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 ρ. As in [2], by $B[X;\rho]$, we denote the ring of all polynomials $\sum_i X^i b_i$ ($b_i \in B$) with an indeterminate X whose multiplication is defined by $bX = X\rho(b)$ for each $b \in B$. Moreover, by $B[X;\rho]_{(2)}$, 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 $f = X^2 - Xa - b \in B[X;\rho]_{(2)}$, $\delta(f)$ 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 $f \in B[X;\rho]_{(2)}$, f is Galois over B if and only if $\delta(f)$ is inversible in B. The purpose of this note is to present some useful conditions for polynomials in $B[X;\rho]_{(2)}$ 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* $B[X;\rho]_{(2)}$. *Then, for a polynomial* $g \in B[X;\rho]_{(2)}$, g *is separable over* B *if and only if* g *is Galois over* B.

Proof. If 4 is inversible 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 inversible in B, that is $B \neq 4B$. We set $\bar{B} = B/4B$ (the factor ring of B modulo $4B$) and $\bar{b} = b + 4B$ for all $b \in B$. Since $\rho(4B) = 4B$, the automorphism ρ induces an automorphism $\bar{\rho}$ in $\bar{B}$ so that $\bar{\rho}(\bar{b}) = \overline{\rho(b)}$ for all $\bar{b} \in \bar{B}$. Moreover, as in [2, p. 69], we write $B_1 = \{b \in B;\ \rho(b) = b\}$, $B(\rho^n) = \{b \in B;\ \alpha b = b\rho^n(\alpha)$ 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 $\bar{b} \in \bar{B}_1$ (resp. $\bar{b} \in \bar{B}(\bar{\rho}^n)$) for all $b \in B_1$ (resp. $b \in B(\rho^n)$). We consider here the skew polynomial ring $\bar{B}[X;\bar{\rho}]$ and write $\bar{g} = X^2 - X\bar{u} - \bar{v}$ ($\in \bar{B}[X;\bar{\rho}]$) for all $g = X^2 - Xu - v \in B[X;\rho]$. Since

$\bar{b} \in \bar{B}_1(\bar{\rho}^n)$ for all $b \in B_1(\rho^n)$, it follows from the result of [2, p. 69] that $\bar{g} \in \bar{B}[X; \bar{\rho}]_{(2)}$ for all $g \in B[X; \rho]_{(2)}$. Now, let $g = X^2 - Xu - v$ be a separable polynomial in $B[X; \rho]_{(2)}$. Then, by [2, Lemma 2.1], there exist elements b_1, b_2, b_3 and b_4 in B such that

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

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

$$\begin{aligned} &\bar{1} = \bar{v}\bar{b}_1 + \bar{b}_4, && \bar{u}\bar{b}_1 + \bar{b}_2 + \bar{b}_3 = \bar{0} \\ &\bar{v}\bar{b}_1 = \bar{u}\bar{b}_2 + \bar{\rho}(\bar{b}_4), && \bar{\rho}(\bar{b}_2) = \bar{b}_3 \\ &\bar{b}_1 \in \bar{B}(\bar{\rho}^{-2}), && \bar{b}_2 \in \bar{B}(\bar{\rho}^{-1}) \end{aligned}$$

and $\bar{b}_4$ is contained in the center of $\bar{B}$. Therefore, by virtue of [2, Lemma 2.1], $\bar{g}$ is separable over B. Now, by our assumption, there is a Galois polynomial $f = X^2 - Xa - b$ in $B[X; \rho]_{(2)}$. Then, by [2, Th. 2.5], $\delta(f)$ is inversible in B, and hence, $\overline{\delta(f)}$ is inversible in $\bar{B}$. Clearly $\overline{\delta(f)} = \bar{a}^2 + 4\bar{b} = \bar{a}^2$ and $\bar{a} \in \bar{B}_1(\bar{\rho})$. Hence $\bar{B}_1(\bar{\rho})$ satisfies the condition [2, p. 74, (C_3')]. Since $\bar{g}$ is separable over $\bar{B}$, it follows from [2, Th. 2.7] that $\delta(\bar{g}) = \bar{u}^2$ is inversible in $\bar{B}$, and so is $\bar{u}$. 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 inversible in B. Therefore, by [2, Th. 2.5], g is Galois over B. Conversely, if $g\ (\in B[X; \rho]_{(2)})$ 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 $B[X; \rho]_{(2)}$ which is not Galois over B. Then, any polynomial in $B[X; \rho]_{(2)}$ is not Galois over B.*

Next, let $B[X; \rho]_{(2)}^{\sim}$ be the set of the equivalence classes in $B[X; \rho]_{(2)}$ with respect the relation $\sim$ so that for $g, h \in B[X; \rho]_{(2)}$, $g \sim h$ if and only if $B[X; \rho]/gB[X; \rho] \cong B[X; \rho]/hB[X; \rho]$ (B-ring isomorphic). Moreover, for any $C \in B[X; \rho]_{(2)}^{\sim}$, we write $C = \langle g \rangle$ where g is an arbitrary element of C. If there is a Galois polynomial f in $B[X; \rho]_{(2)}$ then $B[X; \rho]_{(2)}^{\sim}$ 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], which has the identity element $\langle f \rangle$. Then, we have the following

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

Proof. Let g be an element of $B[X;\rho]_{(2)}$. Then, by [2, Th. 2. 17], $\langle g \rangle$ is inversible in $B[X;\rho]_{(2)}^{\sim}$ 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 ρ so that $\rho(a, b) = (b, a)$ for any (a, b) in S. Clearly $\rho^2 = 1$, and $f = X^2 - (1, 1) (\in S[X;\rho]_{(2)})$. Then, we have the following

(i) if $2 \cdot 1 \neq 0$ $(1 \in R)$ is inversible 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 $S[X;\rho]_{(2)}$.

(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 $S[X;\rho]_{(2)}$ which is not Galois.

REFERENCES

[1] Y. MIYASHITA: Finite outer Galois theory of non-cmmmutative rings, Jour. Fac. Sci. Hokkaido Univ., Ser. I, **19** (1966), 114—134.

[2] T. NAGAHARA: On separable polynomials of degree 2 in skew polynomial rings, Math. J. Okayama Univ. **19** (1976), 65—95.

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(*Received April 30, 1977*)