PORTUGALIAE MATHEMATICA
Vol. 51 Fasc. 2 – 1994

ON $\tilde{\rho}$-SEPARABILITY IN SKEW POLYNOMIAL RINGS

Xialong Lou

Presented by G. Renault

Abstract: A characterization of the $\tilde{\rho}$-separable polynomial is given and a relation between $\tilde{\rho}$-separability and separability is also obtained.

1 – Introduction

Throughout this paper, we let R be an arbitrary ring with 1, and $R[X;\rho]$ be the skew polynomial ring $\sum_{i=0} X^i R$ whose multiplication is given by $aX = X\rho(a)$, $a \in R$, where ρ is an automorphism of R. By $R[X;\rho]_{(0)}$, we denote the set of all monic polynomials g in $R[X;\rho]$ with $g\,R[X;\rho] = R[X;\rho]\,g$. A polynomial g in $R[X;\rho]_{(0)}$ is called a separable (resp. Galois) polynomial if $R[X;\rho]/gR[X;\rho]$ is a separable (resp. Galois) extension of R. Let f be a polynomial in $R[X;\rho]_{(0)}$ with ρ-invariant coefficients. Then f is called a $\tilde{\rho}$-separable polynomial if the derivative f' of f is invertible in $R[X;\rho]$ modulo $f R[X;\rho]$.

In [1] and [2], S. Ikehata studied $\tilde{\rho}$-separable polynomials in skew polynomial rings and obtained many interesting results. The purpose of this paper is to give one more equivalent condition of $\tilde{\rho}$-separability, and a relation between $\tilde{\rho}$-separability and separability.

Throughout, we use the following notations:

$C(A) =$ the center of a ring A.

$R^\rho = \Big\{a \in R \mid \rho(a) = a\Big\}$.

$f = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \,\in\, R[X;\rho]_{(0)}$.

Received: January 17, 1992.

$S = R[X;\rho]/fR[X;\rho] = \left\{\sum_{i=0}^{n-1} r_i\, x^i \mid r_i \in R,\ x = X + R[X;\rho]f\right\}$.

$\pi_i\colon\ S \to R$ is the projection map defined by $\pi_i(\sum_{i=0}^{n-1} r_i\, x^i) = r_i$.

$t\colon\ S \to R$ is the trace map defined by $t(u) = \sum_{i=0}^{n-1} \pi_i(u\, x^i)$, for $u \in S$, and it is easy to verify that t is a R-R-homomorphism.

$T_f = |t(x^i\, x^j)|_{n\times n},\quad n = \deg f$.

$\rho^*\colon\ R[X;\rho] \to R[X;\rho]$ is the ring automorphism defined by

$$\rho^*(\sum_i X^i\, d_i) = \sum_i X^i \rho(d_i), \qquad \text{for} \quad \sum_i X^i\, d_i \,\in\, R[X;\rho]\ .$$

$B_k = \left\{s \in R \mid r\, s = s\, \rho^{-k}(r), \text{ for } r \in R\right\}$, for each integer k.

2 – Basic definition

Let $\mathbb{P}$ be a ring with 1 and $\mathbb{Q}$ a subring of $\mathbb{P}$ containing 1. Then $\mathbb{P}$ is called a separable extension of $\mathbb{Q}$ if there exist a_i, b_i in $\mathbb{P}$, $i = 1,\ldots,n$ for an integer n, such that $\sum a_i\, b_i = 1$ and $\sum_i t(a_i \otimes_R b_i) = \sum_i (a_i \otimes b_i)\, t$ for each t in $\mathbb{P}$, and the set $\{a_i; b_i\}_{i=1}^n$ is called a separable set; $\mathbb{P}$ is called a Galois extension over $\mathbb{Q}$ with Galois group $G = \{g_1,\ldots,g_m\}$ (a finite automorphism group of $\mathbb{P}$) for some integer m, $g_1 = 1$ in G, if there exist c_i, d_i in $\mathbb{P}$, $i = 1,\ldots,k$ for some integer k such that $\sum_i c_i\, g_j(d_i) = \delta_{1j}$ (Kronecker delta) and $\mathbb{Q} = \mathbb{P}^G$ $(= \{t \text{ in } \mathbb{P} \mid g_i(t) = t$ for each g_i in $G\})$, and the set $\{c_i; d_i\}_{i=1}^k$ is called a Galois set.

Remark. By Prop. 1.3 in [5], Galois sets are separable sets.

3 – An equivalent condition of $\tilde{\rho}$-separable

An $n \times n$ matrix $B = |b_{ij}|$ is called a ρ-matrix over R, if for every b_{ij} $(i,j = 1,\ldots,n)$, there exists some integer l such that $b_{ij} \in B_l$.

Now we begin with the following lemma

Lemma 1. *Let $B = |b_{ij}|$ be an $n\times n$-matrix over R. If B satisfies*

1) *$\rho(b_{ij}) = b_{ij}$, $b_{ij} = b_{ji}$, $i,j = 1,2,\ldots,n$, namely $\rho(B) = B$, B^t (the transpose of B) $=B$;*

2) *B is a ρ-matrix;*

3) *B has a left (or right) inverse matrix $A = |a_{ij}|$ which is a ρ-matrix;*

then B is a matrix over $C(R^\rho)$, and $\det(B)$ is invertible in R.

Proof: Since A is a ρ-matrix, then for every a_{ij} $(i,j=1,\dots,n)$ there exists some integer l such that $a_{ij} \in B_l$. So by $b_{st}\,a_{ij} = a_{ij}\,\rho^{-1}(b_{st}) = a_{ij}\,b_{st}$, and $AB = E$ (E is the unitary matrix) iff $\sum_{i=1}^n a_{ki}\,b_{il} = \delta_{kl}$ $(k,l=1,2,\dots,n)$ iff $\sum_{i=1}^n b_{il}\,a_{ki} = \delta_{kl}$ $(k,l=1,2,\dots,n)$ iff $B^t A^t = E$ iff $BA^t = E$, we obtain that $A = A^t$ is the inverse matrix of B. Since $\rho(BA) = B\,\rho(A) = E$, so $\rho(A) = A$. Now we know that B and A are ρ-matrix such that $\rho(A) = A$ and $\rho(B) = B$. These conditions imply that A and B are matrices over $C(R^\rho)$. Finally, by $BA = E$, we have that $\det(B)$ is invertible in R. ∎

Given $f \in R[X;\rho]_{(0)} \cap R^\rho[X]$, by [2], T_f is a matrix over $C(R^\rho)$. Moreover, in [1], S. Ikehata proved the following result.

Lemma 2. *Let $f \in R[X;\rho]_{(0)} \cap R^\rho[X]$, then f is $\tilde{\rho}$-separable iff $\det(T_f) = \delta(f)$ is invertible in R.*

Then we prove the following theorem which gives another equivalent condition of $\tilde{\rho}$-separability.

Theorem 3. *Let $f \in R^\rho[X] \cap R[X;\rho]_{(0)}$, then the following are equivalent:*

1) *f is $\tilde{\rho}$-separable;*

2) $\det(T_f) = \delta(f)$ *is invertible in R;*

3) *T_f has a left inverse matrix which is a ρ-matrix.*

Proof: **1) $\Leftrightarrow$ 2).** This is the result of Lemma 2.

3) $\Rightarrow$ 2). By Lemma 1, it suffices to prove that T_f is a ρ-matrix. For $a \in R$, since

$$\begin{aligned} a\,t_{i+1,j+1} &= a\,t(x^{i+j}) = t(a\,x^{i+j}) = t(x^{i+j}\,\rho^{i+j}(a)) \\ &= t(x^{i+j})\,\rho^{i+j}(a) = t_{i+1,j+1}\,\rho^{i+j}(a)\ . \end{aligned}$$

So $t_{i+1,j+1} \in B_{-i-j}$. Thus T_f is a ρ-matrix.

2) $\Rightarrow$ 3). Let $T_f^* = |A_{i+1,j+1}|$, where $A_{i+1,j+1}$ is the algebraic complement of $t_{j+1,i+1}$ $(i,j=0,1,\dots,n-1)$. Then $T_f^*\,T_f = \delta(f)\,E$. So it suffices to prove that $\delta^{-1}(f)\,T_f^*$ is a ρ-matrix. For $a \in R$,

$$\begin{aligned} &a\,t_{1,j_1}\,t_{2,j_2}\cdots t_{j,j_j}\,t_{j+2,j_{j+2}}\cdots t_{n,j_n} = \\ &\qquad = t_{1,j_1}\,t_{2,j_2}\cdots t_{j,j_j}\,t_{j+2,j_{j+2}}\cdots t_{n,j_n}\,\rho^{n(n-1)-i-j}(a)\ , \end{aligned}$$

where $j_1, j_2, \dots, j_j, j_{j+2}, \dots, j_n$ is a permutation of $1, 2, \dots, i,\ i+2, \dots, n$. So

$$\begin{aligned} a\, A_{i+1,j+1}\, \delta^{-1}(f) &= A_{i+1,j+1}\, \rho^{n(n-1)-i-j}(a)\, \delta^{-1}(f) \\ &= A_{i+1,j+1}\, \delta^{-1}(f)\, \rho^{-i-j}(a)\ . \end{aligned}$$

So $A_{i+1,j+1}\, \delta^{-1}(f) \in B_{i+j}$. Thus $T_f^{-1} = T_f^*\, \delta^{-1}(f)$ is a ρ-matrix. ∎

4 – A relation between separability and $\tilde{\rho}$-separability

By Theorem 2.1 in [1], when f is $\tilde{\rho}$-separable, then f is separable. On the contrary, the conclusion is not right. One of such example was given in [1], and one more example will be given in the final part of this paper. The following theorem at some extent shows the "distance" between the two kinds of separability.

Theorem 4. *Let $f \in R^\rho[X] \cap R[X;\rho]_{(0)}$, then the following are equivalent:*

1) *f is $\tilde{\rho}$-separable;*

2) *f is separable with a separable set $\{x_i, y_i\}$ such that $\sum_i x_i\, t(y_i) = 1$.*

Proof: 2)⇒1). Suppose $\{x_i; y_i\}$ to be a separable set such that $\sum_i x_i\, t(y_i) = 1$, where $x_i = \sum_{k=0}^{n-1} x^k\, p_{ik}$, $y_i = \sum_{k=0}^{n-1} q_{ik}\, x^k$. Then

$$\begin{aligned} \sum_i x_i \otimes y_i &= \sum_i \Big(\sum_{k=0}^{n-1} x^k\, p_{ik}\Big) \otimes \Big(\sum_{s=0}^{n-1} q_{is}\, x^s\Big) \\ &= \sum_{k=0}^{n-1} x^k \otimes \Big(\sum_i \sum_{s=0}^{n-1} p_{ik}\, q_{is}\, x^s\Big)\ . \end{aligned}$$

Setting $d_{ks} = \sum_i p_{ik}\, q_{is}$, $z_k = \sum_{s=0}^{n-1} d_{ks}\, x^s$. Then $\sum_i x_i \otimes y_i = \sum_{k=0}^{n-1} x^k \otimes z_k$. It is easy to verify that $\{x^k; z_k\}$ is still a separable set such that $\sum_k x^k\, t(z_k) = 1$. Now we prove that $u = \sum_{k=0}^{n-1} x^k\, t(z_k\, u)$, for $u \in S$. Since t is a R-R-homomorphism, so we can define the map $1 \otimes t$ from $S \otimes_R S$ to S by $(1 \otimes t)(s_1 \otimes s_2) = s_1\, t(s_2)$. From $(1 \otimes t)(u \sum_{k=0}^{n-1} x^k \otimes z_k) = (1 \otimes t)\, (\sum_{k=0}^{n-1} x^k \otimes z_k\, u)$, we obtain that

$$u = u \sum_{k=0}^{n-1} x^k\, t(z_k) = \sum_{k=0}^{n-1} x^k\, t(z_k\, u)\ .$$

In particular,

$$\begin{aligned} x^j &= \sum_{k=0}^{n-1} x^k\, t(z_k x^j) = \sum_{k=0}^{n-1} x^k\, t\Big(\sum_{s=0}^{n-1} d_{ks}\, x^{s+j}\Big) \\ &= \sum_{k=0}^{n-1} \sum_{s=0}^{n-1} x^k\, d_{ks}\, t(x^{s+j})\,, \qquad j = 0, 1, \dots, n-1\ . \end{aligned}$$

So, $\sum_{s=0}^{n-1} d_{ks}\, t(x^{s+j}) = \delta_{kj}$, $k,j = 0,1,\ldots,n-1$. By setting $A = |d_{k+1,s+1}|$, we have $AT_f = E$, where $T_f = [t_{s+1,j+1}]$. Since $\{x^k; z_k\}$ is a separable set, then for $a \in R$,

$$\sum_{k=0}^{n-1} x^k \otimes z_k\, a = a \sum_{k=0}^{n-1} x^k \otimes z_k = \sum_{k=0}^{n-1} x^k \rho^k(a) \otimes z_k = \sum_{k=0}^{n-1} x^k \otimes \rho^k(a)\, z_k \ .$$

So $\rho^k(a)\, d_{ks} = d_{ks}\, \rho^{-s}(a)$, for $a \in R$. Thus $d_{ks} \in B_{k+s}$, and so A is a ρ-matrix. Hence by theorem 3, f is $\tilde\rho$-separable.

1) $\Rightarrow$ 2). In the proof of 2) $\Rightarrow$ 3) of Theorem 3 , we know that T_f has an inverse matrix which is a ρ-matrix. Setting $T_f^{-1} = |d_{i+j,j+1}|$, and $y_{i+1} \sum_{k=0}^{n-1} d_{i+1,k+1}\, x^k$, $i = 0,1,\ldots,n-1$. By the proof of Lemma 4.1, Lemma 4.2 and Theorem 4.3 in [7], we know that $\{y_{i+1}; x^i\}$ is a separable set. Since $T_f^{-1}\, T_f = E$,

$$\sum_{i=0}^{n-1} d_{i+1,k+1}\, t(x^i) = \delta_{k0}\,, \qquad k = 0,1,\ldots,n-1\ ,$$

and so

$$\sum_{i=0}^{n-1} y_{i+1}\, t(x^i) = \sum_{i=0}^{n-1}\sum_{k=0}^{n-1} d_{i+1,k+1}\, x^k\, t(x^i) = \sum_{k=0}^{n-1}\sum_{i=0}^{n-1} x^k\, d_{i+1,k+1}\, t(x^k) = 1\ .$$

Thus $\{y_{i+1}; x^i\}$ is a separable set such that $\sum_{i=0}^{n-1} y_{i+1}\, t(x^i) = 1$. ∎

By the above proof, we can easily verify the following result.

Theorem 5. *Let $f \in R[X;\rho]_{(0)}$ be separable, and there exists a separable set $\{x_i; y_i\}$ such that $\sum_i x_i\, t(y_i) = 1$, then T_f has a left inverse matrix which is a ρ-matrix.*

Remark. When R is a commutative ring, then under the hypothesis of theorem 5 we know that $\det(T_f)$ is invertible in R.

5 – Application and example

Let f be a Galois polynomial with Galois group G, and $t_G = \sum_{g\in G} g$ be the trace map from S to R. Let $\{x_i; y_i\}$ be a Galois set, then $\sum_i x_i\, t_G(y_i) = 1$. Now we prove a lemma.

Lemma 6. *Let f be a Galois polynomial with Galois group G, and $t_G\rho^* = \rho^*\, t_G$. Then $t = t_G$.*

Proof: Since S/R is a Galois extension, there exists a Galois set $\{x_i; z_i\}$, where $x_i = \sum_{k=0}^{n-1} x^k\, p_{ik}$, $z_i = \sum_{k=0}^{n-1} q_{ik}\, x^k$. Then

$$\sum_i x_i \otimes z_i = \sum_i \Big(\sum_{k=0}^{n-1} x^k\, p_{ik}\Big) \otimes \Big(\sum_{k=0}^{n-1} q_{is}\, x^s\Big) = \sum_{k=0}^{n-1} x^k \otimes \Big(\sum_i \sum_{s=0}^{n-1} p_{ik}\, q_{is}\, x^s\Big) .$$

By setting $d_{ks} = \sum_i p_{ik}\, q_{is}$ and $y_k = \sum_{s=0}^{n-1} d_{ks}\, x^s$, $k = 0, 1, \ldots, n-1$, $\sum_i x_i \otimes z_i = \sum_{k=0}^{n-1} x^k \otimes y_k$. It is easy to verify that $\{x^k; y_k\}$ is still a Galois set. Since t and t_G are R-R-homomorphisms, it suffices to prove that $t(x^l) = t_G(x^l)$ $(0 \le 1 \le n-1)$. Since t_G is a R-R-homomorphism, so we can define the map $1 \otimes t_G$ from $S \otimes_R S$ to S by $(1 \otimes t_G)(s_1 \otimes s_2) = s_1\, t_G(s_2)$. Then

$$\begin{aligned}
x^i &= x^i \sum_{k=0}^{n-1} x^k\, t_G(z_k) = (1 \otimes t_G) \Big(\sum_{k=0}^{n-1} x^i\, x^k \otimes z_k\Big) \\
&= (1 \otimes t_G) \Big(\sum_{k=0}^{n-1} x^k \otimes z_k\, x^i\Big) \\
&= \sum_{k=0}^{n-1} x^k\, t_g(z_k\, x^i) \qquad (0 \le i \le n-1) \ ,
\end{aligned}$$

$$\begin{aligned}
t(x^l) &= \sum_{i=0}^{n-1} \pi_i(x^l x^i) = \sum_{i=0}^{n-1} \pi_i \Big(\sum_{k=0}^{n-1} x^{l+k}\, t_G(z_k x^i)\Big) \\
&= \sum_{k=0}^{n-1} \sum_{i=0}^{n-1} \pi_i(x^{l+k})\, \rho^{-i}(t_G(z_k x^i)) \\
&= \sum_{k=0}^{n-1} \sum_{i=0}^{n-1} \pi_i(x^{l+k}) \Big((\rho^*)^{-i}\, t_G(\rho^*)^i\Big)\, (x^i\, z_k) \\
&= \sum_{k=0}^{n-1} \sum_{i=0}^{n-1} \pi_i(x^{l+k})\, t_G(x^i\, z_k) = \sum_{k=0}^{n-1} t_G \Big(\Big(\sum_{i=0}^{n-1} \pi_i(x^{l+k})\, x^i\Big)\, z_k\Big) \\
&= \sum_{k=0}^{n-1} t_G(x^{l+k}\, z_k) = t_G(x^l \sum_{k=0}^{n-1} x^k\, z_k) = t_G(x^l) \qquad (0 \le 1 \le n-1) \ . \blacksquare
\end{aligned}$$

By Proposition 1.3 in [5], when f is a Galois polynomial, f is a separable polynomial. Thus by Theorem 4, we obtain the following result.

Theorem 7. *Let $f \in R[X;\rho]_{(0)}$ be a Galois polynomial with Galois group G, and $t_G\, \rho^* = \rho^*\, t_G$. Then T_f has a left inverse matrix which is a ρ-matrix. In particular, when $f \in R^\rho[X] \cap R[X;\rho]_{(0)}$, f is $\tilde{\rho}$-separable.*

To show that the condition $t_G\,\rho^* = \rho^*\,t_G$ is possible, we give the following example.

Let $f = X^2 - Xa - b \in R[X;\rho]_{(0)}$ be a Galois polynomial. By Lemma 1.5 in [3], its Galois group is $\{1,\sigma\}$, where σ is defined by $\sigma(xb_1+b_0) = (a-x)\,b_1+b_0$, for $xb_1+b_0 \in S$. Then $t_G(xb_1+b_0) = ab_1+2b_0$, $\rho^* t_G(xb_1+b_0) = \rho(a)\,\rho(b_1)+2\rho(b_0)$, and $t_G\,\rho^*(xb_1+b_0) = a\rho(b_1)+2\rho(b_0)$. Since f is Galois, f is separable. Then by Lemma 2 in [4], $\rho(a) = a$. Hence $t_G\,\rho^* = \rho^*\,t_G$.

Next example will show that there exists a separable polynomial which is not $\tilde{\rho}$-separable.

Setting $R = Z/(4) \otimes Z/(4)$, and ρ is the automorphism of R defined by $\rho(x_1,x_2) = (x_2,x_1)$, for $(x_1,x_2) \in R$. It is easy to verify that $f = X^2-1 \in R[X;\rho]_{(0)} \cap R^\rho[X]$. By setting $d = (1,0)$, then $d+\rho(d) = 1$. By Lemma 3 in [3], f is separable. But $\det(T_f) = \delta(f) = 0$. So by Theorem 4, f is not $\tilde{\rho}$-separable.

ACKNOWLEDGEMENTS – The author would like to thank Prof. G. Szeto, Prof. L.J. Ma and Prof. S. Ikehata for their many suggestions and discussions.

REFERENCES

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

[2] Ikehata, S. – On separable polynomials and Frobenius polynomials in skew polynomial rings II, *Math. J. Okayama Univ.*, 25 (1983), 23–28.

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

[4] Nagahara, T. – Note on skew polynomials, *Math. J. Okayama Univ.*, 25 (1983), 43–48.

[5] Miyashita, Y. – Finite outer Galois theory of non-commutative rings, *J. Fac. Sci. Hokkaido Univ.*, Ser. I, 19 (1966), 114–134.

[6] Miyashita, Y. – On a skew polynomial ring, *J. Math. Soc. Japan*, 31 (1979), 317–330.

[7] Szeto, G. – A characterization of separable polynomials over a skew polynomial ring, *J. Austral. Math. Soc.* (series A), 38 (1985), 275–280.

Xiaolong Lou,
Mathematics Department, Zhongshan University,
Guangzhou – P.R. CHINA