Hokkaido Mathematical Journal Vol. 42 (2013) p. 53–68

On generalizations of separable polynomials over rings

Naoki Hamaguchi and Atsushi Nakajima

(Received February 28, 2011; Revised March 6, 2012)

Abstract. We define that a ring extension S/R is weakly separable or weakly quasi-separable by using R-derivations of S, and give the necessary and sufficient condition that the extension $R[X]/(X^n - aX - b)$ of a commutative ring R is weakly separable. Since the notions of weakly separability and weakly quasi-separability coincide for commutative ring extensions, we treat a quotient ring $R[x;*] = R[X;*]/f(X)R[X;*]$ of a skew polynomial ring $R[X;*]$, and show that if R is a commutative domain, then the extension $R[x;*]/R$ is always weakly quasi-separable, where $*$ is either a ring automorphism or a derivation of R. We also treat the weakly separability of $R[x;*]/R$ and give various types of examples of these extensions.

Key words: Separable extension, separable polynomial, quasi-separable extension, derivation, discriminant, skew polynomial ring.

1. Introduction

Let S/R be a ring extension, M an S-bimodule and x, y arbitrary elements in S. An additive map $D : S \to M$ is called an R-*derivation* if $D(xy) = D(x)y + xD(y)$ and $D(r) = 0$ for any $r \in R$. D is called *central* if $D(x)y = yD(x)$, and D is called *inner* if $D(x) = mx - xm$ for some fixed element $m \in M$. The R-derivations of S to M deeply relate to a separable extension S/R.

In this paper, we generalize the notions of a separable extension and a quasi-separable extension. Since a good example of a ring extension is a quotient ring of a polynomial ring, we treat a polynomial ring and a skew polynomial ring, and characterize weakly separable polynomials and weakly quasi-separable polynomials.

In Section 2, we define the notions of a weakly separable extension and a weakly quasi-separable extension, and give an example of a weakly separable and a weakly quasi-separable extension which is not a separable extension. In Section 3, we discuss the condition of the weakly separability for the extension $R[X]/(X^n - aX - b)$ of a commutative ring R. Since the notions of a weakly separability and a weakly quasi-separability coincide for a commuta-

2000 Mathematics Subject Classification : Primary 16S79; Secondly 13B05.

tive ring extension, we treat a quotient ring $R[x;*] = R[X;*]/f(X)R[X;*]$ of a skew polynomial ring $R[X;*]$ in Section 4, and show that if R is a commutative domain, then the extension $R[x;*]/R$ is weakly quasi-separable for any polynomial $f(X)$ in $R[X;*]$. We also treat the weakly separability of $R[x;*]/R$ and give various types of examples of skew polynomials which relate to these extensions.

Throughout the following all rings have an identity, all modules are unitary and every subring contains the identity of a ring.

2. Definitions and an example

A ring extension S/R is called *separable* if the S-bimodule map

$$\mu : S \otimes_R S \ni x \otimes y \mapsto xy \in S$$

splits. If R is a commutative ring and S is an R-algebra, then it is well known that S/R is separable if and only if for any S-bimodule M, every R-derivation of S to M is inner (cf. [1, pp. 75–76]). This result is also true for a noncommutative ring extension (cf. [2, Satz 4.2]). In [11], Y. Nakai introduced the notion of a quasi-separable commutative ring extension by using the module of differentials, and in the noncommutative case, it was characterized by H. Komatsu [8, Lemma 2.1] as follows:

S/R is *quasi-separable* if and only if for any S-bimodule M, every central R-derivation of S to M is zero.

Under these circumstances, we define several types of separability as follows:

Definition 2.1 Let S/R be a ring extension.
(1) S/R is called *separable* if for any S-bimodule M, every R-derivation of S to M is inner.
(2) S/R is called *weakly separable* if every R-derivation of S to S is inner.
(3) S/R is called *quasi-separable* if for any S-bimodule M, every central R-derivation of S to M is zero.
(4) S/R is called *weakly quasi-separable* if every central R-derivation of S to S is zero.

A separable extension is weakly separable and a quasi-separable extension is weakly quasi-separable. Moreover, in [8, Theorem 2.1], Komatsu proved that a separable extension is quasi-separable.

First, we give an example of a weakly separable and a weakly quasi-separable extension which is not separable.

Example 2.2 Let A be a commutative ring with identity 1 and $M_2(A)$ the 2×2-matrix ring over A. Consider the following subsets of $M_2(A)$:

$$T_2 = \left\{ \begin{bmatrix} r & s \\ 0 & t \end{bmatrix} \mid r, s, t \in A \right\} \quad \text{and} \quad R_2 = \left\{ \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} \mid r \in A \right\}.$$

Then T_2 is a ring extension of R_2 with identity $I_2 = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$. Let $D : T_2 \to T_2$ be an R_2-derivation and $\{E_{ij}\}$ $(1 \leqq i,\ j \leqq 2)$ the matrix units. Since an element $x \in T_2$ is represented by $\{E_{11}, E_{12}, E_{22}\}$, D is determined by the image of E_{ij}. So we have

$$D(E_{11}) = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix},\ D(E_{12}) = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \text{ and } D(E_{22}) = \begin{bmatrix} 0 & -a \\ 0 & 0 \end{bmatrix}$$

for some $a, b \in A$. Therefore, for any $x = \left[\begin{smallmatrix} r & s \\ 0 & t \end{smallmatrix}\right] \in T_2$, every R_2-derivation D of T_2 is given by the following form:

$$D(x) = \begin{bmatrix} 0 & ra + sb - ta \\ 0 & 0 \end{bmatrix}.$$

And by

$$D\left(\begin{bmatrix} r & s \\ 0 & t \end{bmatrix} \right) = \begin{bmatrix} 0 & ra + sb - ta \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} b & -a \\ 0 & 0 \end{bmatrix} \begin{bmatrix} r & s \\ 0 & t \end{bmatrix} - \begin{bmatrix} r & s \\ 0 & t \end{bmatrix} \begin{bmatrix} b & -a \\ 0 & 0 \end{bmatrix},$$

D is inner. Thus T_2/R_2 is a weakly separable extension. If D is central, then for any $x = \left[\begin{smallmatrix} r & s \\ 0 & t \end{smallmatrix}\right]$ and $y = \left[\begin{smallmatrix} u & v \\ 0 & w \end{smallmatrix}\right]$ in T_2, we see $u(ra+sb-ta) = (ra+sb-ta)w$ for all $r, s, t, u, w \in A$, which shows $a = b = 0$. Therefore, the central R_2-derivation of T_2 is zero and so T_2/R_2 is a weakly quasi-separable extension.

Next we show that T_2/R_2 is not a separable extension. Define a map $\varphi : T_2 \to R_2$ as follows:

$$\varphi : T_2 \ni x = \begin{bmatrix} r & s \\ 0 & t \end{bmatrix} \mapsto \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} \in R_2.$$

Then φ is a ring epimorphism with $\varphi\left(\left[\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right]\right) = \left[\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right]$. If T_2/R_2 is separable, then by [13, Proposition 1], there exists a central idempotent $e \in T_2$ such that $\varphi(x)e = ex$ for all $x \in T_2$ and $\varphi(e) = 1$. Since a central idempotent of T_2 is of the form

$$e = \begin{bmatrix} \xi & 0 \\ 0 & \xi \end{bmatrix}, \text{ where } \xi \text{ is an idempotent of } A,$$

then by $\varphi(x)e = ex$, we have $e = 0$. This contradicts $\varphi(e) = 1$ and thus T_2/R_2 is not a separable extension.

3. Weakly separable polynomials

For a commutative ring extension S/R, the notions of the weakly separablity and the weakly quasi-separablity coincide by Definition 2.1. It is equivalent to that every R-derivation of S to S is zero.

Let R be a commutative ring, $R[X]$ a polynomial ring and $f(X)$ a monic polynomial in $R[X]$. We set $R[x] = R[X]/(f(X))$, where $x = X + (f(X))$. According to the extension $R[x]/R$ is weakly separable (resp. weakly quasi-separable), $f(X)$ is said to be *weakly separable* (resp. *weakly quasi-separable*) in $R[X]$.

Let $f(X) = X^n - aX - b$ be in $R[X]$ and $f'(X) = nX^{n-1} - a$. It is well known that $f(X)$ is separable in $R[X]$ if and only if $f'(x) = nx^{n-1} - a$ is invertible in $R[x]$, and it is equivalent to the discriminant of $f(X)$ is invertible in R. In this section, we show that the "invertibility" of a separable case substitutes the "nonzero-divisor" of a weakly separable case.

For $f(X) = X^n - aX - b$ and $f'(X) = nX^{n-1} - a$, the resultant $\mathrm{Res}(f, f')$ is the determinant of the following $(2n-1) \times (2n-1)$ matrix

$$D_{\mathrm{Res}} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & -a & -b & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & -a & -b & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & \cdots & 1 & \cdots & \cdots & 0 & -a & -b \\ n & 0 & 0 & \cdots & 0 & -a & 0 & \cdots & 0 & 0 \\ 0 & n & 0 & \cdots & 0 & 0 & -a & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & \cdots & 0 & n & 0 & \cdots & 0 & -a \end{bmatrix}$$

and the discriminant of $X^n - aX - b$ is $(-1)^{(n(n-1))/2}\,\mathrm{Res}(f,\ f')$. As is easily seen, the determinant $\det(D_{\mathrm{Res}})$ of D_{Res} is $-(n-1)^{n-1}a^n + (-1)^{n-1}n^n b^{n-1}$. Under these preparations, we prove the following

Theorem 3.1 *Let $f(X) = X^n - aX - b$ be in $R[X]$. Then $f(X)$ is weakly separable in $R[X]$ if and only if the discriminant*

$$(-1)^{(n(n-1))/2}\{-(n-1)^{n-1}a^n + (-1)^{n-1}n^n b^{n-1}\}$$

of $f(X)$ is a nonzero-divisor in R.

Proof. Let $D : R[x] \to R[x]$ be an R-derivation and we set

$$D(x) = \alpha_{n-1}x^{n-1} + \alpha_{n-2}x^{n-2} + \cdots + \alpha_1 x + \alpha_0 \quad (\alpha_i \in R). \tag{1}$$

Then by

$$\begin{aligned}
D(x^n) &= nx^{n-1}\big(\alpha_{n-1}x^{n-1} + \alpha_{n-2}x^{n-2} + \cdots + \alpha_1 x + \alpha_0\big)\\
&= n\big(\alpha_{n-1}x^n \cdot x^{n-2} + \alpha_{n-2}x^n \cdot x^{n-3} + \cdots + \alpha_1 x^n + \alpha_0 x^{n-1}\big)\\
&= n\big\{\alpha_{n-1}(ax+b)\cdot x^{n-2} + \alpha_{n-2}(ax+b)\cdot x^{n-3}\\
&\qquad\qquad + \cdots + \alpha_1(ax+b) + \alpha_0 x^{n-1}\big\}\\
&= n\big(a\alpha_{n-1}x^{n-1} + b\alpha_{n-1}x^{n-2} + \cdots + a\alpha_1 x + b\alpha_1 + \alpha_0 x^{n-1}\big)\\
&= D(ax+b)\\
&= a\big(\alpha_{n-1}x^{n-1} + \alpha_{n-2}x^{n-2} + \cdots \alpha_{n-i}x^{n-i} + \cdots + \alpha_1 x + \alpha_0\big),
\end{aligned}$$

we have

$$\begin{aligned}
&\{(n-1)a\alpha_{n-1} + n\alpha_0\}x^{n-1} + \{(n-1)a\alpha_{n-2} + nb\alpha_{n-1}\}x^{n-2}\\
&\qquad + \cdots + \{(n-1)a\alpha_1 + nb\alpha_2\}x + nb\alpha_1 - a\alpha_0 = 0.
\end{aligned}$$

Therefore we have the following linear equations for $\alpha_{n-1}, \cdots, \alpha_1, \alpha_0$:

$$\left.\begin{aligned} (n-1)a\alpha_{n-1} + n\alpha_0 &= 0 \\ nb\alpha_{n-1} + (n-1)a\alpha_{n-2} &= 0 \\ \cdots\cdots\cdots\cdots \\ nb\alpha_2 + (n-1)a\alpha_1 &= 0 \\ nb\alpha_1 - a\alpha_0 &= 0. \end{aligned}\right\} \quad (2)$$

It is easy to see that D is an R-derivation if and only if there exist $\{\alpha_i\}_{i=0}^{n-1}$ which satisfy the equation (2). Since the coefficient matrix of the linear equation (2) with indeterminate $\alpha_{n-1}, \alpha_{n-2}, \cdots, \alpha_0$ is

$$M = \begin{bmatrix} (n-1)a & 0 & 0 & 0 & \cdots & 0 & 0 & n \\ nb & (n-1)a & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & nb & (n-1)a & 0 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \cdots & nb & (n-1)a & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & nb & -a \end{bmatrix} = [m_{ij}],$$

we see

$$\det(M) = \det(D_{\mathrm{Res}}) = -(n-1)^{n-1}a^n + (-1)^{n-1}n^n b^{n-1}.$$

Then by [9, I. 30 Corollary], the equation (2) has a nontrivial solution if and only if $\det(M)$ is a zero divisor. Thus the discriminant of $X^n - aX - b$ is a nonzero-divisor if and only if $R[x]/R$ is a weakly separable extension. □

Corollary 3.2 *$f(X) = X^n - aX - b$ in $R[X]$ is weakly separable if and only if $f'(x) = nx^{n-1} - a$ is a nonzero-divisor in $R[x] = R[X]/(f(X))$.*

Proof. For $g(x) = \sum_{i=0}^{n-1} \alpha_i x^i$ in $R[x]$, we set $f'(x)g(x) = 0$. Then we have the same linear equation (2) for α_i in the proof of Theorem 3.1. Since $f'(x)$ is a nonzero-divisor if and only if the equation (2) has the trivial solution, this condition is equivalent to that $\det(M)$ is a nonzero-divisor. Therefore $f'(x)$ is a nonzero-divisor if and only if the discriminant of $f(X)$ is a nonzero-divisor. □

By Theorem 3.1, $X^2 - aX - b$ is weakly separable in $R[X]$ if and only if $a^2 + 4b$ is a nonzero-divisor in R and so there are a lot of weakly separable polynomials in $R[X]$ which is not separable. For the quadratic polynomials in $\mathbb{Z}[X]$ are classified as follows:

Example 3.3 Let $R = \mathbb{Z}$ be the ring of integers and n, $m \in \mathbb{Z}$. Then

(i) $X^2 - 2nX - m$ is not separable in $\mathbb{Z}[X]$. It is weakly separable if and only if $m \neq -n^2$.

(ii) $X^2 - (2n+1)X - m$ is always weakly separable in $\mathbb{Z}[X]$. It is separable if and only if $n^2 + n + m = 0$.

4. Weakly separability of skew polynomials

Let $* : R \to R$ be a ring automorphism or a derivation and $R[X; *]$ the skew polynomial ring. If $*$ is an automorphism ρ of R, then $rX = X\rho(r)$, and if $*$ is a derivation D of R, then $rX = Xr + D(r)$ for any $r \in R$.

By $R[X; *]_{(0)}$, we denote the set of all monic polynomials $f(X)$ in $R[X; *]$ such that $R[X; *]f(X) = f(X)R[X; *]$, and we set

$$R[x; *] = R[X; *]/f(X)R[X; *], \text{ where } x = X + f(X)R[X; *].$$

As same as the commutative case, $f(X) \in R[X; *]_{(0)}$ is called *weakly separable* (resp. *weakly quasi-separable*) in $R[X; *]$ if the corresponding extension $R[x; *]/R$ is weakly separable (resp. weakly quasi-separable).

Although the several conditions that $f(X)$ is contained in $R[X; *]_{(0)}$ were given in [3], [4], [5], [6], [7], [10] and [12], but for the sake of convenience to the reader, we show some essential part of these calculations.

4.1. Automorphism type

Let $\rho : R \to R$ be a non-trivial ring automorphism. Then we have the following

Theorem 4.1.1 *If R is a commutative domain, then every polynomial in $R[X; \rho]_{(0)}$ is weakly quasi-separable.*

Proof. For any $f(X) \in R[X; \rho]_{(0)}$, we set $R[x; \rho] = R[X; \rho]/f(X)R[X; \rho]$. Let δ be an R-derivation of $R[x; \rho]$ defined by $\delta(x) = \sum_{i=0}^{n-1} x^i b_i \in R[x; \rho]$, where n is the degree of $f(X)$. If δ is central, then by $\delta(x)r = r\delta(x) = \delta(rx) = \delta(x\rho(r)) = \delta(x)\rho(r)$, we see $\delta(x)(\rho(r) - r) = 0$ for any $r \in R$. Since R is a domain and ρ is non-trivial, we have $\delta = 0$. Thus $f(X)$ is weakly quasi-separable. □

The above theorem is true if $(\rho - 1)R = \{\rho(r) - r \mid r \in R\}$ contains a nonzero-divisor. If R has a zero divisor, then there are many non-weakly quasi-separable polynomials over R as follows.

Example 4.1.2 Let $\mathbb{Z}$ be the ring of integers and $A = \mathbb{Z}/6\mathbb{Z} = \{0, 1, \cdots, 5\}$. Let $A[Y]$ be a polynomial ring with indeterminate Y and $R = A[Y]/(Y^6) = A[y]$, where $y = Y + (Y^6)$. Using an A-ring automorphism $\rho : R \ni r = r(y) \mapsto r(5y) \in R$, we have the skew polynomial ring $R[X; \rho]$. For any $r = \sum_{i=0}^{5} \alpha_i y^i \in R$, we see

(i) $r = \rho(r) \Longleftrightarrow r = \sum_{i=0}^{2}(\alpha_{2i}y^{2i} + 3\alpha_{2i+1}y^{2i+1})$.
(ii) $\rho(r) + r = 2(\alpha_0 + \alpha_2 y^2 + \alpha_4 y^4)$.
(iii) $\rho(r) - r = 4(\alpha_1 y + \alpha_3 y^3 + \alpha_5 y^5)$.

Take $a = \sum_{i=0}^{2}(a_{2i}y^{2i} + 3a_{2i+1}y^{2i+1}) \in R$ and set $f(X) = X^2 - a$. Then $f(X) \in R[X; \rho]_{(0)}$, and so we have the quotient ring $R[x; \rho] = R[X; \rho]/f(X)R[X; \rho]$.

Let $\delta : R[x; \rho] \to R[x; \rho]$ be an R-linear map such that $\delta(x) = c$ and $\delta(1) = 0$. It is easy to see that δ is an R-derivation if and only if $\delta(x^2) = \delta(x)x + x\delta(x) = 0$ and $r\delta(x) = \delta(x)\rho(r)$ for any $r \in R$. This conditions are equivalent to the following:

$$\rho(c) + c = c(\rho(r) - r) = 0. \qquad (*)$$

If we take a nonzero element $c = 3\sum_{i=0}^{5} c_i y^i \in R$, then by (ii) and (iii), c satisfies the condition $(*)$ and thus δ is an R-derivation. Moreover, by $\rho(c) = c$ and (iii), we have $\delta(xs)(xr) - (xr)\delta(xs) = xc(\rho(s) - s)r = 0$ for any $r, s \in R$. Therefore δ is a nonzero central derivation, which shows that $X^2 - a$ is not weakly quasi-separable. And $X^2 - a$ is not weakly separable, because δ is inner if and only if there exists $r \in R$ such that $a(\rho(r) - r) = c$. This is impossible by (iii) and $c \neq 0$.

Now, by Theorem 4.1.1, our problem is to obtain some conditions for the weakly separability of $f(X) \in R[X; \rho]_{(0)}$ over a commutative domain R. First, we classify the polynomials in $R[X; \rho]_{(0)}$.

Lemma 4.1.3 (cf. [3]) *Let R be a commutative domain and $k \neq 1$ the order of ρ and $n = tk + \ell$, where $0 \leqq \ell < k$. For $f(X) = X^n - X^{n-1}a_{n-1} - \cdots - Xa_1 - a_0$ in $R[X; \rho]_{(0)}$, we have the following:*

(i) *If $n < k$, then $f(X) = X^n$.*
(ii) *If $n = k$, then $f(X) = X^n - a_0$ with $\rho(a_0) = a_0$.*

(iii) *If* $n = tk + \ell$, *then* $f(X) = X^n - X^{n-k}a_{n-k} - X^{n-2k}a_{n-2k} - \cdots - X^{n-tk}a_{n-tk}$ *with* $\rho(a_{n-jk}) = a_{n-jk}$ $(1 \leqq j \leqq t)$.

Proof. Using $Xf(X) = f(X)X$, $rf(X) = f(X)\rho^n(r)$ and R is commutative, we have

$$\rho(a_{n-i}) = a_{n-i} \quad \text{and} \quad a_{n-i}(\rho^n - \rho^{n-i})(r) = 0 \quad \text{for any } r \in R \ (1 \leqq i \leqq n).$$

Since $\rho^{jk+\ell} = \rho^\ell$ $(0 \leqq j \leqq t)$ and R is a domain, the results are easily seen. □

For the polynomials in Lemma 4.1.3, we only have the following

Theorem 4.1.4 *Let* R *be a commutative domain and* $k \neq 1$ *the order of* ρ, $R[x;\rho] = R[X;\rho]/f(X)R[X;\rho]$ *for* $f(X) \in R[X;\rho]_{(0)}$ *and* δ *an* R*-derivation of* $R[x;\rho]$.

(i) *Assume that* $n \leqq k$ *and* $f(X) = X^n$. *Then* $\delta(x) = xb$ *for some* $b \in R$. *In this case,* $f(X)$ *is weakly separable if and only if* $R = (\rho - 1)R$.

(ii) *Assume that* $n = k$ *and* $f(X) = X^n - a_0$ $(a_0 \neq 0)$. *Then* $\delta(x) = xb_1$ *such that* $\mathrm{Tr}(b_1) = 0$, *where* $\mathrm{Tr} = \rho^{n-1} + \cdots + \rho + 1$. *In this case,* $f(X)$ *is weakly separable if and only if* $R_1 = \{b_1 \in R \mid \mathrm{Tr}(b_1) = 0\} = (\rho - 1)R$.

Proof. We set $\delta(x) = \sum_{i=0}^{n-1} x^i b_i \in R[x;\rho]$. Since $r\delta(x) = \delta(x)\rho(r)$, we note that $(\rho^i(r) - \rho(r))b_i = 0$ $(0 \leqq i \leqq n-1)$ for any $r \in R$.

(i) Let $n \leqq k$ and $f(X) = X^n$. Then $\delta(x) = xb_1$ for some $b_1 \in R$ and

$$\begin{aligned}\delta(x^n) &= \sum_{i=0}^{n-1} x^i\delta(x)x^{n-i-1} = x^n(\rho^{n-1} + \cdots + \rho + 1)(b_1) \\ &= x^n\mathrm{Tr}(b_1) = 0. \qquad (**)\end{aligned}$$

If δ is inner, then $\delta(x) = xg(x) - g(x)x$ for some $g(x) \in R[x;\rho]$, which means $\delta(x) = xb_1 = x(c - \rho(c))$ for some $c \in R$. Since b_1 is arbitrary, X^n is weakly separable if and only if $R = (\rho - 1)R$.

(ii) Similarly, for $f(X) = X^n - a_0$ $(a_0 \neq 0)$, δ is also given by $\delta(x) = xb_1$. In this case, $\mathrm{Tr}(b_1) = 0$ by $(**)$. This shows (ii). □

For the case (iii) of Lemma 4.1.3, by using of $r\delta(x) = \delta(x)\rho(r)$ $(r \in R)$, we see that an R-derivation δ is of the form

$$\delta(x) = \sum_{i=0}^{t} x^{ik+1} b_{ik+1} \quad \text{where } b_{tk+1} = 0 \text{ for } n = tk, tk+1 \tag{3}$$

which satisfies the condition $\delta(x^n) = x^n \sum_{i=0}^{t} x^{ik}\,\mathrm{Tr}(b_{ik+1})$. Thus if all b_{ik+1} are contained in $(\rho - 1)(R)$, then by

$$\begin{aligned}\delta(x) = \sum_{i=0}^{t} x^{ik+1} b_{ik+1} &= \sum_{i=0}^{t} x^{ik+1}(\rho(c_{ik}) - c_{ik}) \\ &= \sum_{i=0}^{t} x^{ik} c_{ik} \cdot x - \sum_{i=0}^{t} x \cdot x^{ik} c_{ik},\end{aligned}$$

δ is inner and thus $f(X)$ is weakly separable. But it seems that the necessary conditions of weakly separability of $f(X)$ is very complicated, and we can not give this conditions.

Remark 4.1.5 In [10, Lemma 2.3], Nagahara showed that $X^2 - b \in R[X;\rho]_{(0)}$ is separable if and only if b is invertible and there exists $z \in R$ such that $z + \rho(z) = 1$. In our case, if there exists such a z, then, $X^2 - b \in R[X;\rho]_{(0)}$ $(b \neq 0)$ is weakly separable. Because, an R-derivation δ of $R[x;\rho]$ is given by $\delta(x) = xb_1$. Then we see $\delta(x^2) = 0 = b(\rho(b_1) + b_1)$ and so $\rho(b_1) = -b_1$. This shows that δ is an inner derivation by $-zb_1$.

In Theorem 4.1.4, we give some conditions such that $f(X)$ is weakly separable. So we give examples of skew polynomials which are not weakly separable.

Example 4.1.6 Let A be a commutative domain with characteristic not 2 and $R = A[Y]$ a polynomial ring. Let $\rho : R \to R$ be an A-automorphism defined by $\rho(Y) = -Y$. Then we have the skew polynomial ring $R[X;\rho]$. Assume that 2 is not invertible.

(1) Quadratic polynomials: If $n = k = 2$, Then by Lemma 4.1.3, a quadratic polynomial $f(X) \in R[X;\rho]_{(0)}$ is of the form $f(X) = X^2 - b(Y^2)$ for some $b(Y) \in R$ and by Theorem 4.1.4(ii), an R-derivation δ of $R[x;\rho]$ is given by $\delta(x) = xYb_1(Y^2)$ for some $b_1(Y) \in R$. In this case,

$$R_1 = \{r \in R \mid (\rho + 1)(r) = 0\} = \{Yg_1(Y^2) \mid g_1(Y) \in R\}$$

and

$$(\rho - 1)R = \{2Yg_2(Y^2) \mid g_2(Y) \in R\},$$

we see that R_1 is not contained in $(\rho-1)R$. Thus $X^2 - b(Y^2)$ is not weakly separable by Theorem 4.1.4 (ii). In fact, δ is inner if and only if for any $b_1(Y)$, there exists $g(Y) \in R$ such that $b_1(Y^2) = 2g(Y^2)$.

(2) Cubic polynomials: Let $n = 3$ and $k = 2$. Then by Lemma 4.1.3, the cubic polynomial $f(X) \in R[X;\rho]_{(0)}$ is of the form $f(X) = X^3 - Xa(Y^2)$ for some $a(Y) \in R$. Assume that $a(Y^2) \neq 0$. Since an R-derivation δ of $R[x;\rho]$ is given by $\delta(x) = xb_1$ for some $b_1 \in R$, and by

$$\begin{aligned}\delta(x^3) &= x^3(\rho^2 + \rho + 1)(b_1) = xa(Y^2)(1 + \rho + 1)(b_1)\\ &= \delta(x)a(Y^2) = xb_1a(Y^2),\end{aligned}$$

we have $(\rho + 1)(b_1) = 0$ and so $b_1 = Yb_2(Y^2)$ for some $b_2(Y) \in R$. In this case, δ is inner if and only if there exist $a_2, a_0 \in R$ such that

$$\begin{aligned}\delta(x) = xb_1 &= (x^2a_2 + a_0)x - x(x^2a_2 + a_0)\\ &= x\{a(Y^2)(\rho(a_2) - a_2) + \rho(a_0) - a_0\}.\end{aligned}$$

Therefore δ is inner if and only if, for any $b_2(Y^2) \in R$, there exist $h_1(Y)$, $h_2(Y) \in R$ such that $b_2(Y^2) = 2\{a(Y^2)h_1(Y^2) + h_2(Y^2)\}$. Since 2 is not invertible, $f(X)$ is not weakly separable.

In each case, if 2 is invertible, then $f(X)$ is weakly separable.

4.2. Derivation type

Let $D : R \to R$ be a non-trivial derivation and $R[X;D]$ the skew polynomial ring of derivation type. For a derivation type, we can easily prove that the same result as to the Theorem 4.1.1 for the automorphism type:

Theorem 4.2.1 *If R is a commutative domain, then every polynomial in $R[X;D]_{(0)}$ is weakly quasi-separable.*

Proof. For any $f(X) \in R[X;D]_{(0)}$, we set $R[x;D] = R[X;D]/f(X)R[X;D]$. Let δ be an R-derivation of $R[x;D]$ defined by $\delta(x) = \sum_{i=0}^{n-1} x^i b_i \in R[x;D]$, where n is the degree of $f(X)$. If δ is central, then for any r, $s \in R$, there holds

$$\begin{aligned}\delta(xr)(xs) &= \delta(x)r(xs) = \delta(x)(xr + D(r))s = \delta(x)(xs)r + \delta(x)D(r)s \\ &= (xs)\delta(xr) + \delta(x)D(r)s.\end{aligned}$$

Thus we have $\delta(x)D(r)s = 0$. Since R is a domain and D is non-trivial, we see $\delta(x) = 0$. Therefore $f(X)$ is weakly quasi-separable. $\square$

As same as the automorphism type, if $D(R) = \{D(r) \mid r \in R\}$ contains a nonzero-divisor, then the above theorem is true. If R has a zero divisor, then there are many non-weakly quasi-separable polynomials as follows.

Example 4.2.2 Let $A = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ and $R = A[Y]/(Y^4) = A[y]$, where $y = Y + (Y^4)$. Define an A-derivation D of R by $D(y) = 2$ and consider $R[X; D]$. Then $2D(r) = D^2(r) = 0$ for any $r = \sum_{i=0}^{3} \alpha_i y^i \in R$. Thus for $a = 2\sum_{i=0}^{3} a_i y^i \in R$ and $f(X) = X^2 - a$, we have the quotient ring $R[x; D] = R[X; D]/f(X)R[X; D]$.

For fixed $b_i = 2\sum_{j=0}^{3} b_{ij} y^j \in R$ $(i = 0, 1)$, we define an R-linear map δ of $R[x; D]$ by $\delta(x) = xb_1 + b_0$ and $\delta(1) = 0$. By $2b_i = D(b_i) = 0$ and $D(r)b_1 = 0$ $(r \in R)$, δ is an R-derivation. Moreover, using $D(b_i) = D(r)b_i = 0$ again, we see $(xr)\delta(xs) = \delta(xs)(xr)$ for any r, $s \in R$. Thus there exists a nonzero central derivation, which shows that $X^2 - a$ is not weakly quasi-separable.

Note that $X^2 - a$ is not weakly separable. Because, if δ is inner, then there exists $xr + s \in R[x; D]$ such that $\delta(x) = (xr + s)x - x(xr + s) = xb_1 + b_0$. This condition is equivalent to $b_1 = D(r)$ and $b_0 = D(s)$. Take $b_1 = 2\sum_{i=0}^{3} b_{1i} y^i$ such that $b_{11} \neq 0$. Then by $D(r) = 2(\alpha_1 + \alpha_3 y^2)$, b_1 is not contained in $D(R)$. Therefore there exists a non-inner R-derivation δ.

Now by Theorem 4.2.1, our problem is the weakly separability of $f(X)$. Let $f(X) = \sum_{i=0}^{n} X^i a_i$ be in $R[X; D]_{(0)}$. Then by $rX^n = \sum_{i=0}^{n} X^{n-i}\binom{n}{i}\cdot D^i(r)$, we have $0 = rf(X) - f(X)r = X^{n-1}nD(r) + \cdots$ and so $n = 0$ by our assumption. Therefore we may assume that the characteristic of R is p. In this case, we can only prove the following weakly separability:

Theorem 4.2.3 *Let R be a commutative domain of characteristic p, and $f(X)$ a polynomial in $R[X; D]_{(0)}$ of degree p. Then $f(X)$ is of the form $X^p - Xa_1 - a_0$ with $D(a_i) = 0$ $(i = 0, 1)$ and $D^p(r) = D(r)a_1$ for all $r \in R$. Moreover, an R-derivation δ of $R[x; D] = R[X; D]/f(X)R[X; D]$ is given* *by* $\delta(x) = b$ *such that* $\delta(x^p) = D^{p-1}(b) = ba_1$*. Therefore* $f(X)$ *is weakly separable if and only if* $\{b \in R \mid D^{p-1}(b) = ba_1\} = D(R)$*.*

Proof. Let $f(X) = X^p - X^{p-1}a_{p-1} - \cdots - Xa_1 - a_0$ be in $R[X;D]_{(0)}$. Then by $Xf(X) = f(X)X$, we see $D(a_i) = 0$ for any $0 \leqq i < p-1$. Since

$$\begin{aligned}
rf(X) &= rX^p - \sum_{i=1}^{p} rX^{p-i}a_{p-i} \\
&= \sum_{j=0}^{p} X^{p-j}\binom{p}{j}D^j(r) - \sum_{i=1}^{p}\sum_{j=0}^{p-i} X^{p-i-j}\binom{p-i}{j}D^j(r)a_{p-i} \\
&= \{X^p r + D^p(r)\} - \{X^{p-1}r + X^{p-2}(p-1)D(r) + \cdots\}a_{p-1} \\
&\quad - \{X^{p-2}r + X^{p-3}(p-2)D(r)) + \cdots\}a_{p-2} - \cdots,
\end{aligned}$$

then, by $rf(X) = f(X)r$, we have $a_{p-1} = 0$ and inductively $a_{p-2} = \cdots = a_2 = 0$. Thus $f(X) = X^p - Xa_1 - a_0$ and $D^p(r) = D(r)a_1$.

Now, for the above $f(X)$, let δ be an R-derivation of $R[x;D]$ defined by $\delta(x) = \sum_{i=0}^{p-1} x^i b_i \in R[x;D]$. Then by $r\delta(x) = \delta(x)r$ and $rx^i = \sum_{j=0}^{i} x^{i-j}\binom{i}{j}D^j(r)$, we easily see $\delta(x) = b_0$. Moreover by $x^p = xa_1 + a_0$, we have

$$\begin{aligned}
\delta(x^p) &= \sum_{i=0}^{p-1} x^{p-i-1}\delta(x)x^i = \sum_{i=0}^{p-1} x^{p-i-1}b_0x^i \\
&= \sum_{i=0}^{p-1} x^{p-i-1}\left\{\sum_{j=0}^{i} x^{i-j}\binom{i}{j}D^j(b_0)\right\} \\
&= px^{p-1}b_0 + x^{p-2}D(b_0)\left\{\binom{1}{1} + \binom{2}{1} + \cdots + \binom{p-1}{1}\right\} \\
&\quad + \cdots + x^{p-i-1}D^i(b_0)\left\{\binom{i}{i} + \binom{i+1}{i} + \cdots + \binom{p-1}{i}\right\} \\
&\quad + \cdots + xD^{p-2}(b_0)\left\{\binom{p-2}{p-2} + \binom{p-1}{p-2}\right\} + D^{p-1}(b_0) \\
&= D^{p-1}(b_0) = \delta(xa_1 + a_0) = b_0a_1,
\end{aligned}$$

because

$$\sum_{i=j}^{p-1}\binom{i}{j}=\binom{j}{j}+\binom{j+1}{j}+\cdots+\binom{p-1}{j}=\binom{p}{j+1}=0$$
$$(1\leqq j\leqq p-2).$$

Therefore $\delta(x)=b_0$ such that $D^{p-1}(b_0)=b_0a_1$. And δ is inner if and only if there exists $g\in R[x;D]$ such that $\delta(x)=b_0=gx-xg$ and $rg=gr$ for all $r\in R$. Then by the similar calculation to $r\delta(x)=\delta(x)r$, we see $g=c_0$ and thus $\delta(x)=b_0=D(c_0)$, completing the proof. □

Note that for the p-polynomial $f(X)=X^{p^e}-X^{p^{e-1}}a_e-\cdots-X^pa_2-Xa_1-a_0$ in $R[X;D]_{(0)}$, it was proved in [6, Lemma 1] that $f(X)$ is a separable if and only if there exists $c\in R$ such that

$$D^{p^e-1}(c)+a_eD^{p^{e-1}-1}(c)+\cdots+a_2D^{p-1}(c)+a_1c=1. \tag{6}$$

Now we give various types of weakly separable or not weakly separable polynomials of derivation type.

Example 4.2.4 Let R be a commutative ring of characteristic 2, $D:R\to R$ a nonzero derivation such that $D^2=0$ and for $f(X)\in R[X;D]_{(0)}$, δ an R-derivation of $R[x;D]=R[X;D]/f(X)R[X;D]$. In this example, we assume that $D(R)$ contains a nonzero-divisor and thus every polynomial in $R[X;D]_{(0)}$ is weakly quasi-separable by Theorem 4.2.1.

(1) Let $f(X)=X^2-Xa_1-a_0$ be in $R[X;D]_{(0)}$. Since $D(R)$ contains a nonzero-divisor, then $f(X)=X^2-a_0$ with $D(a_0)=0$. We set $\delta(x)=xb_1+b_0\in R[x;D]$. Then by $r\delta(x)=\delta(x)r$ $(r\in R)$ and $\delta(x^2)=\delta(x)x+x\delta(x)=0$, δ is an R-derivation if and only if $\delta(x)=b_0$ such that $D(b_0)=0$. And δ is inner if and only if there exists $g\in R[x;D]$ such that $\delta(x)=gx-xg$ and $rg=gr$ for any $r\in R$. This is equivalent to that there exists $c_0\in R$ such that $b_0=D(c_0)$. If $f(X)$ is weakly separable, then every R-derivation is inner and so $\operatorname{Ker}D=\operatorname{Im}D$. Since $1\in\operatorname{Ker}D$, $f(X)$ is separable by (6). Thus $f(X)$ is weakly separable if and only if $f(X)$ is separable.

(2) By $rf(X)=f(X)r$, the characteristic of R is 2 and $D(R)$ contains a nonzero-divisor, a cubic polynomial in $R[X;D]_{(0)}$ does not exist. Let $f(X)=X^4-X^3a_3-X^2a_2-Xa_1-a_0$ be in $R[X;D]_{(0)}$. We can not apply

Theorem 4.2.3, but by easy calculations, $f(X) = X^4 - X^2a_2 - a_0$ such that $D(a_i) = 0$ $(i = 0, 2)$ and δ is given by $\delta(x) = x^2b_2 + b_0 \in R[x; D]$. Since $\delta(x^4) = 0 = \delta(x^2a_2 + a_0)$, δ is an R-derivation if and only if $D(b_2)a_2 = D(b_0)a_2 = 0$. So we divide the following cases:

Case (i). $f(X) = X^4 - a_0$.

Case (ii). $f(X) = X^4 - X^2a_2 - a_0$ $(a_2 \neq 0)$ such that a_2 is a nonzero-divisor.

Case (iii). $f(X) = X^4 - X^2a_2 - a_0$ $(a_2 \neq 0)$ such that a_2 is a zero divisor.

In these cases, as same as (1), δ is inner if and only if there exist $c_i \in R$ such that $b_i = D(c_i)$ $(i = 0, 2)$.

In Case (i), since b_2 and b_0 are arbitrary, $f(X) = X^4 - a_0$ is weakly separable if and only if $D(R) = R$. This is impossible by $D^2 = 0$. Thus $f(X)$ is not weakly separable. In Case (ii), since a_2 is a nonzero-divisor, we have $D(b_2) = D(b_0) = 0$ and so $f(X) = X^4 - X^2a_2 - a_0$ is weakly separable if and only if $\operatorname{Im} D = \operatorname{Ker} D$. In this case, if a_2 is not invertible, then $f(X)$ is not separable by (6). This shows that there exists a weakly separable p-polynomial which is not separable. For a commutative domain A of characteristic 2, the polynomial ring $R = A[Y]$ and the usual A-derivation D satisfies these conditions. In Case (iii), since a_2 is a zero divisor, $f(X)$ is not separable by (6) and if $\{b \in R \mid D(b)a_2 = 0\} \subseteq \operatorname{Im} D$, then $f(X)$ is weakly separable. But this condition is not so clear.

These examples in this section show us that to determine the types of weakly separable or weakly quasi-separable polynomials in the skew polynomial ring $R[X; *]$ is not so easy. And we can not find a skew polynomial $f(X) \in R[X; *]$ such that $f(X)$ is weakly separable but not weakly quasi-separable. Does there exist such a polynomial?

Acknowledgement. The authors would like to thank the referee for his valuable suggestions.

References

[1] DeMeyer F. and Ingraham E., *Separable Algebras Over Commutative Rings*. Lecture Note in Mathematics **181** (1971), Springer-Verlag, Berlin·Heidelberg·New York.

[2] Elliger S., *Über automorphismen und derivationen von ringen*. J. Reine

Angew. Math. **277** (1975), 155–177.
[3] Ikehata S., *On separable polynomials and Frobenius polynomials in skew polynomial rings*. Math. J. Okayama Univ. **22** (1980), 115–129.
[4] Ikehata S., *Azumaya algebras and skew polynomial rings*. Math. J. Okayama Univ. **23** (1981), 19–32.
[5] Ikehata S., *On separable polynomials and Frobenius polynomials in skew polynomial rings II*. Math. J. Okayama Univ. **25** (1983), 23–28.
[6] Ikehata S., *Purely inseparable extensions and Azumaya algebras*. Math. J. Okayama Univ. **41** (1999), 63–69.
[7] Kishimoto K., *On abelian extensions of rings I*. Math. J. Okayama Univ. **14** (1970), 159–174.
[8] Komatsu H., *Quasi-separable extensions of noncommutative rings*. Comm. Algebra **29** (2001), 1011–1019.
[9] McDonald B. R., *Linear Algebras Over Commutative Rings*. Pure and Applied Mathematics **87** (1984), Marcel Dekker, New York and Basel.
[10] Nagahara T., *On separable polynomials of degree* 2 *in skew polynomial rings*. Math. J. Okayama Univ. **19** (1976), 65–95.
[11] Nakai Y., *On the theory of differentials in commutative rings*. J. Math. Soc. Japan **13** (1961), 63–84.
[12] Okamoto H. and Ikehata S., *On H-separable polynomials of degree* 2. Math. J. Okayama Univ. **32** (1990), 53–59.
[13] Sugano K., *On separable extensions over a local ring*. Hokkaido Math. J. **11** (1982), 111–115.

Naoki Hamaguchi
Department of General Education
Nagano National College of Technology
716 Tokuma, Nagano 381-8550, Japan
E-mail: hama@nagano-nct.ac.jp

Atsushi Nakajima
327-1 Nakai, Naka-Ku, Okayama
703-8205, Japan
E-mail: a2017bj.naka@hi2.enjoy.ne.jp