Supplements to the previous paper “On separable polynomials of degree 2 in skew polynomial rings”

Takasi Nagahara*

*Okayama University

SUPPLEMENTS TO THE PREVIOUS PAPER

"ON SEPARABLE POLYNOMIALS OF DEGREE 2
IN SKEW POLYNOMIAL RINGS"

Dedicated to Professor Tominosuke Otsuki on his 60th birthday

TAKASI NAGAHARA

Throughout this paper, $B$ will mean a (non-commutative) ring with identity element 1 which has an automorphism $\rho$. As in [2], by $B[X; \rho]$, we denote the ring of all polynomials $\sum \lambda_i X^i b_i (b_i \in B)$ with an indeterminate $X$ whose multiplication is defined by $bX = X\rho(b)$ for each $b \in B$. Moreover, by $B[X; \rho]_{cd}$ we denote the subset of $B[X; \rho]$ of all polynomials $f = X^2 - Xa - b$ with $fB[X; \rho] = B[X; \rho]f$ and $Xa = aX$. Further, for $f = X^2 - Xa - b \in B[X; \rho]_{cd}$, $\delta(f)$ denotes $a^2 + 4b$, which will be called the discriminant of $f$; and if the factor ring $B[X; \rho]/fB[X; \rho]$ is separable (resp. Galois) over $B$ then $f$ will be called to be separable (resp. Galois) over $B$. In [2], we proved that for $f \in B[X; \rho]_{cd}$, $f$ is Galois over $B$ if and only if $\delta(f)$ is invertible in $B$. The purpose of this note is to present some useful conditions for polynomials in $B[X; \rho]_{cd}$ to be separable (or, Galois) (Ths. 1 and 2).

As to notations and terminologies used in this note, we follow the previous one [2]. First, we shall prove the following theorem which is our main result.

**Theorem 1.** Assume that there is a Galois polynomial in $B[X; \rho]_{cd}$. Then, for a polynomial $g \in B[X; \rho]_{cd}$, $g$ is separable over $B$ if and only if $g$ is Galois over $B$.

**Proof.** If $4$ is invertible in $B$ then so is 2, and hence the assertion follows immediately from the result of [2, Th. 2.7]. We shall therefore assume that 4 is not invertible in $B$, that is $B \neq 4B$. We set $B = B/4B$ (the factor ring of $B$ modulo 4B) and $\overline{b} = b + 4B$ for all $b \in B$. Since $\rho(4B) = 4B$, the automorphism $\rho$ induces an automorphism $\overline{\rho}$ in $\overline{B}$ so that $\overline{\rho}(\overline{b}) = \overline{\rho(\overline{b})}$ for all $\overline{b} \in \overline{B}$. Moreover, as in [2, p. 69], we write $B_1 = \{ b \in B; \rho(b) = b \}$, $B(\alpha) = \{ b \in B; \alpha b = b\rho(\alpha) \}$ for all $\alpha \in B$, and $B_1(\rho^n) = B_1 \cap B(\rho^n)$, where $n$ is any integer. Then, one will easily see that $\overline{b} \in \overline{B_1}$ (resp. $\overline{b} \in \overline{B(\rho^n)}$) for all $b \in B_1$ (resp. $b \in B(\rho^n)$). We consider here the skew polynomial ring $\overline{B}[X; \overline{\rho}]$ and write $\overline{g} = X^2 - Xu - \overline{v}(\in \overline{B}[X; \overline{\rho}])$ for all $g = X^2 - Xu - v \in B[X; \rho]$. Since
$b \in B_1(\overline{\rho})$ for all $b \in B_1(\rho)$, it follows from the result of [2, p. 69] that
$\overline{g} \in \overline{B}[X; \overline{\rho}]_{(\rho)}$ for all $g \in B[X; \rho]_{(\rho)}$. Now, let $g = x^2 - Xu - v$ be a separable polynomial in $B[X; \rho]_{(\rho)}$. Then, by [2, Lemma 2.1], there exist elements $b_1, b_2, b_3$ and $b_4$ in $B$ such that

$$1 = vb_1 + b_2, \quad ub_1 + b_2 + b_3 = 0$$
$$vb_1 = ub_2 + \rho(b_4), \quad \rho(b_2) = b_3$$
$$b_1 \in B(\rho^{-2}), \quad b_2 \in B(\rho^{-1})$$

and $b_4$ is contained in the center of $B$. Hence we obtain

$$\overline{1} = \overline{v\overline{b}_1} + \overline{\rho}, \quad \overline{u\overline{b}_1} + \overline{\rho} = \overline{0}$$
$$\overline{v\overline{b}_1} = \overline{u\overline{b}_2} + \overline{\rho}(\overline{b_4}), \quad \overline{\rho}(\overline{b_2}) = \overline{b_3}$$
$$\overline{b_1} \in \overline{B}(\overline{\rho}^{-2}), \quad \overline{b_2} \in \overline{B}(\overline{\rho}^{-1})$$

and $\overline{b_4}$ is contained in the center of $\overline{B}$. Therefore, by virtue of [2, Lemma 2.1], $\overline{g}$ is separable over $B$. Now, by our assumption, there is a Galois polynomial $f = x^2 - xa - b$ in $B[X; \rho]_{(\rho)}$. Then, by [2, Th. 2.5], $\delta(f)$ is invertible in $B$, and hence, $\delta(f)$ is invertible in $\overline{B}$. Clearly $\delta(f) = \overline{a^2} + 4\overline{b} = \overline{a^2}$ and $\overline{a} = \overline{B_1(\overline{\rho})}$. Hence $\overline{B_1(\overline{\rho})}$ satisfies the condition [2, p. 74, (C$_3$)]. Since $\overline{g}$ is separable over $\overline{B}$, it follows from [2, Th. 2.7] that $\delta(g) = \overline{u^2}$ is invertible in $\overline{B}$, and so is $\overline{u}$. This implies $uB + 4B = B$. By [2, Lemma 2.2 (2, xix)], $u$ and 4 are contained in $\delta(g)B$. Hence $B = uB + 4B \subset \delta(g)B \subset B$. Since $\delta(g)B = B\delta(g), \delta(g)$ is invertible in $B$. Therefore, by [2, Th. 2.5], $g$ is Galois over $B$. Conversely, if $g \in B[X; \rho]_{(\rho)}$ is Galois over $B$ then the factor ring $B[X; \rho]/gB[X; \rho]$ is Galois over $B$, and hence by [1, Th. 1.5], this is separable over $B$, which implies that $g$ is separable over $B$, completing the proof.

As a direct consequence of Th. 1, we obtain the following

**Corollary.** Assume that there is a separable polynomial in $B[X; \rho]_{(\rho)}$ which is not Galois over $B$. Then, any polynomial in $B[X; \rho]_{(\rho)}$ is not Galois over $B$.

Next, let $B[X; \rho]_{(\overleftarrow{\rho})}$ be the set of the equivalence classes in $B[X; \rho]_{(\rho)}$ with respect the relation $\sim$ so that for $g, h \in B[X; \rho]_{(\rho)}$, $g \sim h$ if and only if $[B[X; \rho]/gB[X; \rho] \cong B[X; \rho]/hB[X; \rho]$ (B-ring isomorphic). Moreover, for any $C \in B[X; \rho]_{(\overleftarrow{\rho})}$, we write $C = \langle g \rangle$ where $g$ is an arbitrary element of $C$. If there is a Galois polynomial $f$ in $B[X; \rho]_{(\rho)}$ then $B[X; \rho]_{(\overleftarrow{\rho})}$ forms an abelian semigroup under the composition $\langle g \rangle \langle g_1 \rangle = \langle f \times \delta(f)^{-1} \times (g \times g_1) \rangle$ as in [2, Th. 2.17],
SUPPLEMENTS TO THE PREVIOUS PAPER

which has the identity element $\langle f \rangle$. Then, we have the following

**Theorem 2.** Assume that there is a Galois polynomial in $B[X; \rho]_{(\omega)}$. Then, for $g \in B[X; \rho]_{(\omega)}$, $g$ is separable over $B$ if and only if $\langle g \rangle$ is invertible in the semigroup $B[X; \rho]_{(\omega)}$.

**Proof.** Let $g$ be an element of $B[X; \rho]_{(\omega)}$. Then, by [2, Th. 2.17], $\langle g \rangle$ is invertible in $B[X; \rho]_{(\omega)}$ if and only if $g$ is Galois over $B$. Moreover, by Th. 1, $g$ is Galois over $B$ if and only if $g$ is separable over $B$. This enables us to obtain the theorem.

**Examples.** Let $R$ be a ring with identity element 1 and $S = R \oplus R$ the direct sum of rings $R$. Then, there is an automorphism $\rho$ so that $\rho(a, b) = (b, a)$ for any $(a, b)$ in $S$. Clearly $\rho^2 = 1$, and $f = X^2 - (1, 1)(\in S[X; \rho]_{(\omega)})$. Then, we have the following

(i) If $2 \cdot 1 \neq 0 (1 \in R)$ is invertible in $R$ (for example, take $R$ to be the field of rational numbers) then, by [2, Lemma 2.3], $f$ is a Galois polynomial in $S[X; \rho]_{(\omega)}$.

(ii) If $2 \cdot 1 = 0$ (for example, take $R$ to be $GF(2)$) then, $(1, 0) + \rho(1, 0) = (1, 1)$, and by [2, Lemma 2.3], $f$ is a separable polynomial in $S[X; \rho]_{(\omega)}$ which is not Galois.

**REFERENCES**


DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(Received April 30, 1977)