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

Katsunori HONGOU[1], Kanaru IKEGAMI[2], Satoshi YAMANAKA[3]

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

Abstract

K. Kishimoto gave conditions for a polynomial of the form $X^m - a$ (resp. $X^p - X - a$) in skew polynomial rings of automorphism type (resp. derivation type) to be a Galois polynomial. In this paper, we shall give conditions for quadratic polynomials of the form $X^2 - a$ and $X^2 - X - a$ in the general skew polynomial ring to be a Galois polynomial, respectively.

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 $B = A^G$ (the fix ring of G in A) and, for some positive integer n, there exists a finite set $\{u_i\,;\,v_i\}_{i=1}^n = \{u_1, u_2, \cdots, u_n\,;\,v_1, v_2, \cdots, v_n\}$ $(u_i, v_i \in A)$ 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.

Throughout this paper, let B be an associative ring with identity element 1, ρ an automorphism of B, and D a ρ-derivation (that is, D is an additive endomorphism of B such that $D(\alpha\beta) = D(\alpha)\beta + \rho(\alpha)D(\beta)$ for any $\alpha, \beta \in B$). 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 $f \in B[X;\rho,D]_{(0)}$ is a *Galois polynomial* in $B[X;\rho,D]$ if the residue ring $B[X;\rho,D]/fB[X;\rho,D]$ is a G-Galois extension of B for some finite subgroup G of $\mathrm{Aut}(B[X;\rho,D]/fB[X;\rho,D])$.

We set $B[X;\rho] = B[X;\rho,0]$, $B[X;D] = B[X;1,D]$, $B[X;\rho]_{(0)} = B[X;\rho,0]_{(0)}$, and $B[X;D]_{(0)} = B[X;1,D]_{(0)}$. In [3] and [4], K. Kishimoto studied Galois polynomials in $B[X;\rho]$ and $B[X;D]$, respectively. In particular, Kishimoto showed the following propositions concerning Galois polynomials.

Proposition 1.1. *Let $m \geq 2$ be a positive integer, $f = X^m - a$ $(a \in B)$ in $B[X;\rho]_{(0)}$, $A = B[X;\rho]/fB[X;\rho]$, $x = X + fB[X;\rho]$, and assume that B contains a m-th root ω of unity such that $\rho(\omega) = \omega$, $\alpha\omega = \omega\alpha$ $(\forall\alpha \in B)$. Then there exists a B-ring automorphism σ of A defined by $\sigma(x) = x\omega$. In addition, if m and a are invertible in B and $1 - \omega^i$ $(1 \leq i \leq m-1)$ is non-zero divisor in B, then f is a Galois polynomial in $B[X;\rho]$ with a cyclic Galois group of order m. More precisely,* *if we let $G =< \sigma >$, then A/B is a G-Galois extension whose G-Galois coordinate system is given by*

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

Proposition 1.2. *Let p be a prime number, B of characteristic p, $f = X^p - X - a$ $(a \in B)$ in $B[X;D]_{(0)}$, $A = B[X;D]/fB[X;D]$, and $x = X + fB[X;D]$. Then there exists a B-ring automorphism σ of A defined by $\sigma(x) = x+1$, and f is a Galois polynomial in $B[X;D]$ with a cyclic Galois group of order p. More precisely, if we let $G =< \sigma >$, then A/B is a G-Galois extension whose G-Galois coordinate system is given by*

$$\{x^i\,;\, z_i\}_{i=0}^{p-1}. \tag{1.2}$$

where $z_0 = 1 - x^{p-1}$ and $z_i = (-1)^{i-1}\binom{p-1}{i}x^{p-i-1}$ $(1 \leq i \leq p-1)$.

In this paper, we shall extend Proposition 1.1 (resp. Proposition 1.2) to the case of general skew polynomial rings $B[X;\rho,D]$ when $m = 2$ (resp. $p = 2$). In section 2, we shall give conditions for $f = X^2 - a$ $(a \in B)$ in $B[X;\rho,D]$ to be a Galois polynomial with a (cyclic) Galois group of order 2. In section 3, assume that B is of characteristic 2, and we shall give conditions for $f = X^2 - X - a$ $(a \in B)$ in $B[X;\rho,D]$ to be a Galois polynomial with a (cyclic) Galois group of order 2.

2 Conditions for $X^2 - a$ to be a Galois polynomial

Thoroughout this section, let $R = B[X;\rho,D]$, $R_{(0)} = B[X;\rho,D]_{(0)}$, $f = X^2 - a \in R_{(0)}$ $(a \in B)$, $A = R/fR$, and $x = X + fR \in A$. Note that, by [2, Lemma 1.3], $f = X^2 - a$ is in $R_{(0)}$ if and only if

$$\begin{cases} \rho(a) = a,\ D(a) = 0,\ \rho D + D\rho = 0, \\ D^2(\alpha) = \alpha a - a\rho^2(\alpha)\ (\forall\, \alpha \in B). \end{cases}$$

Let ω be in B such that

$$\begin{cases} \rho(\omega) = \omega,\ D(\omega) = 0,\ \alpha\omega = \omega\alpha\ (\forall\, \alpha \in B), \\ \omega \text{ is a square root of unity in } B. \end{cases} \tag{2.1}$$

Moreover, assume that there exists $b \in B$ such that

$$\begin{cases} \rho(b) = -b, \quad D(b) = -b^2\omega(\omega - 1), \\ D(\alpha)\omega + \alpha b(\omega - 1) = b(\omega - 1)\rho(\alpha) + D(\alpha) \quad (\forall\, \alpha \in B). \end{cases} \tag{2.2}$$

For any $\alpha \in B$, it follows from (2.2) that

$$\alpha\,(X\omega + b(\omega - 1)) = \alpha X\omega + \alpha b(\omega - 1)$$

$$
\begin{aligned}
&= X\rho(\alpha)\omega + D(\alpha)\omega + \alpha b(\omega - 1)\\
&= X\omega\rho(\alpha) + b(\omega - 1)\rho(\alpha) + D(\alpha)\\
&= (X\omega + b(\omega - 1))\,\rho(\alpha) + D(\alpha).
\end{aligned}
$$

Hence, by [1, Lemma 2.1], there exists an B-ring endomorphism σ^* of R defined by $\sigma^*(X) = X\omega + b(\omega - 1)$. It is easy to see that $\sigma^{*2}(X) = X$. This implies that σ^* is a B-ring automorphism of R such that $\sigma^{*2} = 1$. Moreover, since (2.1) and (2.2), we have

$$
\begin{aligned}
\sigma^*(f) &= \sigma^*(X^2 - a)\\
&= (X\omega + b(\omega - 1))\,(X\omega + b(\omega - 1)) - a\\
&= X\omega X\omega + X\omega b(\omega - 1) + b(\omega - 1)X\omega + b^2(\omega - 1)^2 - a\\
&= X^2\omega^2 + X\omega b(\omega - 1) + (X\rho(b)(\omega - 1) + D(b)(\omega - 1))\,\omega + b^2(\omega - 1)^2 - a\\
&= X^2 + X\omega(\omega - 1)\,(b + \rho(b)) + (\omega - 1)\,\big(D(b)\omega + b^2(\omega - 1)\big) - a\\
&= X^2 + X\omega(\omega - 1)(b - b) + (\omega - 1)\,\big(-b^2\omega^2(\omega - 1) + b^2(\omega - 1)\big) - a\\
&= X^2 - a\\
&= f.
\end{aligned}
$$

This implies that $\sigma^*(fR) \subset fR$, and hence there exists an automorphism of A defined by $\sigma(x) = x\omega + b(\omega - 1)$ which is naturally induced by σ^*. It is obvious that $\sigma^2 = 1$.

So we shall state the following theorem which is the first main results in this paper.

Theorem 2.1. *Assume that there exist ω and b in B such which satisfy* (2.1) *and* (2.2)*, respectively. Then there exists an automorphism σ of A defined by $\sigma(x) = x\omega + b(\omega - 1)$ such taht $\sigma^2 = 1$.*

In addition, if 2 and a are invertible in B, $1 - \omega$ is a non-zero divisor in B, and $b^2 = 0$, then A is a G-Galois extension of B (namely, $f = X^2 - a$ is a Galois polynomial in R), where $G = <\sigma>$. In fact, a G-Galois coordinate system of A/B is given by

$$
\left\{\frac{1}{2},\ \frac{1}{2}(x + b)\ ;\ (x + b)^2 a^{-1},\ (x + b)a^{-1}\right\} \tag{2.3}
$$

Proof. Assume that there exist ω and b in B which satisfy (2.1) and (2.2). We have already proved that there exists a B-ring automorphism σ of A defined by $\sigma(x) = x\omega + b(\omega - 1)$ such that $\sigma^2 = 1$. Let $G = <\sigma> = \{1, \sigma\}$.

Assume that 2 and a are invertible in B, $1 - \omega$ is a non-zero divisor in B, and $b^2 = 0$. Then we see that ω is a primitive square root of unity, and $D(b) = 0$ since (2.2).

First, we shall show $A^G = B$. It is clear that $B \subset A^G$. Let $z = xc_1 + c_0$ (c_1, $c_0 \in B$) be in A^G. Since $z = \sigma(z)$, we obtain

$$
xc_1 + c_0 = \sigma(xc_1 + c_0)
$$

$$\begin{aligned} &= (x\omega + b)c_1 + c_0 \\ &= x\omega c_1 + bc_1 + c_0. \end{aligned}$$

Comparing coefficients of both sides, we have $(1-\omega)c_1 = 0$. So, since $1-\omega$ is a non-zero divisor in B, we obtain $c_1 = 0$. Therefore we see that $z = c_0 \in B$, namely, $A^G \subset B$.

Next, we shall show that (2.3) is a G-Galois coordinate system of A/B. Since $1-\omega$ is a non-zero dibisor in B, we see that $1+\omega = 0$. Let k be a integer such taht $0 \leq k \leq 1$. It is easy to see that $\sigma^k(x+b) = x\omega^k + b\omega^k = \omega^k(x+b)$. Noting that $x^2 = a$, we obtain

$$\begin{aligned} (x+b)^2 &= (x^2 + xb + bx + b^2) \\ &= (a + xb + x\rho(b)) \\ &= (a + xb - xb) \\ &= a. \end{aligned}$$

We have then

$$\begin{aligned} \frac{1}{2}\sigma^k\left((x+b)^2a^{-1}\right) + \frac{1}{2}(x+b)\sigma^k\left((x+b)a^{-1}\right) &= \frac{1}{2}\left(\sigma^k(aa^{-1}) + (x+b)\omega^k(x+b)a^{-1}\right) \\ &= \frac{1}{2}\left(1 + \omega^k(x+b)^2a^{-1}\right) \\ &= \frac{1}{2}\left(1 + \omega^k aa^{-1}\right) \\ &= \frac{1}{2}\left(1 + \omega^k\right) \\ &= \delta_{0,k}. \end{aligned}$$

Thus, (2.3) is a G-Galois coordinate system of A/B. □

Remark 1. In Theorem 2.1, assumet that $b = 0$. So, it follows from (2.2) that $D = 0$, and hence $B[X;\rho,D] = B[X;\rho]$. Moreover, a G-Galois coordinate system (2.3) is equal to (1.1) in the case $m = 2$ in Proposition 1.1.

3 Conditions for $X^2 - X - a$ to a Galois polynomial

Thoroughout this section, let B be of characteristic 2, $R = B[X;\rho,D]$, $R_{(0)} = B[X;\rho,D]_{(0)}$, $f = X^2 - X - a \in R_{(0)}$ $(a \in B)$, $A = R/fR$, and $x = X + fR \in A$. Note that, by [2, Corollary 1.7], $f = X^2 - X - a$ is in $R_{(0)}$ if and only if

$$\begin{cases} \rho(a) = a, \ D(a) = 0, \\ \rho D(\alpha) + D\rho(\alpha) = \rho(\alpha) - \rho^2(\alpha), \quad (\forall\, \alpha \in B) \\ D^2(\alpha) - D(\alpha) = \alpha a - a\rho^2(\alpha). \end{cases}$$

Let ω be in B such that

$$\alpha\omega = \omega\rho(\alpha)\ (\forall\, \alpha \in B),\ \ \rho(\omega) = -\omega,\ \ D(\omega) = \omega - \omega^2. \tag{3.1}$$

So, for any $\alpha \in B$, we see that

$$\begin{aligned}\alpha(X+\omega) &= \alpha X + \alpha\omega \\ &= X\rho(\alpha) + D(\alpha) + \omega\rho(\alpha) \\ &= (X+\omega)\rho(\alpha) + D(\alpha).\end{aligned}$$

Hence, by [1, Lemma 2.1], there exists a B-ring endomorphism σ^* of R defined by $\sigma^*(X) = X+\omega$. It is easy to see that $\sigma^{*2}(X) = X$. This implies that σ^* is a B-ring automorphism of R such that $\sigma^{*2} = 1$. Moreover, since (3.1), we obtain

$$\begin{aligned}\sigma^*(f) &= \sigma^*(X^2 - X - a) \\ &= (X+\omega)^2 - (X+\omega) - a \\ &= X^2 + X\omega + X\rho(\omega) + D(\omega) + \omega^2 - X - \omega - a \\ &= X^2 + X\omega - X\omega + \omega - \omega^2 + \omega^2 - X - \omega - a \\ &= X^2 - X - a \\ &= f.\end{aligned}$$

This implies that $\sigma^*(fR) \subset fR$, and hence there exists a B-ring automorphism of A defined by $\sigma(x) = x+\omega$ which is naturally induced by σ^*. Obviously, $\sigma^2 = 1$.

Now we shall state the following theorem which is the second main results in this paper.

Theorem 3.1. *Assume that there exists ω in B which satisfies* (3.1). *Then there exists an automorphism σ of A defined by $\sigma(x) = x+\omega$ such that $\sigma^2 = 1$.*

In addition, if ω is invertible in B, then A is a G-Galois extension of B (namely, $f = X^2 - X - a$ is a Galois polynomial in R), where $G =<\sigma>$. In fact, a G-Galois coordinate system of A/B is given by the following :

$$\left\{1,\ x\ ;\ 1 - x\omega^{-1},\ \omega^{-1}\right\} \tag{3.2}$$

Proof. Assume that there exists ω in B which satisfies (3.1). We have already showed that there exists a B-ring automorphism σ of A defined by $\sigma(x) = x+\omega$ such that $\sigma^2 = 1$. Let $G =<\sigma>= \{1, \sigma\}$.

Assume that ω is invertible in B. First, we shall show $A^G = B$. It is obvious that $B \subset A^G$. Let $z = xc_1 + c_0$ (c_1, $c_0 \in B$) be in A^G. Since $z = \sigma(z)$, we obtain

$$\begin{aligned}xc_1 + c_0 &= \sigma(xc_1 + c_0) \\ &= (x+\omega)c_1 + c_0 \\ &= xc_1 + \omega c_1 + c_0\end{aligned}$$

Comparing coefficients of both sides, we have $\omega c_1 = 0$, and hence $c_1 = 0$ because ω is invertible in B. Therefore, we see that $z = c_0 \in B$, namely, $A^G \subset B$.

Next, we shall show that (3.2) is a G-Galois coordinate system of A/B. Let k be a integer such taht $0 \leq k \leq 1$. It is easy to see that $\sigma^k(x) = x + k\omega$. We have then

$$\begin{aligned} \sigma^k(1 - x\omega^{-1}) + x\sigma^k(\omega^{-1}) &= 1 - (x + k\omega)\omega^{-1} + x\omega^{-1} \\ &= 1 - x\omega^k + k\omega\omega^{-1} + x\omega^{-1} \\ &= 1 + k \\ &= \delta_{0,k}. \end{aligned}$$

Therefore, (3.2) is a G-Galois coordinate system of A/B. □

Remark 2. In Theorem 3.1, assumet that $\omega = 1$. So, it follows from (3.1) that $\rho = 1$, and hence $B[X;\rho,D] = B[X;D]$. Moreover, a G-Galois coordinate system (3.2) is equal to (1.2) in the case of $p = 2$ in Proposition 1.2.

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.

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

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

[8] 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.

[9] 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
[1]E-mail address: d-hk3215@tsuyama.kosen-ac.jp
[2]E-mail address: kanaru0510@icloud.com
[3]E-mail address: yamanaka@tsuyama.kosen-ac.jp