NOTE ON SEPARABLE CROSSED PRODUCTS

SHÛICHI IKEHATA

Throughout this paper, $B$ will mean a ring with identity element 1, $Z$ the center of $B$, $G$ a finite group of automorphisms of $B$, $B^G$ the set of all elements in $B$ fixed under $G$. A ring extension $T/S$ is called a separable extension, if the $T$-$T$-homomorphism of $T \otimes_S T$ onto $T$ defined by $a \otimes b \to ab$ splits, and $T/S$ is called an $H$-separable extension, if $T \otimes_S T$ is $T$-$T$-isomorphic to a direct summand of a finite direct sum of copies of $T$. As is well known every $H$-separable extension is a separable extension.

Let $\Delta = \Delta(B, G, f)$ be a crossed product with a free basis $\{u_\sigma | \sigma \in G$ and $u_1 = 1 \}$ over $B$ and the multiplication is given by $u_\sigma b = \sigma(b)u_\sigma$ and $u_\sigma u_\tau = f(\sigma, \tau)u_{\sigma\tau}$ for $b \in B$ and $\sigma, \tau \in G$, where $f$ is a factor set from $G \times G$ to $U(Z^G)$ such that $f(\sigma, \tau)f(\sigma_\tau, \rho) = f(\tau, \rho)f(\sigma, \tau\rho)$.

We have several theorems which assert that a separable extension with some condition is an $H$-separable extension. The following are examples of such theorems.

(1) If $f = X^2 - Xa - b$ is a separable polynomial in $B[X; \rho]$ whose discriminant $\delta(f) = a^2 + 4b$ is contained in the Jacobson radical $J(B)$ of $B$, then $f$ is an $H$-separable polynomial in $B[X; \rho]$ with $2 \in J(B)$. (Nagahara [5, Theorem 2], [6, Corollary 2.2])

(2) Let $f = X^{pe} - u$ be a separable polynomial in $B[X; \rho]$. If $p$ is a prime number, and $p$ is contained in the Jacobson radical of $B$, then $f$ is an $H$-separable polynomial in $B[X; \rho]$. ([3, Theorem 4])

As was shown in [6, Corollary 3.3], in the above statement (2), if $u$ is contained in the center $Z$ of $B$, then the factor ring $B[X; \rho]/fB[X; \rho]$ is a crossed product. The purpose of this paper is to prove the following theorem which is a generalization of the above theorems.

**Theorem 1.** Let $\Delta = \Delta(B, G, f)$ be a separable extension of $B$. Assume that $p$ is a prime number and $p$ is contained in the Jacobson radical $J(B)$ of $B$. If $G$ is a $p$-group, then $\Delta$ is an $H$-separable extension of $B$. 

---

1991 Mathematics Subject Classification. 16S35, 16W20.

Key words and phrases. Separable extensions, $H$-separable extensions, crossed products, Galois extensions.
Proof. Since $\Delta$ is a separable extension over $B$, it follows from [4, Theorem 2.11] that there exists an element $c$ in $Z$ such that
\[ \sum_{\sigma \in G} \sigma(c) = 1. \]
We shall show that $Z$ is a Galois extension over $Z^G$ with Galois group $G|Z$.

Case I. Assume that $G = \langle \rho \rangle$ is a cyclic group of order $p$. Since $c + \rho(c) + \rho^2(c) + \cdots + \rho^{p-1}(c) = 1$,
we have
\[ 1 - p\rho(c) = c - \rho(c) + \rho^2(c) - \rho(c) + \cdots + \rho^{p-1}(c) - \rho(c) \]
\[ = c - \rho(c) + \rho^2(c) - \rho(c) + \{ (\rho^3(c) - \rho^2(c)) + (\rho^2(c) - \rho(c)) \} \]
\[ + \cdots + \{ (\rho^{p-1}(c) - \rho^{p-2}(c)) + \cdots + (\rho^2(c) - \rho(c)) \}. \]
Since $p \in J(B)$, $1 - p\rho(c)$ is invertible in $B$. Since $1 - p\rho(c)$ is in $Z$, it is invertible in $Z$. Hence the ideal of $Z$ generated by $\{ \alpha - \rho(\alpha) | \alpha \in Z \}$ coincides with $Z$. By the similar way, we can show that the ideal of $Z$ generated by $\{ \alpha - \rho^k(\alpha) | \alpha \in Z \}$ equals to $Z$, for $2 \leq k \leq p - 1$. Hence, by [1, Theorem 1.3(f)], $Z$ is a Galois extension of $Z^G$ with Galois group $G|Z$.

Case II. We shall now prove the general case. Since $G$ is a $p$-group, $G|Z$ is also a $p$-group. Hence there exist normal subgroups $K_i$ of $G|Z$ such that
\[ G|Z = K_r \supsetneq K_{r-1} \supsetneq \cdots \supsetneq K_1 \supsetneq K_0 = \{1\}, \]
and
\[ K_{i+1}/K_i \text{ is a cyclic group of order } p \text{ (} 0 \leq i \leq r - 1\). \]
Then we have
\[ Z \supset Z^{K_1} \supset Z^{K_2} \supset \cdots \supset Z^{K_{r-1}} \supset Z^{K_r} = Z^{G|Z}. \]
Clearly, each $K_{i+1}/K_i$ induces automorphisms of $Z^{K_i}$ and
\[ (Z^{K_i})^{K_{i+1}/K_i} = Z^{K_{i+1}}. \]
We shall now prove that there exists $c_i$ in $Z^{K_i}$ such that
\[ \text{tr}_{K_{i+1}/K_i}(c_i) = 1 \text{ (} 0 \leq i \leq r - 1\). \]
We have coset decompositions
\[ G|Z = \bigcup_{k=1}^{p^u} \sigma_k K_{i+1} \quad [G|Z : K_{i+1}] = p^u, \]
\[ K_{i+1} = \bigcup_{j=1}^{p} \tau_j K_i \quad [K_{i+1} : K_i] = p. \]
We put here
\[ c_i = \sum_{k=1}^{p^n} \sum_{\rho \in K_i} \sigma_k \rho(c). \]

Then it is easy to see that \( c_i \in Z^{K_i} \) and \( \text{tr}_{K_{i+1}/K_i}(c_i) = \text{tr}_G(c) = 1 \). It is easy to see that \( p \) is contained in the Jacobson radical of \( Z^{K_i} \) for every \( i \) \((0 \leq i \leq r - 1)\). Then since \( K_{i+1}/K_i \) is a cyclic group of order \( p \), \( Z^{K_i} \) is a Galois extension of \( Z^{K_{i+1}} \) with Galois group \( K_{i+1}/K_i \) by Case I. Therefore we see that \( Z \) is a Galois extension of \( Z^G \) with Galois group \( G|Z \). Then the assertion of the theorem follows from [7, Theorem 3.2]

**Corollary 2.** Let \( \Delta = \Delta(B,G,f) \) be a separable extension of \( B \). Assume that \( B \) is of prime characteristic \( p \). If \( G \) is a \( p \)-group, then \( \Delta \) is an \( H \)-separable extension of \( B \).

In the proof of Theorem 1, we essentially proved the following

**Corollary 3.** Let \( S \) be a commutative ring, and let \( p \) be a prime number such that \( p \) is contained in the Jacobson radical of \( S \). Let \( G \) be a \( p \)-group of automorphisms of \( S \) and \( R = S^G \). If there exists an element \( c \) in \( S \) such that \( \text{tr}_G(c) = \sum_{\sigma \in G} \sigma(c) = 1 \), then \( S \) is a Galois extension of \( R \) with Galois group \( G \).

Finally we shall state an example which asserts that the condition “\( p \) is contained in the Jacobson radical” is essential in Theorem 1.

**Example 4.** Let \( C \) be the complex number field and \( S = C[x]/(x^p) \). Let \( \rho : S \to S \) the \( C \)-automorphism defined by \( \rho(x) = \zeta x \), where \( \zeta \) is a primitive \( p \)-the root of 1. Then \( G = \langle \rho \rangle \) is a cyclic group of order \( p \), \( S^G = C \) and \( \text{tr}_G(\frac{1}{p}) = 1 \). However, we can easily see that \( S \) is not a Galois extension of \( C \) with Galois group \( G \).

**References**


Shūichi Ikehata
Department of Mathematical Science
Faculty of Environmental Science and Technology
Okayama University
Tsushima, Okayama 700-8530, Japan

E-mail address: ikehata@ems.okayama-u.ac.jp

(Received June 13, 2000)