On Galois polynomials with a cyclic Galois group in skew polynomial rings II

Satoshi YAMANAKA

Department of Integrated Science and Technology
National Institute of Technology, Tsuyama College

Abstract

K. Kishimoto gave the sufficient conditions for a polynomial of the form $X^m - a$ in skew polynomial rings of automorphism type to be a Galois polynomial with a cyclic Galois group. In this paper, we shall generalize Kishimoto's results for the general skew polynomial rings.

1 Introduction and Preliminaries

My talk at the conference was based on the paper [1]. The contents of this paper therefore overlaps with the publication.

Let A/B be a ring extension with common identity, $\mathrm{Aut}(A)$ a ring automorphism group of A, and G a finite subgroup of $\mathrm{Aut}(A)$. We call then A/B a *G-Galois extension* if $B = A^G$ and, there exist positive integer n and a finite set $\{u_i\,;\, v_i\}_{i=1}^n$ $(u_i,\, v_i \in A)$ of A such that $\sum_{i=1}^n u_i\varphi(v_i) = \delta_{1,\varphi}$ (the Kronecker's delta) for any $\varphi \in G$. In this case, we say that G is a *Galois group* of A/B, and $\{u_i; v_i\}_{i=1}^n$ is a *G-Galois coordinate system* of A/B. It is well known that a Galois extension of fields with a finite Galois group G is a G-Galois extension.

Throughout this paper, let B be an associative ring with identity 1, ρ an automorphism of B, and D a ρ-derivation. By $B[X;\rho,D]$ we denote the skew polynomial ring in which the multiplication is given by $\alpha X = X\rho(\alpha) + D(\alpha)$ for any $\alpha \in B$. Moreover, by $B[X;\rho,D]_{(0)}$, we denote the set of all monic polynomials f in $B[X;\rho,D]$ such that $fB[X;\rho,D] = B[X;\rho,D]f$. We say that a polynomial f in $B[X;\rho,D]_{(0)}$ is a *Galois polynomial* in $B[X;\rho,D]$ if $B[X;\rho,D]/fB[X;\rho,D]$ is a G-Galois extension of B for some finite subgroup G of $\mathrm{Aut}(B[X;\rho,D]/fB[X;\rho,D])$.

We put here $B[X;\rho] = B[X;\rho,0]$. In [4], K. Kishimoto showed the following.

Lemma 1.1. *Let $m \geq 2$ be a positive integer, $R = B[X;\rho]$, $R_{(0)} = B[X;\rho]_{(0)}$, $f = X^m - a \in R_{(0)}$ $(a \in B)$ $A = R/fR$, $x = X + fR \in A$, $C^\rho = \{b \in B \mid \rho(b) = b,\ \alpha b = b\alpha\ (\forall\alpha \in B)\}$, and assume that C^ρ contains a m-th root ω of unity. If m and a are invertible in B and $1-\omega^i$ $(1 \leq i \leq m-1)$ is a non-zero divisor in B, then $f = X^m - a$ is a Galois polynomial in R. More precisely, if we let σ be a B-ring automorphism of A defined by $\sigma(x) = x\omega$ and $G = \{1, \sigma, \sigma^2, \cdots, \sigma^{m-1}\}$, then A/B is a G-Galois extension whose G-Galois coordinate system is given by*

$$\left\{m^{-1}x^i\,;\, x^{m-i}a^{-1}\right\}_{i=0}^{m-1}. \tag{1.1}$$

The purpose of this article is to generalize Lemma 1.1 for the general skew polynomial ring $B[X;\rho,D]$. In section 2, we shall give the sufficient conditions for a polynomial $f = X^m - a \in B[X;\rho,D]_{(0)}$ $(m \geq 2,\ a \in B)$ to be a Galois polynomial in $B[X;\rho,D]$ with a cyclic Galois group, that is a generalization of Lemma 1.1.

2 Main result

Throughout this section, let $R = B[X;\rho,D]$ and $R_{(0)} = B[X;\rho,D]_{(0)}$. As in [8, pp.48], we inductively define additive endomorphisms $\Phi_{[i,j]}$ $(0 \leq j \leq i)$ of B as follows:

$$\Phi_{[i,j]} = \begin{cases} 1_B & (i=j=0) \\ D^i & (j=0,\ i \geq 1) \\ \rho^i & (i=j\geq 1) \\ \rho\Phi_{[i-1,j-1]} + D\Phi_{[i-1,j]} & (i \geq 2,\ 1 \leq j \leq i-1) \end{cases}.$$

By Lemma [8, Lemma 2.2], $f = X^m - a \in R$ $(m \geq 2,\ a \in B)$ is in $R_{(0)}$ if and only if

$$\begin{cases} D^m(\alpha) = \alpha a - a\rho^m(\alpha)\ (\forall\,\alpha \in B) \\ \Phi_{[m,j]} = 0\ (1 \leq j \leq m-1) \\ \rho(a) = a \\ D(a) = 0 \end{cases}.$$

From now on in this section, we shall use the following conventions:

- $C^{\rho,D} = \{b \in B \mid \rho(b) = b,\ D(b) = 0,\ \alpha b = b\alpha\ (\forall \alpha \in B)\}$
- $N_\rho = \{b \in B \mid \rho^i(b)b = b\rho^i(b) = 0\ (\forall\, i \geq 0)\}$

Moreover, for some non-negative integer k, we define an additive endomorphism τ_ρ^k of B by

$$\tau_\rho^k(\alpha) = \sum_{i=0}^{k} \rho^i(\alpha) \quad (\alpha \in B).$$

Now we shall state the following theorem which is a generalization of Lemma 1.1.

Theorem 2.1. *Let $m \geq 2$ be a positive integer, $f = X^m - a \in R_{(0)}$ $(m \geq 2,\ a \in B)$, $A = R/fR$, and $x = X + fR \in A$. Assume that $C^{\rho,D}$ contains a m-th root ω of unity, there exists $b \in N_\rho$ such that $\tau_\rho^{m-1}(b) = 0$, and ω and b satisfy*

$$D(\alpha)\omega + \alpha b(\omega - 1) = b(\omega-1)\rho(\alpha) + D(\alpha) \quad (\forall\,\alpha \in B).$$

If m and a are invertible in B and $1-\omega^i$ $(1 \leq i \leq m-1)$ is a non-zero divisor in B, then $f = X^m - a$ is a Galois polynomial in R. More precisely, if we let σ be a B-ring *automorphism of A defined by $\sigma(x) = x\omega + b(\omega - 1)$ and $G = \{1, \sigma, \sigma^2, \cdots, \sigma^{m-1}\}$, then A/B is a G-Galois extension whose G-Galois coordinate system is given by*

$$\left\{m^{-1}(x+b)^i \,;\, (x+b)^{m-i}a^{-1}\right\}_{i=0}^{m-1}.$$

Remark 1. In Theorem 2.1, assume that $b = 0$. Then, it is easy to see that Theorem 2.1 is equal to Lemma 1.1.

Example 2.2. We shall show an example of a Galois polynomial of degree 2 in skew polynomial rings. Let $B = \begin{bmatrix} \mathbb{R} & \mathbb{R} \\ \mathbb{R} & \mathbb{R} \end{bmatrix}$ (the 2×2 matrix ring over the real umber filed $\mathbb{R}$), $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in B$, and $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in B$. We define two maps $\rho : B \to B$, $D : B \to B$ by

$$\rho\left(\begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}\right) = \begin{bmatrix} \alpha_{11} & -\alpha_{12} \\ -\alpha_{21} & \alpha_{22} \end{bmatrix}$$

$$D\left(\begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}\right) = \begin{bmatrix} -\alpha_{21} & \alpha_{22} - \alpha_{11} \\ 0 & -\alpha_{21} \end{bmatrix} \quad (\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in \mathbb{R}).$$

It is easy to see that ρ is an automorphism of B such that $\rho^2 = 1$, and D is a ρ-derivation of B. Let $R = B[X; \rho, D]$, $R_{(0)} = B[X; \rho, D]_{(0)}$, $a = I \in B$, and $f = X^2 - a \in R$. It is obvious that $\rho(a) = a$ and $D(a) = O$. In addition, for any $\alpha \in B$, one easily see that

$$D^2(\alpha) = O = \alpha a - a\rho^2(\alpha), \quad \Phi_{[2,1]}(\alpha) = O.$$

Therefore $f = X^2 - a$ is in $R_{(0)}$ by Lemma [8, Lemma 2.2]. Let $A = R/fR$, $x = X + fR \in A$, $\omega = -I$, and $b = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. It is obvious that ω is a (primitive) square root of unity in $C^{\rho,D}$, b is in N_ρ such that $\tau_\rho^1(b) = b + \rho(b) = O$. Moreover, for any $\alpha \in B$, we can see that

$$D(\alpha)\omega + \alpha b(\omega - I) = b(\omega - I)\rho(\alpha) + D(\alpha).$$

Noting that $2I$ and $a = I$ are invertible in B and $I - \omega = 2I$ is a non-zero divisor in B, f is a Galois polynomial in R by Theorem 2.1. More precisely, if we let σ be a B-ring automorphism of A defined by $\sigma(x) = x\omega + b(\omega - I)$ and $G = \{1, \sigma\}$, then A/B is a G-Galois extension whose G-Galois coordinate system is given by

$$\left\{2^{-1}(x+b)^i \,;\, (x+b)^{2-i}a^{-1}\right\}_{i=0}^{1} = \left\{\frac{1}{2}I, \frac{1}{2}(x+b) \,;\, (x+b)^2, x+b\right\}.$$

ACKNOWLEDGEMENTS. This work was supported by the Research Institute for Mathematical Sciences,an International Joint Usage/Research Center located in Kyoto University.

References

[1] K. Ikegami and S. Yamanaka, *Note on Galois polynomials with a cyclic Galois group in skew polynomial rings*, submitted to Southeast Asian Bull. Math., submitted.

[2] S. Ikehata, *On separable polynomials and Frobenius polynomials in skew polynomial rings*, Math. J. Okayama Univ., **22** (1980), 115–129.

[3] K. Kishimoto, *On abelian extensions of rings. I*, Math. J. Okayama Univ., **14** 1970, 159–174.

[4] K. Kishimoto, *On abelian extensions of rings. II*, Math. J. Okayama Univ., **15** (1971), 57–70.

[5] Y. Miyashita, *On a skew polynomial ring*, J. Math. Soc. Japan, **31** (1979), no.2, 317–330.

[6] K. Sugano, *Note on cyclic Galois extensions*, Proc. Japan Acad., **57**, Ser. A 1981, 60–63.

[7] S. Yamanaka and S. Ikehata, *On Galois polynomials of degree p in skew polynomial rings of derivation type*, Southeast Asian Bull. Math., **37** 2013, 625–634.

[8] S. Yamanaka, *On weakly separable polynomials in skew polynomial rings*, Math.J. Okayama Univ., **64** (2022), 47–61.

Department of Integrated Science and Technology
National Institute of Technology, Tsuyama College
624-1 Numa, Tsuyama city, Okayama, 708-8509, Japan
E-mail address: yamanaka@tsuyama.kosen-ac.jp