

ON THE IKEHATA THEOREM FOR H -SEPARABLE SKEW POLYNOMIAL RINGS

GEORGE SZETO AND LIANYONG XUE

ABSTRACT. Let B be a ring with 1, ρ an automorphism of B , C the center of B , $B[x; \rho]$ a skew polynomial ring with a free basis $\{1, x, x^2, \dots, x^{n-1}\}$ over B , $x^n = v$ a unit in B such that $\rho(v) = v$. Then it is shown that $B[x; \rho]$ is a H -separable extension of B if and only if C is a ρ -Galois algebra over C^ρ . This proves the Ikehata theorem for any order n .

1. INTRODUCTION.

Let B be a ring with 1, ρ an automorphism of B , C the center of B , B^ρ and C^ρ the sets of elements fixed under ρ in B and C respectively, $B[X; \rho]$ a skew polynomial ring in which $Xb = \rho(b)X$ for all $b \in B$. For a monic polynomial $f(X)$ in $B[X; \rho]$ of degree m for some integer m such that $f(X)B[X; \rho] = B[X; \rho]f(X)$, $B[x; \rho]$ is called a skew polynomial ring of degree m with a basis $\{1, x, x^2, \dots, x^{m-1} \mid x = X + f(X)B[X; \rho]\}$ over B . In [5], S. Ikehata showed that $B[X; \rho]$ contains a H -separable polynomial $f(X)$ of degree p for some prime integer p (that is, $B[x; \rho]$ is a H -separable extension of B) if and only if C is a ρ -Galois extension of C^ρ where ρ restricted to C has order p . For any positive integer n not necessarily prime, let $f(X) = X^n - v$ be in $B[X; \rho]$ with v a unit in B^ρ and $f(X)B[X; \rho] = B[X; \rho]f(X)$, S. Ikehata and G. Szeto ([6]) showed that C is a ρ -Galois extension of C^ρ with Galois group $\langle \rho \rangle$ restricted to C of order n if and only if $B[x^k; \rho^k]$ is a H -separable extension of B for every divisor k of n . The purpose of the present paper is to show the above Ikehata theorem for any integer n , that is, C is a ρ -Galois algebra over C^ρ with Galois group $\langle \rho \rangle$ restricted to C of order n if and only if $B[x; \rho]$ is a H -separable extension of B where $x = X + (X^n - v)B[X; \rho]$ with v invertible in B^ρ . Moreover, when C is a ρ -Galois algebra over C^ρ with Galois group $\langle \rho \rangle$ of order n , we shall give some expression for the commutator subring of B^ρ in a H -separable skew polynomial ring $B[x; \rho]$ and show a characterization of the ρ -Galois extension B of B^ρ in terms of the $\bar{\rho}$ -Galois extension $B[x; \rho]$, where $\bar{\rho}$ is the inner automorphism of $B[x; \rho]$ induced by x . The present paper was revised under the suggestions of the referee. The authors would like to thank the referee for the valuable suggestions.

1991 *Mathematics Subject Classification.* : 16S30, 16W20.

Key words and phrases. Galois extensions of rings, H -separable extensions, Skew polynomial rings, Azumaya algebras.

2. PRELIMINARIES AND BASIC DEFINITIONS.

Throughout this paper, B will represent a ring with 1, ρ an automorphism of B , C the center of B , $B[x; \rho]$ a skew polynomial ring in which the multiplications are given by $xb = \rho(b)x$ for $b \in B$ and $x^n = v \in U(B^\rho)$, the set of units of B^ρ where B^ρ is the set of elements in B fixed under ρ , $\bar{\rho}$ the inner automorphism of $B[x; \rho]$ induced by x , that is, $\bar{\rho}(f) = xfx^{-1}$ for each $f \in B[x; \rho]$. We note that $\bar{\rho}$ restricted to B is ρ .

Let A be a subring of a ring S with the same identity 1. We denote $V_S(A)$ the commutator subring of A in S . We call S a separable extension of A if there exist $\{a_i, b_i \text{ in } S, i = 1, 2, \dots, m \text{ for some integer } m\}$ such that $\sum a_i b_i = 1$, and $\sum sa_i \otimes b_i = \sum a_i \otimes b_i s$ for all s in S where \otimes is over A , and a ring S is called a H -separable extension of A if $S \otimes_A S$ is isomorphic to a direct summand of a finite direct sum of S as a S -bimodule. An Azumaya algebra is a separable extension of its center. S is called a ρ -Galois extension of S^ρ if there exist elements $\{c_i, d_i \text{ in } S, i = 1, 2, \dots, m\}$ for some integer m such that $\sum_{i=1}^m c_i d_i = 1$ and $\sum_{i=1}^m c_i \rho^k(d_i) = 0$ for $0 < k < n$. The set $\{c_i, d_i\}$ is called a ρ -Galois system for S .

3. THE IKEHATA THEOREM.

In this section, we shall prove the Ikehata theorem as given in section 1. Some properties of H -separable skew polynomial rings and Galois algebras will take an important role in the proof of the theorem. For convenience, they are listed below:

Proposition 3.1 ([7], Theorem 3.3). *If C is a Galois extension over C^ρ with Galois group $\langle \rho/C \rangle$ of order n , then $B[x; \rho]$ is a H -separable extension of B .*

Proposition 3.2 ([10], Proposition 1.2). *Let T be a subring of a ring S with the same identity 1. If S is a H -separable extension of T such that T is a direct summand of S as a left T -module, then T satisfies the double centralizer property in S , that is, $V_S(V_S(T)) = T$.*

Proposition 3.3 ([2], Theorem 11, or [8], Theorem 4). *If a ring B is a Galois algebra over a commutative ring R with a cyclic Galois group $\langle \rho \rangle$ of order n for some integer n , then B is a commutative ring.*

Proposition 3.4 ([7], Theorem 3.2). *$B[x; \rho]$ is a H -separable extension of B if and only if $V_{B[x; \rho]}(B)$ is a Galois extension over C^ρ with Galois group $\langle \bar{\rho}/V_{B[x; \rho]}(B) \rangle$ of order n .*

Now we prove the Ikehata theorem. We begin with a lemma.

Lemma 3.5. *Let $J_i = \{a \in B \mid ba = a\rho^i(b) \text{ for all } b \in B\}$ and $I_i = \{y \in V_{B[x; \rho]}(B) \mid zy = y\bar{\rho}^{-i}(z) \text{ for all } z \in V_{B[x; \rho]}(B)\}$, $i = 0, 1, 2, \dots, n-1$. Then $V_{B[x; \rho]}(B) = \sum_{i=0}^{n-1} J_i x^i$ and $J_i x^i \subset I_i$.*

Proof. Let $\sum_{i=0}^{n-1} a_i x^i$ be an element in $V_{B[x;\rho]}(B)$. Then, for any $b \in B$, $b \sum_{i=0}^{n-1} a_i x^i = \sum_{i=0}^{n-1} a_i x^i b$, so $ba_i = a_i \rho^i(b)$ for $i = 0, 1, 2, \dots, n-1$. Hence a_i is in J_i . Conversely, for any a_i in J_i and b in B , $b \sum_{i=0}^{n-1} a_i x^i = \sum_{i=0}^{n-1} a_i \rho^i(b) x^i = \sum_{i=0}^{n-1} a_i x^i b$. So $\sum_{i=0}^{n-1} a_i x^i$ is in $V_{B[x;\rho]}(B)$. Thus, $V_{B[x;\rho]}(B) = \sum_{i=0}^{n-1} J_i x^i$. Moreover, for any $a_i x^i$ in $J_i x^i$ and z in $V_{B[x;\rho]}(B)$, $z(a_i x^i) = a_i z x^i = a_i x^i x^{-i} z x^i = a_i x^i \bar{\rho}^{-i}(z)$, so $a_i x^i$ in I_i . Thus, $J_i x^i \subset I_i$ for each i . \square

Theorem 3.6. *Let $B[x;\rho]$ be a skew polynomial ring. Then the following conditions are equivalent:*

- (a) $B[x;\rho]$ is a H -separable extension of B .
- (b) C is a ρ -Galois extension of C^ρ with Galois group $\langle \rho/C \rangle$ of order n .

Proof. (a) \implies (b): By Proposition 3.4, $V_{B[x;\rho]}(B)$ is a Galois algebra over C^ρ with Galois group $\langle \bar{\rho}/V_{B[x;\rho]}(B) \rangle$ of order n . So by Proposition 3.3, $V_{B[x;\rho]}(B)$ is a commutative ring. Moreover, by Lemma 3.5, $V_{B[x;\rho]}(B) = \sum_{i=0}^{n-1} J_i x^i$ and $J_i x^i \subset I_i$ for each $i = 0, 1, 2, \dots, n-1$. Since $I_i = \{y \in V_{B[x;\rho]}(B) \mid zy = y \bar{\rho}^{-i}(z) \text{ for all } z \in V_{B[x;\rho]}(B)\}$, $y(z - \bar{\rho}^{-i}(z)) = 0$ for each $y \in I_i$ and all $z \in V_{B[x;\rho]}(B)$. But, for each $i = 1, 2, \dots, n-1$, the ideal of $V_{B[x;\rho]}(B)$ generated by $\{(z - \bar{\rho}^{-i}(z)) \mid z \in V_{B[x;\rho]}(B)\}$ is $V_{B[x;\rho]}(B)$ ([1], Proposition 1.2-(5), Page 80). Therefore, $yV_{B[x;\rho]}(B) = 0$ for each $y \in I_i$, $i = 1, 2, \dots, n-1$. Hence $I_i = 0$ for each $i = 1, 2, \dots, n-1$. Thus $V_{B[x;\rho]}(B) = J_0 \subset B$; and so $V_{B[x;\rho]}(B) = C$. This implies part (b). (b) \implies (a) is a consequence of Proposition 3.1. \square

Remark . *The proof of the fact that $V_{B[x;\rho]}(B) = C$ as given in (a) \implies (b) in Theorem 3.6 can be done by using the double centralizer property $V_{B[x;\rho]}(V_{B[x;\rho]}(B)) = B$ from Proposition 3.2. Since $V_{B[x;\rho]}(B)$ was shown to be a commutative ring, so $V_{B[x;\rho]}(B) \subset V_{B[x;\rho]}(V_{B[x;\rho]}(B)) = B$. Hence $V_{B[x;\rho]}(B) = C$.*

4. COMMUTATOR SUBRINGS.

In this section, we shall give an expression for the commutator subring of B^ρ in a H -separable skew polynomial ring $B[x;\rho]$ and show a characterization of the ρ -Galois extension B of B^ρ in terms of the $\bar{\rho}$ -Galois extension $B[x;\rho]$.

Theorem 4.1. *Let $x^n = v \in U(C^\rho)$. If C is a ρ -Galois extension of C^ρ , then $V_{B[x;\rho]}(B^\rho) = \sum_{i=0}^{n-1} Cx^i$.*

Proof. To show that $\sum_{i=0}^{n-1} Cx^i = V_{B[x;\rho]}(B^\rho)$, we first show that $B = B^\rho C$. Since C is a ρ -Galois extension of C^ρ , B and $B^\rho C$ are ρ -Galois extension of B^ρ with the same ρ -Galois system as C . Noting that $B^\rho C \subset B$, we have $B^\rho C = B$. Then $V_{B[x;\rho]}(B^\rho) = \sum_{i=0}^{n-1} V_B(B^\rho) x^i = \sum_{i=0}^{n-1} V_B(B^\rho C) x^i = \sum_{i=0}^{n-1} V_B(B) x^i = \sum_{i=0}^{n-1} Cx^i$. \square

Corollary 4.2. *Let $x^n = v \in U(C^\rho)$. If C is a ρ -Galois extension of C^ρ , then $V_{B[x;\rho]}(B^\rho)$ is an Azumaya C^ρ -algebra.*

Proof. By Theorem 4.1, $V_{B[x;\rho]}(B^\rho) = \sum_{i=0}^{n-1} Cx^i$. But $x^n = v \in C^\rho$, so $\sum_{i=0}^{n-1} Cx^i = C[x;\rho]$, a skew polynomial ring over a commutative ring C . Thus, the corollary is a consequence of ([3], Theorem 2.2). \square

The Ikehata theorem as given in Theorem 3.6 characterizes the ρ -Galois extension C in terms of the H -separable skew polynomial ring $B[x;\rho]$ over B . Next we give a characterization of the ρ -Galois extension B of B^ρ in terms of the $\bar{\rho}$ -Galois skew polynomial ring $B[x;\rho]$ where $x^n = v \in U(B^\rho)$.

Theorem 4.3. *B is a ρ -Galois extension of B^ρ if and only if $B[x;\rho]$ is a $\bar{\rho}$ -Galois extension of $(B[x;\rho])^{\bar{\rho}}$.*

Proof. The necessity is clear because a ρ -Galois system for B can be used as a

$\bar{\rho}$ -Galois system for $B[x;\rho]$. For the sufficiency, suppose that $B[x;\rho]$ a $\bar{\rho}$ -Galois extension of $(B[x;\rho])^{\bar{\rho}}$. Then there is a $\bar{\rho}$ -Galois system for $B[x;\rho]$, $\{f_i, g_i$ in $B[x;\rho]$, $i = 1, 2, \dots, m\}$ for some integer m such that $\sum_{i=1}^m f_i g_i = 1$ and $\sum_{i=1}^m f_i \bar{\rho}^k(g_i) = 0$ for $0 < k < n$.

Let $f_i = \sum_{j=0}^{n-1} a_j^{(f_i)} x^j$, $g_i = \sum_{l=0}^{n-1} b_l^{(g_i)} x^l$, $a_{ij} = a_j^{(f_i)}$ for $i = 1, 2, \dots, m$ and $j = 0, 1, 2, \dots, n-1$, $b_{i0} = b_0^{(g_i)}$ for $i = 1, 2, \dots, m$, and $b_{ij} = \rho^j(b_{n-j}^{(g_i)})v$ for $i = 1, 2, \dots, m$, and $j = 1, 2, \dots, n-1$. We claim that $\{a_{ij}, b_{ij} \mid i = 1, 2, \dots, m$ and $j = 0, 1, 2, \dots, n-1\}$ is a ρ -Galois system for B . Since $\sum_{i=1}^m f_i g_i = 1$,

$$1 = \sum_{i=1}^m \left(\sum_{j=0}^{n-1} a_j^{(f_i)} x^j \right) \left(\sum_{l=0}^{n-1} b_l^{(g_i)} x^l \right) = \sum_{i=1}^m \left(\sum_{t=0}^{2n-2} \left(\sum_{j+l=t} a_j^{(f_i)} \rho^j(b_l^{(g_i)}) x^t \right) \right).$$

The constant terms on the right end of the above equation are those when $t = 0$ (that is, $j = l = 0$) and $t = n$ (that is, $l = n - j$). Hence

$$1 = \sum_{i=1}^m (a_0^{(f_i)} b_0^{(g_i)}) + \sum_{j=1}^{n-1} a_j^{(f_i)} \rho^j(b_{n-j}^{(g_i)})v = \sum_{i=1}^m \sum_{j=0}^{n-1} a_{ij} b_{ij}.$$

Since $\sum_{i=1}^m f_i \bar{\rho}^k(g_i) = 0$ for $0 < k < n$,

$$\begin{aligned} 0 &= \sum_{i=1}^m \left(\sum_{j=0}^{n-1} a_j^{(f_i)} x^j \right) \bar{\rho}^k \left(\sum_{l=0}^{n-1} b_l^{(g_i)} x^l \right) = \sum_{i=1}^m \left(\sum_{j=0}^{n-1} a_j^{(f_i)} x^j \right) \left(\sum_{l=0}^{n-1} \rho^k(b_l^{(g_i)}) x^l \right) \\ &= \sum_{i=1}^m \left(\sum_{t=0}^{2n-2} \left(\sum_{j+l=t} a_j^{(f_i)} \rho^{k+j}(b_l^{(g_i)}) \right) x^t \right). \end{aligned}$$

Hence,

$$0 = \sum_{i=1}^m (a_0^{(f_i)} \rho^k(b_0^{(g_i)})) + \sum_{j=1}^{n-1} a_j^{(f_i)} \rho^k(\rho^j(b_{n-j}^{(g_i)})v) = \sum_{i=1}^m \sum_{j=0}^{n-1} a_{ij} \rho^k(b_{ij})$$

for $0 < k < n$. Thus, $\{a_{ij}, b_{ij} \mid i = 1, 2, \dots, m \text{ and } j = 0, 1, 2, \dots, n - 1\}$ is a ρ -Galois system for B . □

We conclude the present paper with an example of a H -separable skew polynomial ring to demonstrate our results.

Example . Let $B = M_2(Z) \oplus M_2(Z)$, the direct sum of 2 by 2 matrices over the ring of integers Z , and $\rho(a \oplus b) = b \oplus a$ for all $a \oplus b$ in B . Then

- (1) The order of ρ is 2 and ρ is an automorphism of B .
- (2) ρ restricted to the center of B is isomorphic with ρ , where $C = Z \oplus Z$.
- (3) Let I_2 be the 2 by 2 identity matrix and 0_2 the 2 by 2 zero matrix.

Then, C is a

ρ -Galois extension of C^ρ with a ρ -Galois system $\{a_1 = I_2 \oplus 0_2, a_2 = 0_2 \oplus I_2; b_1 = I_2 \oplus 0_2, b_2 = 0_2 \oplus I_2\}$, that is, $a_1 b_1 + a_2 b_2 = I_2 \oplus I_2$, the identity of B and $a_1 \rho(b_1) + a_2 \rho(b_2) = 0_2 \oplus 0_2$, the zero of B . (4) Let $v = (-I_2) \oplus (-I_2)$, then v is a unit in C^ρ , such that $x^2 = v$. Thus $B[x; \rho]$ is a H -separable extension of B by Theorem 3.6.

- (5) $V_{B[x; \rho]}(B) = Z \oplus Z$.
- (6) $V_{B[x; \rho]}(Z \oplus Z) = M_2(Z) \oplus M_2(Z)$.
- (7) $V_{B[x; \rho]}(B^\rho) = \sum_{i=0}^1 Cx^i$.
- (8) $V_{B[x; \rho]}(B^\rho) = C[x; \rho]$ is an Azumaya C^ρ -algebra.

REFERENCES

- [1] F.R. DeMeyer and E. Ingraham: Separable Algebras over Commutative Rings, Volume 181, Springer Verlag, Berlin, Heidelberg, New York, 1971.
- [2] F.R. DeMeyer: Some notes on the general Galois theory of rings, Osaka J. Math., 2(1965), 117-127.
- [3] S. Ikehata: Azumaya algebras and skew polynomial rings, Math. J. Okayama Univ. 23(1981), 19-32.
- [4] S. Ikehata: Azumaya algebras and skew polynomial rings II, Math. J. Okayama Univ. 26(1984), 49-57.
- [5] S. Ikehata: On H -separable polynomials of prime degree, Math. J. Okayama Univ. 33(1991), 21-26.
- [6] S. Ikehata and G. Szeto: On H -separable polynomials in skew polynomial rings of automorphism type, Math. J. Okayama Univ. 34(1992), 49-55.
- [7] S. Ikehata and G. Szeto: On H -skew polynomial rings and Galois extensions, Rings, Extension and Cohomology (Evanston, IL, 1993), 113-121, Lecture Notes in Pure and Appl. Math., 159, Dekker, New York, 1994.
- [8] T. Kanzaki: On Galois algebra over a commutative ring, Osaka J. Math., 2(1965), 309-317.
- [9] Y. Miyashita: On a skew polynomial ring, J. Math. Soc. Japan 31(1979), 317-330.
- [10] K. Sugano: Note on semisimple extensions and separable extensions, Osaka J. Math., 4(1967), 265-270.

GEORGE SZETO
DEPARTMENT OF MATHEMATICS
BRADLEY UNIVERSITY
PEORIA, ILLINOIS 61625 - U.S.A.

LIANYONG XUE
DEPARTMENT OF MATHEMATICS
BRADLEY UNIVERSITY
PEORIA, ILLINOIS 61625 - U.S.A.
(Received October 27, 1998)