On Galois polynomials of Artin-Schreier type in skew polynomial rings

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 $X^p - X - a$ in skew polynomial rings of Derivation type to be a Galois polynomial, where p is a prime number. In this paper, we shall generalize Kishimoto's results for the general skew polynomial rings.

1 Introduction and Preliminaries

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 call $X^p - X - a \in B[X;\rho,D]$ ($a \in B$) a polynomial of *Artin-Schreier type* for p, where p is a prime number. We put here $B[X;D] = B[X;1,D]$. In [2], K. Kishimoto showed the following.

Lemma 1.1. *Assume that B is of prime characteristic p, and let f be a polynomial of Artin-Schreier type for p in $B[X;D]_{(0)}$. Then f is a Galois polynomial in R. More precisely, if we let $A = B[X;D]/fB[X;D]$, $x = X + fB[X;D]$, and σ an automorphism of A defined by $\sigma(x) = x + 1$, then A is $a < \sigma >$-Galois extension of B.*

Remark 1.2. By [6, Lemma 1.2], it is already known that a $< \sigma >$-Galois coordinate sytem of A/B in Lemma 1.1 is given by

$$\left\{1, x, \cdots, x^i, \cdots, x^{p-1}\ ;\ 1 - x^{p-1}, (p-1)x^{p-2}, \cdots, (-1)^{i-1}\binom{p-1}{i}x^{p-1-i}, \cdots, -1\right\}.$$

The purpose of this article is to generalize Lemma 1.1 for the general skew polynomial ring $B[X;\rho,D]$. In the next section, we shall give the sufficient conditions for a polynomial of Artin-Schreier type for p to be a Galois polynomial in $B[X;\rho,D]$ with cyclic Galois group, that is a generalization of Lemma 1.1.

2 Main result

Throughout this section, assume that B is of prim caharacteristic p, and let $R = B[X;\rho,D]$, $R_{(0)} = B[X;\rho,D]_{(0)}$, f a polynomial of Artin-Schreier type for p in $R_{(0)}$ of the form $f = X^p - X - a$ $(a \in B)$, $A = R/fR$, and $x = X + fR \in A$. As in [7, pp.48], we inductively define additive endomorphisms $\Phi_{[i,j]}$ $(0 \leq j \leq i)$ of B as follows:

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

By Lemma [7, Lemma 2.2], $f = X^p - X - a$ is in $R_{(0)}$ if and only if

$$\Phi_{[p,j]}(\alpha) = \begin{cases} D(\alpha) + \alpha a - a\rho^p(\alpha) & (j = 0) \\ \rho(\alpha) - \rho^p(\alpha) & (j = 1) \\ 0 & (2 \leq j \leq p-1) \end{cases} \qquad (\forall\, \alpha \in B),\ \rho(a) = a,\ D(a) = 0. \tag{2.1}$$

We assume that there exists an element $\omega \in B$ such that

$$\alpha\omega = \omega\rho(\alpha) \quad (\forall \alpha \in B). \tag{2.2}$$

Let $\omega_{1,1} = 1$ and $\omega_{1,0} = \omega$. For $i \geq 2$ and $0 \leq j \leq i$, we inductively define

$$\omega_{i,j} = \begin{cases} 1 & (j = i) \\ \omega + \rho(\omega_{i-1,i-2}) & (j = i-1) \\ D(\omega_{i-1,j}) + \omega_{i-1,j}\omega + \rho(\omega_{i-1,j-1}) & (1 \leq j \leq i-2) \\ D(\omega_{i-1,0}) + \omega_{i-1,0}\omega & (j = 0) \end{cases}.$$

An easy induction shows that

$$(X + \omega)^i = \sum_{j=0}^{i} X^j \omega_{i,j} \quad (i \geq 1). \tag{2.3}$$

Moreover, we suppose that

$$\omega_{p,0} = \omega, \quad \omega_{p,j} = 0 \quad (1 \leq j \leq p-1). \tag{2.4}$$

First, we shall state the following lemma.

Lemma 2.1. *In the above situation, there exists a B-ring automorphism σ of A defined by $\sigma(x) = x + \omega$.*

Proof. Let σ^* be an endomorphism of R as a right B-module defined by $\sigma^*(X) = X + \omega$. It follows from (2.2) that $\alpha\sigma^*(X) = \sigma^*(X)\rho(\alpha) + D(\alpha)$. This implies that σ^* is a B-ring endomorphism of R. It is easy to see that $\sigma^{*p}(X) = X$, and hence, σ^* is a B-ring automorphism of R. In addition, since (2.3) and (2.4), we have

$$\sigma^*(f) = (X+\omega)^p - (X+\omega) - a = X^p + \omega - X - \omega - a = f.$$

This implies that $\sigma^*(fR) \subset fR$. Noting that $A = R/fR$ and $x = X + fR$, there exists a B-ring automorphism σ of A defined by $\sigma(x) = x + \omega$, which is naturally induced by σ^*. □

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

Theorem 2.2. *Assume that B is of prime characteristic p and there exist elements a, ω in B which satisfy (2.1), (2.2), and (2.4). Let $R = B[X; \rho, D]$, $R_{(0)} = B[X; \rho, D]_{(0)}$, $f = X^p - X - a \in R_{(0)}$, $A = R/fR$, and $x = X + fR \in A$.*

If ω is invertible in B and $D(\omega) = 0$, then f is a Galois polynomial in R. More precisely, A is a $< \sigma >$-Galois extension of B and $a < \sigma >$-Galois coordinate system of A/B is given by

$$\Big\{1, x, \cdots, x^i, \cdots, x^{1-p}\ ;\ 1 - x^{p-1}\omega^{1-p}, (p-1)x^{p-2}\omega^{1-p}, \cdots \\ \cdots, (-1)^{i-1}\binom{p-1}{i}x^{p-1-i}\omega^{1-p}, \cdots, -\omega^{1-p}\Big\}, \qquad (2.5)$$

where σ is a B-ring automorphism of A in Lemma 2.1.

Proof. Since ω is invertible and (2.2), we see that $\rho(\omega) = \omega$. So, we obtain $(x+\omega)^i = \sum_{j=0}^{i} x^j \binom{i}{j}\omega^{i-j}$ $(i \geq 1)$. Let σ be a B-ring automorphism of A in Lemma 2.1. First, we shall state $A^{<\sigma>} = B$. Let $z = \sum_{i=0}^{p-1} x^i c_i$ $(c_i \in B)$ be in $A^{<\sigma>}$. Then, $z = \sigma(z)$ implies that

$$\sum_{i=0}^{p-1} x^i c_i = \sum_{i=0}^{p-1}(x+\omega)^i c_i = \sum_{i=0}^{p-1}\sum_{j=0}^{i} x^j \binom{i}{j}\omega^{i-j}c_i = \sum_{j=0}^{p-1} x^j \sum_{i=j}^{p-1}\binom{i}{j}\omega^{i-j}c_i.$$

Comparing coefficients of both sides, we have

$$c_j = \sum_{i=j}^{p-1}\binom{i}{j}\omega^{i-j}c_i \quad (0 \leq j \leq p-1).$$

We obtain then $c_j = 0$ $(1 \leq j \leq p-1)$, inductively. Thus, $z = c_0 \in B$, that is, $A^{<\sigma>} \subset B$. It is obvious that $A^{<\sigma>} \supset B$.

Next, we shall show taht (2.5) is a $< \sigma >$-Galois coordinate system of A/B. Let k be a positive integer such that $1 \leq k \leq p-1$. It follow from the Fermat's little theorem that $k^{p-1} = 1$. Since $\sigma^k(x) = x + k\omega$ (that is, $k = (-x + \sigma^k(x))\omega^{-1}$), we see that

$$1 = k^{p-1} = \left\{(-x + \sigma^k(x))\omega^{-1}\right\}^{p-1} = \sum_{i=0}^{p-1} x^i \sigma^k \left((-1)^i \binom{p-1}{i} x^{p-1-i}\omega^{1-p}\right).$$

On the other hands, it is obvious that

$$0 = (-x + x)^{p-1}\omega^{1-p} = \sum_{i=0}^{p-1} x^i \left((-1)^i \binom{p-1}{i} x^{p-1-i}\omega^{1-p}\right).$$

Therefore, we have

$$1 = 1 - 0 = 1 - x^{p-1}\omega^{1-p} + \sum_{i=1}^{p-1} x^i \left((-1)^{i-1} \binom{p-1}{i} x^{p-1-i}\omega^{1-p}\right),$$

and

$$0 = 1 - 1 = \sigma^k\left(1 - x^{p-1}\omega^{1-p}\right) + \sum_{i=1}^{p-1} x^i \sigma^k \left((-1)^{i-1} \binom{p-1}{i} x^{p-1-i}\omega^{1-p}\right).$$

This means that (2.5) in Theorem 2.2 is a $< \sigma >$-GCS of A/B.

□

Remark 1. In Theorem 2.2, assume that $\omega = 1$. Then, it is easy to see that Theorem 2.2 is equal to Lemma 1.1.

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

References

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

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

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

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

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

[6] 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.

[7] 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