THE GENERAL IKEHATA THEOREM FOR $H$-SEPARABLE CROSSED PRODUCTS

GEORGE SZETO and LIANYONG XUE

(Received 26 March 1999)

ABSTRACT. Let $B$ be a ring with $1$, $C$ the center of $B$, $G$ an automorphism group of $B$ of order $n$ for some integer $n$, $C^G$ the set of elements in $C$ fixed under $G$, $\Delta = \Delta(B,G,f)$ a crossed product over $B$ where $f$ is a factor set from $G \times G$ to $U(C^G)$. It is shown that $\Delta$ is an $H$-separable extension of $B$ and $V_{\Delta}(B)$ is a commutative subring of $\Delta$ if and only if $C$ is a Galois algebra over $C^G$ with Galois group $G|_{C^G} \cong G$.

Keywords and phrases. Crossed products, Galois extensions, $H$-separable extensions.

2000 Mathematics Subject Classification. Primary 16S35; Secondary 16W20.

1. Introduction. Let $B$ be a ring with $1$, $\rho$ an automorphism of $B$ of order $n$, $B[x;\rho]$ a skew polynomial ring with a basis $\{1, x, x^2, \ldots, x^{n-1}\}$ and $x^n = v \in U(B^\rho)$ for some integer $n$, where $B^\rho$ is the set of elements in $B$ fixed under $\rho$ and $U(B^\rho)$ is the set of units of $B^\rho$.

In [4] it was shown that any skew polynomial ring $B[x;\rho]$ of prime degree $n$ is an $H$-separable extension of $B$ if and only if $C$ is a Galois algebra over $C^\rho$ with Galois group $\langle \rho|_C \rangle$ of order $n$. This theorem was extended to any degree $n$ [5, Theorem 1]. Recently, the theorem was completely generalized by the present authors in [8], that is, let $B[x;\rho]$ be a skew polynomial ring of degree $n$ for some integer $n$. Then, $B[x;\rho]$ is an $H$-separable extension of $B$ if and only if $C$ is a Galois algebra over $C^\rho$ with Galois group $\langle \rho|_C \rangle \cong \langle \rho \rangle$. The purpose of the present paper is to generalize the above Ikehata theorem to an automorphism group of $B$ (not necessarily cyclic) and $f$ is a factor set from $G \times G$ to $U(C^G)$. We show that $\Delta$ is an $H$-separable extension of $B$ and $V_{\Delta}(B)$ is a commutative subring of $\Delta$ if and only if $C$ is a Galois algebra over $C^G$ with Galois group $G|_{C^G} \cong G$.

2. Preliminaries and basic definitions. Throughout this paper, $B$ represents a ring with $1$, $C$ the center of $B$, $G$ an automorphism group of $B$ of order $n$ for some integer $n$, $B^G$ the set of elements in $B$ fixed under $G$, $\Delta = \Delta(B,G,f)$ a crossed product with a free basis $\{U_g \mid g \in G \text{ and } U_1 = 1\}$ over $B$ and the multiplications are given by $U_gb = g(b)U_g$ and $U_gU_h = f(g,h)U_{gh}$ for $b \in B$ and $g, h \in G$ where $f$ is a map from $G \times G$ to $U(C^G)$ such that $f(g,h)f(gh,k) = f(h,k)f(g,hk)$, $Z$ the center of $\Delta$, $G$ the inner automorphism group of $\Delta$ induced by $G$, that is, $\bar{g}(x) = U_gxU_g^{-1}$ for each $x \in \Delta$ and $g \in G$. We note that $f(1,1) = f(1,1) = f(1,1) = 1$ for all $g \in G$ and $G$ restricted to $B$ is $G$.

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 $S$. A ring $S$ is called a $G$-Galois extension of $S^G$ if there exist elements $\{a_i, b_i \in S, i = 1, 2, \ldots, m\}$ for some integer $m$ such that $\sum_{i=1}^{m} a_i g(b_i) = \delta_{1,g}$. The set $\{a_i, b_i\}$ is called a $G$-Galois system for $S$. $S$ is called an $H$-separable extension of $A$ if there exists an $H$-separable system $\{x_i \in V_S(A), y_i \in V_{S_{b_i}}(S) \mid i = 1, 2, \ldots, m\}$ for $S$ over $A$ for some integer $m$ such that $\sum_{i=1}^{m} x_i y_i = 1 \otimes_A 1$.

3. The Ikehata theorem. In this section, we show that $\Delta$ is an $H$-separable extension of $B$ and $V_\Delta(B)$ is a commutative subring of $\Delta$ if and only if $C$ is a Galois algebra over $C^G$ with Galois group $G|_C \cong G$. We begin with a lemma.

**Lemma 3.1.** (a) $V_\Delta(B) = \sum_{g \in G} J_g U_g$ where $J_g = \{b \in B \mid ab = bg(a) \text{ for all } a \in B\}$.
(b) $V_{\Delta_{b(g,h)}}(\Delta) = \{\sum_{g \in G} \sum_{h \in G} b_{(g,h)} U_g \otimes_B U_h \mid b_{(g,h)} \in J_{gh} \text{ and } k(b_{(k^{-1}g,h)})f(k, k^{-1}g) = b_{(g,hk^{-1})}f(hk^{-1}, k) \text{ for all } g, k \in G\}$.
(c) If $\sum_{g \in G} \sum_{h \in G} b_{(g,h)} U_g \otimes U_h \in V_{\Delta_{b(g,h)}}(\Delta)$, then $b_{(g,h)} U_{gh} \in V_\Delta(B)$.
(d) If $\sum_{g \in G} \sum_{h \in G} b_{(g,h)} U_g \otimes U_h \in V_{\Delta_{b(g,h)}}(\Delta)$, then $b_{(g,h^{-1})} = g(b_{1,1}) (f(g^{-1}, g))^{-1}$ for all $g \in G$.

**Proof.** (a) Let $b \in J_g$. Then $a(b U_g) = (ab) U_g = bg(a) U_g = (bu_g) a$ for all $a \in B$. Hence $J_g U_g \subset V_\Delta(B)$. Therefore, $\sum_{g \in G} J_g U_g \subset V_\Delta(B)$. Conversely, let $\sum_{g \in G} b_g U_g \in V_\Delta(B)$. Then $a \sum_{g \in G} b_g U_g = \sum_{g \in G} b_g a U_g = \sum_{g \in G} b_g g(a) U_g$ for all $a \in B$, and so $ab_g = b_g g(a)$ for all $a \in B$ and $g \in G$, that is, $b_g \in J_g$ for all $g \in G$. Thus $V_\Delta(B) \subset \sum_{g \in G} J_g U_g$.

(b) $\chi = \sum_{g \in G} \sum_{h \in G} b_{(g,h)} U_g \otimes U_h \in V_{\Delta_{b(g,h)}}(\Delta)$ if and only if $bx = xb$ and $U_k x = x U_k$ for all $a \in B$ and $k \in G$. But

$$bx = \sum_{g \in G} \sum_{h \in G} b_{(g,h)} U_g \otimes_B U_h,$$

$$xb = \sum_{g \in G} \sum_{h \in G} b_{(g,h)} U_g \otimes_B U_h b = \sum_{g \in G} \sum_{h \in G} b_{(g,h)} U_g \otimes_B h(b) U_h$$

$$= \sum_{g \in G} \sum_{h \in G} b_{(g,h)} U_h b \otimes_B U_h = \sum_{g \in G} \sum_{h \in G} b_{(g,h)} (gh)(b) U_g \otimes_B U_h,$$

so $bx = xb$ if and only if $bb_{(g,h)} = b_{(g,h)} ((gh)(b))$ for all $b \in B$ and $g, h \in G$, that is, $b_{(g,h)} \in J_{gh}$ by noting that $\{U_g \otimes_B U_h \mid g, h \in G\}$ is a basis for $\Delta$ over $B$. Moreover,

$$U_k x = U_k \sum_{g \in G} \sum_{h \in G} b_{(g,h)} U_g \otimes_B U_h = \sum_{g \in G} \sum_{h \in G} k(b_{(g,h)}) U_k U_g \otimes_B U_h$$

$$= \sum_{g \in G} \sum_{h \in G} k(b_{(g,h)}) f(k, g) U_{kg} \otimes_B U_h$$

$$= \sum_{g \in G} \sum_{h \in G} k(b_{(k^{-1}g,h)}) f(k, k^{-1}(kg)) U_{(kg)} \otimes_B U_h$$

$$= \sum_{g \in G} \sum_{h \in G} k(b_{(k^{-1}g,h)}) f(k, k^{-1}g) U_{gh} \otimes_B U_h$$

$$= \sum_{g \in G} \sum_{h \in G} k(b_{(k^{-1}g,h)}) f(k, k^{-1}g) U_{g} \otimes_B U_h.$$
and
\[ xU_k = \sum_{g \in G} \sum_{h \in G} b_{(g,h)}U_g \otimes_B U_h U_k = \sum_{g \in G} \sum_{h \in G} b_{(g,h)}U_g \otimes_B f(h,k)U_{hk} \]
\[ = \sum_{g \in G} \sum_{h \in G} b_{(g,h)}U_g f(h,k) \otimes_B U_{hk} = \sum_{g \in G} \sum_{h \in G} b_{(g,h)}f(h,k)U_g \otimes_B U_{hk} \]
\[ = \sum_{g \in G} \sum_{h \in G} b_{(g,h)} f(lk^{-1},k) U_g \otimes_B U_l = \sum_{g \in G} \sum_{h \in G} b_{(g,h)} f(lk^{-1},k) U_g \otimes_B U_{lh}. \]

Hence, \( U_k x = xU_k \) if and only if \( k(b_{(k^{-1},g,h)}) f(k,k^{-1}g) = b_{(g,hk^{-1})} f(hk^{-1},k) \) for all \( g,h,k \in G \).

(c) If \( \sum_{g \in G} \sum_{h \in G} b_{(g,h)}U_g \otimes_B U_h \in V_{\Delta \otimes B \Delta}(\Delta) \), then \( b_{(g,h)} \in J_{gh} \) by (b); and so \( b_{(g,h)}U_{gh} \in V_{\Delta}(B) \) by (a).

(d) If \( \sum_{g \in G} \sum_{h \in G} b_{(g,h)}U_g \otimes_B U_h \in V_{\Delta \otimes B \Delta}(\Delta) \), then \( k(b_{(k^{-1},g,h)}) f(k,k^{-1}g) = b_{(g,hk^{-1})} f(hk^{-1},k) \) for all \( g,h,k \in G \) by (b). Let \( k = g \) and \( h = 1 \). Then \( b_{(g,gh^{-1})} f(g^{-1},g) = g(b_{(1,1)} f(g,1)) = g(b_{(1,1)}) = g(1) \) for all \( g \in G \). This implies that \( b_{(g,gh^{-1})} = g(1) \) for all \( g \in G \).

\[ \Box \]

**Theorem 3.2.** \( \Delta \) is an \( H \)-separable extension of \( B \) and \( V_{\Delta}(B) \) is a commutative subring of \( \Delta \) if and only if \( C \) is a Galois algebra over \( C^G \) with Galois group \( G|_C \cong G \).

**Proof.** (\( \Rightarrow \)) Since \( \Delta \) is an \( H \)-separable extension of \( B \) and \( B \) is a direct summand of \( \Delta \) as a left \( B \)-module, \( V_{\Delta}(V_{\Delta}(B)) = B \) [7, Proposition 1.2]. But \( V_{\Delta}(B) \) is commutative, so \( V_{\Delta}(B) \subset V_{\Delta}(V_{\Delta}(B)) = B \). Thus \( V_{\Delta}(B) = C \).

Since \( \Delta \) is an \( H \)-separable extension of \( B \) again, there exists an \( H \)-separable system \( \{x_i \in V_{\Delta}(B) \mid i = 1,2,\ldots, m\} \) for some integer \( m \) such that \( \sum_{i=1}^m x_i y_i = 1 \otimes_B 1 \). Let \( y_i = \sum_{g \in G} \sum_{h \in G} b_{(g,h)}^{(i)} U_g \otimes_B U_h \). We claim that \( \{a_i \mid i = 1,2,\ldots, m\} \) is a 1-Galois system for \( C \). In fact, \( a_i = \sum_{g \in G} g(b_{(1,1)} b_{(1,1)} f(g^{-1},g))^{-1} g(b_{(1,1)} f(g^{-1},g))^{-1} U_g \otimes_B U_{g^{-1}} \).

\[ 1 \otimes_B 1 = \sum_{i=1}^m x_i y_i = \sum_{i=1}^m a_i \sum_{g \in G} g(b_{(1,1)} b_{(1,1)} f(g^{-1},g))^{-1} U_g \otimes_B U_{g^{-1}} \]
\[ = \sum_{g \in G} \sum_{i=1}^m a_i g(b_{(1,1)} f(g^{-1},g))^{-1} U_g \otimes_B U_{g^{-1}}. \]

This implies that \( \sum_{i=1}^m a_i g(b_{(1,1)} f(g^{-1},g))^{-1} = \delta_{1,1} \), so \( \sum_{i=1}^m a_i g(b_{(i,j)}) = \delta_{1,1} \), that is \( \{a_i, b_i \mid i = 1,2,\ldots, m\} \) is a 1-Galois system for \( C \). Therefore, \( C \) is a Galois algebra over \( C \) with Galois group \( G|_C \cong G \).

\[ (\Leftarrow) \] Since \( C \) is a Galois algebra over \( C^G \) with Galois group with \( G|_C \cong G \), there exists a 1-Galois system \( \{a_i, b_i \in C \mid i = 1,2,\ldots, m\} \) for some integer \( m \) such that \( \sum_{i=1}^m a_i g(b_{(1,1)} f(g^{-1},g))^{-1} = \delta_{1,1} \). Let \( x_i = a_i \) and \( y_i = \sum_{g \in G} g(b_{(1,1)} f(g^{-1},g))^{-1} U_g \otimes_B U_{g^{-1}} \). We claim that \( \{x_i \in \ldots} \]
$V_\Delta(B)$, $y_i \in V_{\Delta \otimes B}(\Delta)$ \( i = 1, 2, \ldots, m \) is an $H$-separable system for $\Delta$ over $B$. In fact, $x_i = a_i \in C \subseteq V_\Delta(B)$. Noting that $U_{g^{-1}} = f(g, g^{-1})^{-1}U_{g^{-1}}$, we have $U_{g^{-1}}b = f(g, g^{-1})^{-1}U_{g^{-1}}b = f(g, g^{-1})^{-1}g^{-1}(b)f(g, g^{-1})^{-1}U_{g^{-1}} = g^{-1}(b)U_{g^{-1}}$ for any $b \in B$. Hence

$$b g y_i = b \sum_{g \in G} g(b_i)U_g \otimes_B U_{g^{-1}} = \sum_{g \in G} g(b_i)U_g \otimes_B U_{g^{-1}} = \sum_{g \in G} g(b_i)U_g \otimes_B g^{-1}(b)U_{g^{-1}} = \sum_{g \in G} g(b_i)U_g \otimes_B g^{-1}(b)U_{g^{-1}}$$

(3.5)

for any $h \in G$,

$$U_h y_i = U_h \sum_{g \in G} g(b_i)U_g \otimes_B U_{g^{-1}} = \sum_{g \in G} (hg)(b_i)U_hU_g \otimes_B U_{g^{-1}} = \sum_{g \in G} (hg)(b_i)U_hU_g \otimes_B f(h, g)U_{g^{-1}}$$

(3.6)

Thus $y_i \in V_{\Delta \otimes B}(\Delta)$. Moreover, $\sum_{i=1}^m x_i y_i = \sum_{i=1}^m a_i \sum_{g \in G} g(b_i)U_g \otimes_B U_{g^{-1}} = \sum_{g \in G} \sum_{i=1}^m a_i g(b_i)U_g \otimes_B U_{g^{-1}} = \sum_{g \in G} \delta_{1, g} U_g \otimes_B U_{g^{-1}} = 1 \otimes 1$. This implies that $\{x_i \in V_\Delta(B), \ y_i \in V_{\Delta \otimes B}(\Delta) \mid i = 1, 2, \ldots, m \}$ is an $H$-separable system for $\Delta$ over $B$. Thus, $\Delta$ is an $H$-separable extension of $B$. Moreover, $B$ is a direct summand of $\Delta$ as a left $B$-module, so $V_\Delta(B) = B$ [7, Proposition 1.2]. But then, the center of $\Delta, Z \subset B$; and so $Z = C^G$. Clearly, $V_\Delta(B)^G = Z = C^G$ and $C \subset V_\Delta(B)$, so $V_\Delta(B)$ is a $G$-Galois algebra over $C^G$ with the same Galois system as $C$. Therefore, $V_\Delta(B) = C$ which is commutative. The proof is completed.

The Ikehata theorem is an immediate consequence of Theorem 3.2 by the fact that any Galois algebra with a cyclic Galois group is a commutative ring [1, Theorem 11].

**Corollary 3.3** (the Ikehata theorem). *Let $\rho$ be an automorphism of $B$ of order $n$ and $B[x; \rho]$ a skew polynomial ring of degree $n$ with $x^n = v \in U(B^\rho)$ for some integer $n$. Then, $B[x; \rho]$ is an $H$-separable extension of $B$ if and only if $C$ is a Galois algebra over $C^\rho$ with Galois group $\langle \rho \mid c \rangle \cong \langle \rho \rangle$.***

**Proof.** It is easy to check that if $\rho$ has order $n$, then $x^n = v \in U(C^\rho)$. Let $B[x; \rho]$ be an $H$-separable extension of $B$. Then $V_{B[x; \rho]}(B)$ is a Galois algebra over $C^\rho$ with cyclic Galois algebra group $\langle \rho \rangle$ generated by $\rho$ [6, Theorem 3.2]; and so $V_{B[x; \rho]}(B)$ is a commutative ring by [1, Theorem 11]. On the other hand, $B[x; \rho]$ is a crossed product $\Delta(B, \langle \rho \rangle, f)$ where $f : \langle \rho \rangle \times \langle \rho \rangle \rightarrow U(C^\rho)$ by $f(\rho^i, \rho^j) = 1$ if $i + j < n$, $f(\rho^i, \rho^j) = v$ if $i + j \geq n$, and $U_{\rho^i} = x^i$ for $i = 0, 1, 2, \ldots, n - 1$. Thus the corollary is immediate from Theorem 3.2.
Next we prove more characterizations of the ring $B$ as given in Theorem 3.2.

**Theorem 3.4.** Assume $\Delta$ is an $H$-separable extension of $B$. Then the following statements are equivalent:

1. $V_\Delta(B)$ is a commutative subring of $\Delta$.
2. $V_\Delta(B) = C$.
3. $V_\Delta(C) = B$.
4. $J_g = \{0\}$ for each $g \neq 1$ where $J_g = \{b \in B \mid ab = bg(a) \text{ for all } a \in B\}$.
5. $I_g = \{0\}$ for each $g \neq 1$ where $I_g = \{b \in B \mid cb = bg(c) \text{ for all } c \in C\}$.

**Proof.** We prove (1)$\Rightarrow$(2)$\Rightarrow$(3)$\Rightarrow$(4)$\Rightarrow$(5)$\Rightarrow$(1).

1)$\Rightarrow$(2). This was given in the proof of the necessity of Theorem 3.2.
2)$\Rightarrow$(3). Clearly, for each $\sum_{g \in G} b_g U_g$, we have $c(\sum_{g \in G} b_g U_g) = \sum_{g \in G} b_g \mu(g)c$ for each $c \in C$, so $cb_g = b_g \mu(g)c$, that is $b_g(c - g(c)) = 0$ for each $g \in G$ and $c \in C$. But $C$ is a commutative $G$-Galois extension of $C^G$, so the ideal of $C$ generated by $\{c - g(c) \mid c \in C\}$ is $C$ when $g \neq 1$ [2, Proposition 1.2(5)]. Hence $b_g = 0$ for each $g \neq 1$. But then $\sum_{g \in G} b_g U_g = b_1 \in B$. Thus $V_\Delta(C) \subseteq B$, and so $V_\Delta(C) = B$.
3)$\Rightarrow$(4). By hypothesis, $V_\Delta(C) = B$ so $V_\Delta(B) \subseteq V_\Delta(C) = B$. But $V_\Delta(B) = \sum_{g \in G} J_g U_g$ by Lemma 3.1(a), so $\sum_{g \in G} J_g U_g = V_\Delta(B) \subseteq B$. Thus $J_g = \{0\}$ for each $g \neq 1$.
4)$\Rightarrow$(5). By Lemma 3.1(a) again, $V_\Delta(B) = \sum_{g \in G} J_g U_g$, and by hypothesis, $J_g = \{0\}$ for each $g \neq 1$, so $V_\Delta(B) = J_1 \subseteq C$. Hence part (2) holds; and so $V_\Delta(C) = B$ by (2)$\Rightarrow$(3).

Clearly, $V_\Delta(C) = \sum_{g \in G} I_g U_g$, so $\sum_{g \in G} I_g U_g = B$. Thus $I_g = \{0\}$ for each $g \neq 1$.

5)$\Rightarrow$(1). Since $C \subseteq B$, $J_g \subseteq I_g$ for all $g \in G$. Hence $I_g = \{0\}$ implies $J_g = \{0\}$. But then $V_\Delta(B) = \sum_{g \in G} J_g U_g = J_1 = C$ which is commutative.

**Corollary 3.5.** $C$ is a Galois algebra over $C^G$ with Galois group $G|_C \cong G$ if and only if $\Delta$ is an $H$-separable extension of $B$ and anyone of the equivalent conditions in Theorem 3.4 holds.

We conclude the present paper with two examples of crossed products $\Delta$ to demonstrate our results:

1. $\Delta$ is an $H$-separable extension of $B$, but $V_\Delta(B)$ is not commutative.
2. $V_\Delta(B)$ is commutative, but $\Delta$ is not an $H$-separable extension of $B$.

Hence $C$ is not a Galois algebra over $C^G$ with $G|_C \cong G$ in either example by Theorem 3.2.

**Example 3.6.** Let $B = Q[i, j, k] = Q + Q i + Q j + Q k$ be the quaternion algebra over the rational field $Q$, $G = \{g_1 = 1, g_i, g_j, g_k \mid g_1(x) = ix^{-1}, g_j(x) = jxj^{-1}, g_k(x) = kxk^{-1} \text{ for all } x \in B\}$, and $\Delta = \Delta(B, G, 1)$. Then

1. The center of $\Delta$, $Z = Q$, the center of $B$.
2. $\Delta$ is a separable extension of $B$ and $B$ is an Azumaya $Q$-algebra, so $\Delta$ is an Azumaya $Q$-algebra. Since $\Delta$ is a free left $B$-module, $\Delta$ is an $H$-separable extension of $B$ [3, Theorem 1].
3. $V_\Delta(B) = Q + Qi U_{g_1} + Qj U_{g_1} + Qk U_{g_1}$ which is not commutative, so $C$ is not a Galois algebra over $C^G$ with Galois group $G|_C \cong G$ by Theorem 3.2.

**Example 3.7.** Let $B = Q[i, j, k] = Q + Q i + Q j + Q k$ be the quaternion algebra over the rational field $Q$, $G = \{g_1 = 1, g_i \mid g_1(x) = ix^{-1} \text{ for all } x \in B\}$, and $\Delta = \Delta(B, G, 1)$.
Then

1. The center of $B$, $C = Q = C^G$.

2. $V_\Delta(B) = Q + Q_i U_{\beta_i}$, which is commutative.

3. The center of $\Delta$, $Z = Q + Q_i U_{\beta_i} \neq C^G$. On the other hand, assume that $\Delta$ is an $H$-separable extension of $B$. Since $B$ is a direct summand of $\Delta$ as a left $B$-module, $V_\Delta(V_\Delta(B)) = B$ [7, Proposition 1.2]. This implies that the center of $\Delta$, $Z = C^G$, a contradiction. Thus $\Delta$ is not an $H$-separable extension of $B$. Therefore, $C$ is not a $G$-Galois algebra over $C^G$ with $G|_c \cong G$ by Theorem 3.2.

Acknowledgement. This paper was written under the support of a Caterpillar Fellowship at Bradley University. We would like to thank Caterpillar Inc. for the support.

References


Szeto: Department of Mathematics, Bradley University, Peoria, Illinois 61625, USA
E-mail address: szeto@bradley.bradley.edu

Xue: Department of Mathematics, Bradley University, Peoria, Illinois 61625, USA
E-mail address: lxue@bradley.bradley.edu