarrow Hom_R(A, A)$ defined by $\phi(a \# h)(x) = ah(x)$ is an R-algebra isomorphism. Note that A is an H_u-Hopf Galois extension of R if and only if A is a Galois $H^* = Hom_R(H, R)$-object in the sense of Chase-Sweedler ([1, Th.9.3]).

Theorem 3 ([3, Cor.1.6]). Let A be a f. g. projective H_u-module algebra. Assume $p = 2$. Then the followings are equivalent.

(1) A is an H_u-Hopf Galois extension of R.

(2) There exists an element $x \in A$ such that $\delta(x)$ is invertible in R and $x^2 = ux + s$ for some $s \in R$. When this is the case, A is a free R-module with basis $\{1, x\}$.

This theorem is generalized as follows.

Theorem 4 ([4]). If A is an H_u-Hopf Galois extension of R, then there exists $x \in A$ such that $\delta(x) = 1$ and $x^p = u^{p-1}x + r_0$ for some $r_0 \in R$. When this is the case $\{1, x, \ldots, x^{p-1}\}$ is a free basis of A. Conversely, let $f(X) = X^p - r_1X - r_0 \in R[X]$. If there exists $v \in R$ such that $v^{p-1} = r_1$, then $A = R[X]/(f(X))$ is an H_v-Hopf Galois extension of R.

Remark 5. In Th.4, if u is nilpotent, then A is purely inseparable, and if $u = 1$, then $f(X)$ is an Artin-Schreier polynomial. In detail, see [4].

These extensions are p-extensions. We give a simple example of p^m-extension. Assume $p = 2$. Let H be a Hopf algebra with free basis $\{1, \delta, \delta^2, \delta^3\}$ such that the Hopf algebra structure is defined by

$$\delta^4 = 0, \quad \Delta(\delta) = \delta \otimes 1 + 1 \otimes \delta + u(\delta \otimes \delta), \quad \Delta(\delta^j) = \Delta(\delta)^j,$$

$$\varepsilon(\delta) = 0, \quad \varepsilon(\delta^j) = \varepsilon(\delta)^j, \quad \lambda(\delta) = \sum_{i=1}^{3}(-1)^i u^{i-1}\delta^i \quad \text{and}$$

$$\lambda(\delta^j) = \lambda(\delta)^j \quad (1 \leqq j \leqq 3).$$

Since H is a Galois H-object with comodule structure map Δ: $H \longrightarrow H \otimes H$ ([1, Prop.9.1]), H has an H^*-module algebra structure defined by $h^* \rightharpoonup h = \sum_{(h)} h^*(h_{(1)})h_{(2)}$. Thus H is an H^*-Hopf Galois extension of R. Replacing H with H^*, H^* is an H-Hopf Galois extension of R. Using the H^*-module structure, it can be seen that

$$H^* \cong R[X]/(X^2 - uX) \otimes R[Y]/(Y^2 - u^2 Y)$$

as H-Hopf Galois extension, where X, Y are indeterminates. This extension is not isomorphic to cyclic extension. A Hopf algebra which corresponds to a cyclic extension is not H_u-type.

References

[1] S. U. Chase and M. E. Sweedler: Hopf Algebras and Galois Theory, Lecture notes in Math. 97, Springer-Verlag, Berlin, 1969.

[2] N. H. McCoy: Rings and Ideals, Carus Math. Monograph 8, The Math. Ass. Amer. 1948.

[3] A. Nakajima: Free algebras and Galois objects of rank 2 (to appear, Okayama Math. J).

[4] A. Nakajima: Some type of Hopf Galois extensions (in preparation).

[5] M. E. Sweedler: Hopf Algebras, Benjamin, New York, 1969.

[6] M. E. Sweedler: Purely inseparable algebras, J. Alg. 35 (1975), 342-355.