Math. J. Okayama Univ. 29 (1987), 109—117

ON HOPF GALOIS EXTENSIONS, AZUMAYA ALGEBRAS AND SKEW POLYNOMIAL RINGS

Dedicated to Professor Hisao Tominaga on his 60th birthday

ATSUSHI NAKAJIMA

In [4], S. Ikehata gave some characterizations of Galois extensions of commutative rings and applied these results to construct Azumaya algebras from skew polynomial rings in [5]. The essential part in his main theorems [5, Theorems 2.2 and 3.3] is to determine H-separable polynomials in skew polynomial rings. In this paper, we give a characterization of Hopf Galois extensions which is a generalization of [4, Theorem 2], and show that H-separable polynomials in the skew polynomial rings are closely related to the dual Hopf Galois extensions. Moreover we give another examples of H-separable polynomials.

Throughout the following, R is a commutative ring with identity 1, and A is a Hopf algebra over R which is a finitely generated projective R-module unless otherwise stated. An R-algebra means a ring extension of R with the same identity 1 such that R is contained in the center. Each $\otimes$, Hom, etc. is taken over R and each map is R-linear. As for notations and terminologies of Hopf algebras and Hopf Galois extensions used here, we follow [1], [6] and [9].

Let A be a Hopf algebra which is not necessary finitely generated projective R-module. Let S be an R-algebra which is a left A-module. Then $S \otimes S$ and R are left A-modules by the comultiplication Δ and the counit ε of A:

$$a(x \otimes y) = \sum_{(a)} a^{(1)}x \otimes a^{(2)}y \quad \text{where} \quad \Delta(a) = \sum_{(a)} a^{(1)} \otimes a^{(2)}$$

and

$$ar = \varepsilon(a)r,$$

respectively (a in A, x, y in S and r in R). An R-algebra S is called a left A-*module algebra* if S is a left A-module such that the structure maps

$$\mu_S\colon S \otimes S \to S(x \otimes y \mapsto xy) \quad \text{and} \quad 1_S\colon R \to S(r \mapsto r)$$

are left A-module homomorphisms. These conditions say that

$$a(xy) = \sum_{(a)} (a^{(1)}x)(a^{(2)}y) \quad \text{and} \quad a1 = \varepsilon(a)1.$$

Let T be an R-algebra. T is called an *A-comodule algebra* if T is a right A-comodule with the structure map ρ: $T \to T \otimes A$ such that ρ is an R-algebra homomorphism. For an A-module algebra S and an A-comodule algebra T, we can define the *smash product algebra* $S \# T$ which is equal to $S \otimes T$ as R-module but the multiplication given by

$$(s_1 \# t_1)(s_2 \# t_2) = \sum_{(t_1)} s_1(t_1^{(1)} s_2) \# t_1^{(0)} t_2,$$

where $\rho(t_1) = \sum_{(t_1)} t_1^{(0)} \otimes t_1^{(1)}$ is in $T \otimes A$. As is easily seen, $S \# T$ is an R-algebra with identity $1 \# 1$ and the maps

$$i_S:\ S \to S \# T (s \mapsto s \# 1), \quad i_T:\ T \to S \# T (t \mapsto 1 \# t)$$

are R-algebra homomorphisms. Since A is an A-comodule algebra by Δ, we can construct the usual smash product $S \# A$.

Let A be a Hopf algebra. A left A-module algebra S is called an *A-Hopf Galois extension* of R if S is a finitely generated projective faithful R-module and the map ϕ: $S \# A \to \mathrm{Hom}(S, S)$ defined by $\phi(s \# a)(x) = sa(x)$ is an R-algebra isomorphism. Since S is a faithfully flat R-module, S is an A-Hopf Galois extension of R if and only if S is a *Galois $A^* = \mathrm{Hom}(A, R)$-object* in the sense of Chase-Sweedler [1, Theorem 9.3]. When this is the case, $S^A = \{s \text{ in } S \mid as = \varepsilon(a)s \text{ for any } a \text{ in } A\}$ is equal to R. For details, we refer to [6].

Definition 1. A *Morita context* consists of the following data

(a) R-algebras S and T.

(b) An (S, T)-bimodule P and a (T, S)-bimodule Q, both centralized by R; i.e., $rx = xr$ for all x in P or Q, r in R.

(c) An (S, S)-bimodule homomorphism $\{\ ,\ \}$: $P \otimes {}_T Q \to S$ and a (T, T)-bimodule homomorphism $[\ ,\ ]$: $Q \otimes {}_S P \to T$. Given x in P, y in Q, we shall denote the images of $x \otimes y$ and $y \otimes x$, under these mappings, by $\{x, y\}$ and $[y, x]$, respectively. These mappings will be called *pairings*.

(d) The following equations hold for all x, z in P and y, w in Q

$$\{x, y\}z = x[y, z], \quad [y, z]w = y\{z, w\}.$$

The Morita context will be called *strict* if the pairings $\{\ ,\ \}$ and $[\ ,\ ]$ are surjective ([1, Chap. II, §8]).

Definition 2. Let S be a left A-module algebra. Assume that $S^A = R$. Let $D = S \# A$, and $Q = D^A = \{w \text{ in } S \# A \mid (1 \# a)w = \varepsilon(a)w$ for any a in A }, a right ideal in D. Define pairings { , }: $S \otimes {}_R Q \to D$, [,]: $Q \otimes {}_D S \to S^A = R$ by the formulae

$$\{x, w\} = (x \# 1)w, \ [w, x] = w(x) \ (x \text{ in } S \text{ and } w \text{ in } Q),$$

where S is a left D-module via $(s \# a)(x) = sa(x)$. Note that the definition of Q guarantees that [,] is well defined. Then the algebras D and R, the (D, R)-bimodule S, the (R, D)-bimodule Q, and the pairings { , }, [,] constitute a Morita context ([1, Definition and Remarks 9.4]).

Lemma 3. *Let S be a left A-module algebra, and $S^A = R$. Then the map*

$$\alpha: \mathrm{Hom}_{S\# A}(S, S \# A) \to (S \# A)^A$$

defined by $\alpha(f) = f(1)$ is an $(R, S \# A)$-bimodule isomorphism, where the right $S \# A$-module structure of $\mathrm{Hom}_{S\# A}(S, S \# A)$ *is given by* $(f(s \# a))(x) = f(x)(s \# a)$.

Proof. For any a in A and f in $\mathrm{Hom}_{S\# A}(S, S \# A)$, we have $(1 \# a)f(1) = f((1 \# a)1) = f(\varepsilon(a)1) = \varepsilon(a)f(1)$ and so α is well defined. Clearly α is one to one and $(R, S \# A)$-bimodule homomorphism. If $s \# a$ is in $(S \# A)^A$, then the map $f_{s\# a}$ defined by $f_{s\# a}(x) = (x \# 1)(s \# a)$ is a left $S \# A$-module homomorphism and thus α is an isomorphism. Q.E.D.

Let T be a ring extension of R with the common identity 1. If $T \otimes T$ is isomorphic to a direct summand of a finite direct sum of T as a (T, T)-bimodule, then T is called an *H-separable extension* of R.

Now, we have the following theorem which is a generalization of [4, Theorem 2].

Theorem 4. *Let S be a left A-module algebra. Assume that $S^A = R$. Then the following statements are equivalent.*

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

(2) *$S \# A$ is an Azumaya R-algebra.*

(3) *$S \# A$ is an H-separable extension of S.*

(4) *The Morita context of* Definition 2 *is strict.*

Proof. (1) ⇒ (2) follows from definition. (2) ⇒ (3). Since $S \# A$ is projective left S-module, it follows from [4, Theorem 1]. (3) ⇒ (4) ⇒ (1). By [4, Lemma], the left $S \# A$-module S is a generator, i.e., the map τ:

$S\otimes \mathrm{Hom}_{S\# A}(S, S\# A)\to S\# A$ defined by $\tau(s\otimes f)=f(s)$ is an epimorphism. By Lemma 3, we have the following commutative diagram

$$\begin{array}{ccc} S\otimes \mathrm{Hom}_{S\# A}(S, S\# A) & \xrightarrow{\;1\otimes\alpha\;} & S\otimes(S\# A)^{A} \\ {\scriptstyle\tau}\searrow & & \swarrow{\scriptstyle\{\ ,\ \}} \\ & S\# A & \end{array}$$

Since τ is an epimorphism, $\{\ ,\ \}$ is an epimorphism and by [1, Theorem 8.4], the Morita context defined in Definition 2 is strict. Thus by the same argument as used in the proof of [1, Theorem 9.6], S is an A-Hopf Galois extension of R. Q.E.D.

Let S be a commutative left A-module algebra over R and R in S^{A}. Let $R< X_1,\dots,X_n>$ be the (non-commutative) free algebra on n-variables. Suppose that $R< X_1,\dots,X_n>$ is a right A-comodule algebra. We say that $S[X_1,\dots,X_n;\ A]=S\# R< X_1,\dots,X_n>$ is a *generalized skew polynomial ring of type* A. In this definition, we do not assume that A is a finitely generated projective R-module.

Example 5. Let S be a commutative R-algebra. Let σ be an R-algebra automorphism of S and let D be a σ-derivation of S (i.e., D is an R-module endomorphism of S such that $D(xy)=D(x)\sigma(y)+xD(y)$). We set

$$S^{\sigma}=\{s \text{ in } S\mid \sigma(s)=s\},\ S^{D}=\{s \text{ in } S\mid D(s)=0\}.$$

Then R is contained in $S^{\sigma}\cap S^{D}$. Let $R[\sigma, D]$ be the commutative free R-algebra on variables σ, D which has coalgebra structure maps and antipode as follows:

$$\Delta(\sigma^{i})=\sigma^{i}\otimes\sigma^{i},\quad \varepsilon(\sigma^{i})=1,\quad \lambda(\sigma^{i})=\sigma^{-i},$$
$$\Delta(D^{i})=(D\otimes\sigma+1\otimes D)^{i},\quad \varepsilon(D^{i})=0 \quad\text{and}\quad \lambda(D^{i})=(-D\sigma^{-1})^{i}.$$

As is easily seen, $R[\sigma, D]$ is a Hopf algebra and S is a left $R[\sigma, D]$-module algebra. Let $R[X]$ be the polynomial ring over R. Define an R-linear map ρ: $R[X]\to R[X]\otimes R[\sigma, D]$ by

$$\rho(X^{i})=(X\otimes\sigma+1\otimes D)^{i}.$$

Then $R[X]$ is a right $R[\sigma, D]$-comodule algebra. Let $S[X;\ \sigma, D]$ be the *skew polynomial ring* in which the multiplication is given by

$$Xs = \sigma(s)X+D(s) \ (s \text{ in } S),$$

(cf. [3]). We define a map ψ: $S \# R[X] \to S[X; \sigma, D]$ by $\psi(\sum s_i \# X^i) = \sum s_i X^i$. Then it is easy to check that ψ is an R-algebra isomorphism. Therefore the skew polynomial ring $S[X; \sigma, D]$ is a special case of our generalized skew polynomial ring.

In the following, we denote $R[\sigma, 0]$ (resp. $R[1, D]$) by $R[\sigma]$ (resp. $R[D]$). When this is the case, we also denote $S[X; \sigma, 0]$ (resp. $S[X; 1, D]$) by $S[X; \sigma]$ (resp. $S[X; D]$), which is called the *skew polynomial ring of automorphism* (resp. *derivation*) *type*.

A Hopf algebra A is called a *free Hopf algebra* if there exists a (non-commutative) free R-algebra $R < X_1,\dots,X_n >$ with Hopf algebra structure such that A is isomorphic to $R < X_1,\dots,X_n >$ as Hopf algebras. If A is a finitely generated free Hopf algebra, then there exist polynomials $h_1,\dots,h_m$ in $R < X_1,\dots,X_n >$ such that A is isomorphic to $R < X_1,\dots,X_n > /(h_1,\dots, h_m)$ as Hopf algebras. Since this Hopf algebra isomorphism is an A-comodule algebra isomorphism, $S \# A$ is isomorphic to $S \# R < X_1,\dots, X_n > /(h_1,\dots,h_m)$ as R-algebras for any left A-module algebra S. Thus by Theorem 4, we have the following theorem (cf. [5, Theorems 2.2 and 3.3]).

Theorem 6. *Let A be a free Hopf algebra and let S be an R-algebra. Assume that S is a left A-module algebra such that $S^A = R$. Then the following statements are equivalent.*

(1) *A is a finitely generated free Hopf algebra and S is an A-Hopf Galois extension of R.*

(2) *There exist polynomials $g_1,\dots,g_m$ in $R < X_1,\dots,X_n >$ satisfying the following conditions:*

(a) *$R < X_1,\dots,X_n > /(g_1,\dots,g_m) \cong A$ as right A-comodule algebras.*

(b) *$S \# R < X_1,\dots,X_n > /(g_1,\dots,g_m)$ is an Azumaya algebra.*

(3) *There exist polynomials $h_1,\dots,h_m$ in $R < X_1,\dots,X_n >$ satisfying the following conditions:*

(a) *$R < X_1,\dots,X_n > /(h_1,\dots,h_m) \cong A$ as right A-comodule algebras.*

(b) *$S \# R < X_1,\dots,X_n > /(h_1,\dots,h_m)$ is an H-separable extension of S.*

Let A be a Hopf algebra which is not necessary finitely generated projective R-module. Let $R[X_1,\dots,X_n]$ be the polynomial ring on n-variables which is a right A-comodule algebra, and let $\{f_1,\dots,f_m\}$ be monic polynomials in $R[X_1,\dots,X_n]$. A set $\{f_1,\dots,f_m\}$ is called a *set of comodule polynomials* if the ideal generated by $\{f_1,\dots,f_m\}$ is a right A-subcomodule in $R[X_1,\dots,X_n]$. Let S be a left A-comodule algebra over R. A set of comodule polynomials $\{f_1,\dots,f_m\}$ in $R[X_1,\dots,X_n]$ is said to be *H-separable* in $S[X_1,\dots,X_n;\ A]$ if $S[X_1,\dots,X_n;\ A]/(f_1,\dots,f_m)$ is an H-separable extension of S.

Let A be a Hopf algebra, S an A^*-comodule algebra and T an A-comodule algebra. In [2], J. Gamst and K. Hoechsman defined a smash product $S \# T$ as follows: As an R-module $S \# T$ equals to $S \otimes T$ and the product is defined by

$$(s_1 \# t_1)(s_2 \# t_2) = \textstyle\sum_{(s_2),(t_1)} s_1 s_2^{(0)} < s_2^{(1)},\ t_1^{(1)} > \otimes t_1^{(0)} t_2,$$

where ρ_S: $S \to S \otimes A^*$ (resp. ρ_T: $T \to T \otimes A$) is defined by $\rho_S(s_2) = \sum_{(s_2)} s_1^{(0)} \otimes s_2^{(1)}$(resp. $\rho_T(t_1) = \sum_{(t_1)} t_1^{(0)} \otimes t_1^{(1)}$) and $< , >$: $A^* \otimes A \to R$ is the evaluation. Since S is an A^*-comodule algebra, S is an A-module algebra by $as = \sum_{(s)} < s^{(1)},\ a > s^{(0)}$. When this the case, we can construct our smash product $S \# T$, which is equal to that of [2].

Theorem 7. *Let S be a commutative A-Hopf Galois extension of R. If $\{f_1,\dots,f_m\}$ is a set of comodule polynomials in $R[X_1,\dots,X_n]$ such that $R[X_1,\dots,X_n]/(f_1,\dots,f_m)$ is an A^*-Hopf Galois extension of R, then $\{f_1,\dots,f_m\}$ is H-separable in $S[X_1,\dots,X_n;\ A]$.*

Proof. By [2, Theorem 1], $S \# R[X_1,\dots,X_n]/(f_1,\dots,f_m)$ is an Azumaya R-algebra and so by [4, Theorem 1], $S \# R[X_1,\dots,X_n]/(f_1,\dots,f_m)$ is an H-separable extension of S. Since $S \# R[X_1,\dots,X_n]/(f_1,\dots,f_m)$ is isomorphic to $S[X_1,\dots,X_n;\ A]/(f_1,\dots,f_m)$, $\{f_1,\dots,f_m\}$ is H-separable in $S[X_1,\dots,X_n;\ A]$. Q.E.D.

Example 8. Let R be a commutative algebra over the prime field $GF(2)$. Define a commutative Hopf algebra $A = R[\sigma, D]$ by

algebra structure: $\sigma^4 = 1$ and $D^2 = \sigma^2 + 1$,
coalgebra structure: $\Delta(\sigma) = \sigma \otimes \sigma$, $\Delta(D) = D \otimes \sigma + 1 \otimes D$,
$\varepsilon(\sigma) = 1$ and $\varepsilon(D) = 0$,
antipode: $\lambda(\sigma) = \sigma^{-1} (= \sigma^3)$ and $\lambda(D) = D\sigma^{-1}$.

Let $R[X, Y]$ be the polynomial ring on two variables. Define a map ρ: $R[X, Y] \to R[X, Y] \otimes A$ by

$$\rho(X) = X \otimes \sigma,\ \rho(Y) = Y \otimes \sigma + 1 \otimes D \text{ and } \rho(X^i Y^j) = \rho(X)^i \rho(Y)^j.$$

Then $R[X, Y]$ is a right A-comodule algebra via ρ. When this is the case, the ideal generated by X^4+1 and Y^2+X^2+1 is a right A-subcomodule in $R[X, Y]$. Since $R[X, Y]/(X^4+1, Y^2+X^2+1)$ is isomorphic to $R[\sigma, D]$ as $R[\sigma, D]$-comodule algebras and $R[\sigma, D]$ is a Galois $R[\sigma, D]$-object by [1, Proposition 9.1], i.e., $R[X, Y]/(X^4+1, Y^2+X^2+1)$ is a $R[\sigma, D]^*$-Hopf Galois extension of R, the pair of polynomials $\{X^4+1, Y^2+X^2+1\}$ satisfies the condition in Theorem 7. Moreover if S is a commutative $R[\sigma, D]$-Hopf Galois extension of R, then by Theorem 6, $S \# R[X, Y]/(X^4+1, Y^2+X^2+1) \cong S[X, Y;\ \sigma, D]/(X^4+1, Y^2+X^2+1)$ is Azumaya R-algebra.

Theorems 6 and 7 give some information in relation to Hopf algebras, H-separable polynomials in skew polynomial rings and Azumaya algebras. Under suitable conditions, H-separable polynomials in $S[X;\ \sigma]$ (resp. $S[X;\ D]$) were completely determined by S. Ikehata [5]. There are closely related to A^*-Hopf Galois extension of R, where $A = R[\sigma]$ or $A = R[D]$.

Now let A be a Hopf algebra which is not necessary finitely generated projective R-module. Let S be a commutative A-module algebra such that $S^A = R$. Let $f(X)$ be a monic polynomial in $R[X]$ such that $S[X;\ A]f(X) = f(X)S[X;\ A]$.

Automorphism type. Assume that σ is an R-algebra automorphism of S and $A = R[\sigma]$. If $f(X)$ is H-separable in $S[X;\ \sigma]$, then by [5, Theorem 2.1], the order of σ is m and $f(X) = X^m+r$, where r is invertible in R. When this is the case, $R[X]/(X^m+r)$ has an $R[\sigma]$-comodule structure map ρ: $R[x] \to R[x] \otimes R[\sigma]$ defined by $\rho(x) = x \otimes \sigma$, where $x = X+(X^m+r)$. As is easily checked, ρ induces an R-algebra isomorphism $R[x] \otimes R[x] \cong R[x] \otimes R[\sigma]$, which shows that $R[x]$ is an $R[\sigma]^*$-Hopf Galois extension of R (cf. [1, Chapter I, § 4]).

Derivation type. Let R be a commutative algebra over the prime field $GF(p)$. Assume that D is a derivation of S and $A = R[D]$. If $f(X)$ is H-separable in $S[X;\ D]$, then by [5, Lemma 1.6 and Theorem 3.3],

$$f(X) = X^{p^e} - u_{e-1}X^{p^{e-1}} - \cdots - u_1 X^p - u_0 X - u_{-1}\ (u_i \text{ in } R)$$

and $f(D) = -u_{-1}$. Define a map ρ: $R[x] \to R[x] \otimes R[D]$ by $\rho(x) = x \otimes 1 + 1 \otimes D$, where $x = X+(f(X))$. Then we can check that ρ gives an $R[D]$-comodule structure on $R[x]$ and induces an R-algebra isomorphism $R[x] \otimes$

$R[x] \cong R[x] \otimes R[D]$, which shows that $R[x]$ is an $R[D]^*$-Hopf Galois extension of R (cf. [8, Theorem 1.3]). Under the above assumptions and notations, we get the following

Theorem 9. *If $f(X)$ is H-separable in $S[X; \sigma]$ (resp. $S[X; D]$), then $R[X]/(f(X))$ is an $R[\sigma]^*$ (resp. $R[D]^*$)-Hopf Galois extension of R.*

By [1, Chapter I, § 4], [8, Theorem 1.4], [2] and [5, Theorems 2.1 and 3.1], we have the converse case of Theorem 9.

Theorem 10. *Let $f(X)$ be a monic polynomial in $R[X]$.*

(1) *If σ is of order m and if $R[X]/(f(X))$ is an $R[\sigma]^*$-Hopf Galois extension of R, then for any $R[\sigma]$-Hopf Galois extension S of R, $f(X)S[X; \sigma] = S[X; \sigma]f(X)$ and $f(X)$ is H-separable in $S[X; \sigma]$.*

(2) *Let R be a commutative algebra over the prime field $GF(p)$. If $D^{p^e} - u_{e-1}D^{p^{e-1}} - \cdots - u_1D^p - u_0D = 0$ (u_i in R) and if $R[X]/(f(X))$ is an $R[D]^*$-Hopf Galois extension of R, then for any $R[D]$-Hopf Galois extension S of R, $f(X)S[X; D] = S[X; D]f(X)$ and $f(X)$ is H-separable in $S[X; D]$.*

Remark 11. In the skew polynomial rings of automorphism type and derivation type, the following hold by [3, Corollary 1.5 and Lemma 1.6]. Let $f(X)$ be in $S[X; \xi]$ and $f(X)S[X; \xi] = S[X; \xi]f(X)$, where $\xi = \sigma$ or $\xi = D$. Then, $f(X)$ is in $R[X]$ when $f(X)$ is in $S[X; \sigma]$ and S is a semiprime ring, or when $f(X)$ is in $S[X; D]$. Thus the assumption that $f(X)$ is contained in $R[X]$ in Theorem 10 is reasonable.

Finally we give the following example which is an H-separable polynomial of another case.

Example 12. Let R be a commutative algebra over the prime field $GF(p)$. Let u be a fixed element in R and $H(u, p^e)$ the Hopf algebra defined in [7], that is, $H(u, p^e)$ has an R-free basis $1, D, \ldots, D^{p^e-1}$ and a Hopf algebra structure is given by the following;

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

For a polynomial ring $R[X]$, we define an R-module homomorphism ρ: $R[X]$

$\to R[X] \otimes H(u, p^e)$ by $\rho(X^i) = (X \otimes \sigma + 1 \otimes D)^i$, where $\sigma = 1 + uD$. Then it is easy to see that $R[X]$ is a right $H(u, p^e)$-comodule algebra by ρ. Let S be an $H(u, p^e)$-module algebra over R. Since $\Delta(\sigma) = \sigma \otimes \sigma$, $\varepsilon(\sigma) = 1$ and $\Delta(D) = \sigma \otimes D + D \otimes 1$, D is a σ-derivation on S and thus we can construct the skew polynomial ring $S[X; \sigma, D]$. Then by

$$X^{p^i}s = \sigma^{p^i}(s)X^{p^i} + D^{p^i}(s) \ (s \text{ in } S),$$

we have $X^{p^e}s = sX^{p^e}$. Moreover $S \# H(u, p^e)$ is canonically isomorphic to $S[X; \sigma, D]/X^{p^e}S[X; \sigma, D]$ as R-algebras. Therefore if S is an $H(u, p^e)$-Hopf Galois extension of R, then $S[X; \sigma, D]/X^{p^e}S[X; \sigma, D]$ is an Azumaya R-algebra and by [4, Theorem 1], $S[X; \sigma, D]/X^{p^e}S[X; \sigma, D]$ is an H-separable extension of S. This shows that X^{p^e} is an H-separable polynomial in $S[X; \sigma, D]$. When this is the case, $R[X]/(X^{p^e})$ is also an $H(u, p^e)^*$-Hopf Galois extension of R. Finally we note that if we set $\theta = D - uD$, then θ is also a σ-derivation and we can prove that $S[X; \sigma, \theta]/(X^{p^e} - 1)\, S[X; \sigma, \theta]$ is Azumaya R-algebra. Thus $X^{p^e} - 1$ is H-separable in $S[X; \sigma, \theta]$.

References

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

[2] J. Gamst and K. Hoechsmann: Quaternions generalises, C. R. Acad. Sci. Paris, **269** (1969), 560–562.

[3] S. Ikehata: On separable polynomials and Frobenius polynomials in skew polynomial rings, Math. J. Okayama Univ. 22 (1980), 115–129.

[4] S. Ikehata: A note on Azumaya algebras and H-separable extensions, Math. J. Okayama Univ. 23 (1981), 17–18.

[5] S. Ikehata: Azumaya algebras and skew polynomial rings, Math. J. Okayama Univ. 23 (1981), 19–32.

[6] H. F. Kreimer and M. Takeuchi: Hopf algebras and Galois extensions of an algebra, Indiana Univ. Math. J. 30 (1981), 675–692.

[7] A. Nakajima: A certain type of commutative Hopf Galois extensions and their groups, Math. J. Okayama Univ. 24 (1982), 137–152.

[8] A. Nakajima: P-polynomials and H-Galois extensions, J.Alg. **110**(1987), 124–133.

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

Okayama University
Okayama 700, Japan

(Received March 12, 1986)