Math. J. Okayama Univ. 21 (1979), 167—177

ON SEPARABLE POLYNOMIALS OF DEGREE 2 IN SKEW POLYNOMIAL RINGS II

TAKASI NAGAHARA

Throughout this paper, B will mean a (non-commutative) ring with identity element 1 which has an automorphism ρ and a derivation D so that $\rho D = D\rho$ and $D(ab) = D(a)\rho(b) + aD(b)$ $(a, b \in B)$. By $B[X; \rho, D]$, we denote the ring of all polynomials $\sum_i X^i b_i$ $(b_i \in B)$ with an indeterminate X whose multiplication is defined by $bX = X\rho(b) + D(b)$ for each $b \in B$. Moreover, by $B[X; \rho, D]_2$ (resp. $B[X; \rho, D]_{(2)}$), we denote the subset of $B[X; \rho, D]$ of all ploynomials $f = X^2 - Xa - b$ with $fB[X; \rho, D] = B[X; \rho, D]f$ (resp. $fB[X; \rho, D] = B[X; \rho, D]f$, $\rho(a) = a$, and $D(a) = 0$). For $f = X^2 - Xa - b \in B[X; \rho, D]_2$, $\delta(f)$ denotes the discriminant $a^2 + 4b$, and $B[x; a, b]$ denotes the factor ring $B[X; \rho, D]/fB[X; \rho, D]$ where $x = X + fB[X; \rho, D]$. If the ring $B[x; a, b]$ is separable (resp. Galois) over B then $X^2 - Xa - b$ will be called to be separable (resp. Galois).

In § 1, we prove that any separable polynomial of $B[X; \rho]_2$ $(D = 0)$ belongs to $B[X; \rho]_{(2)}$, and in virtue of the result, we give some generalizations of the results of [3, Ths. 2. 5, 2. 7] and [4, Th. 1] (Ths. 1, 2 and 3).

In § 2, we consider $B[X; \rho, D]_2$ and present some conditions on which polynomials in $B[X; \rho, D]_2$ are separable (Galois). The study contains our main result which is as follows: If there is a polynomial in $B[X; \rho, D]_{(2)}$ whose discriminant is inversible in B then, for $f \in B[X; \rho, D]_2$, f is Galois if and only if f is separable, which is equivalent to that $\delta(f)$ is inversible in B (Th. 16.)

In this note, Z denotes the center of B. Moreover, for any $b \in B$, we write $I_{b,\rho^n}(\alpha) = \alpha b - b\rho^n(\alpha)$ $(\alpha \in B)$, and by b_l (resp. b_r), we denote the left (resp. right) multiplication of B determened by b.

Now, let $X^2 - Xa - b \in B[X; \rho, D]_2$, and consider $B[x; a, b]$. Then, for any $\alpha \in B$, we have

$$\begin{aligned}\alpha x^2 &= (\alpha x)x = (x\rho(\alpha) + D(\alpha))x = x\rho(\alpha)x + D(\alpha)x \\ &= x(x\rho^2(\alpha) + D\rho(\alpha)) + x\rho D(a) + D^2(a) \\ &= x(a\rho^2(\alpha) + 2D\rho(\alpha)) + b\rho^2(\alpha) + D^2(\alpha), \text{ and} \\ \alpha x^2 &= \alpha(xa + b) = \alpha xa + \alpha b = x\rho(\alpha)a + D(\alpha)a + \alpha b.\end{aligned}$$

Since $\{1, x\}$ is a right (left) free B-basis of $B[x; a, b]$, it follows that $\alpha b - b\rho^2(\alpha) = D^2(\alpha) - D(\alpha)a$, and $\rho(\alpha)a - a\rho^2(\alpha) = 2D\rho(\alpha)$, that is, $\alpha a - a\rho(\alpha) = 2D(\alpha)$. Thus we obtain

(i) $I_{a,\rho}=2D$ (ii) $I_{b,\rho^2}=D^2-a_rD.$

Moreover, we have

$$x^3=x(xa+b)=(xa+b)a+xb=x(a^2+b)+ba, \text{ and}$$
$$\begin{aligned}x^3&=(xa+b)x=x(x\rho(a)+D(a))+x\rho(b)+D(b)\\&=(xa+b)\rho(a)+x(D(a)+\rho(b))+D(b)\\&=x(a\rho(a)+D(a)+\rho(b))+b\rho(a)+D(b).\end{aligned}$$

Hence $ba=b\rho(a)+D(b)$ and $a^2+b=a\rho(a)+D(a)+\rho(b)=a^2-I_{a,\rho}(a)+D(a)+\rho(b)=a^2-2D(a)+D(a)+\rho(b)=a^2-D(a)+\rho(b)$. Thus, it follows that

(iii) $ba=b\rho(a)+D(b)$ (iv) $\rho(b)=b+D(a).$

Conversely, if a system $\{a, b\}$ of elements of B satisfies the conditions (i—iv) then the polynomial X^2-Xa-b belongs to $B[X;\ \rho,\ D]_2$. (Cf. [2, Lemma 2. 1]).

1. On $B[X;\rho]_2$ $(D=0)$. First, we shall prove the following theorem which is useful in our study.

Theorem 1. *Let* $f\in B[X;\ \rho]_2$.
(a) *If* $\delta(f)$ *is inversible in* B *then* $f\in B[X;\ \rho]_{(2)}$.
(b) *If* f *is separable then* $f\in B[X;\ \rho]_{(2)}$. (Cf. [5, Remark] and [2, Th. 2. 4]).

Proof. By (i—iv), we have

(1) $$I_{a,\rho}=I_{b,\rho^2}=0,\ \rho(b)=b$$
(2) $$ab=ba=b\rho(a)=\rho(a)b$$
(3) $$a^2=a\rho(a)=\rho(a)\rho(a)=\rho(a^2).$$

By (2) and (3), we obtain $(a^2+4b)\rho(a)=a^2\rho(a)+4b\rho(a)=a^2a+4ba=(a^2+4b)a$. Hence, if a^2+4b is inversible in B then $\rho(a)=a$, and so, $f\in B[X;\ \rho]_{(2)}$. Next, we assume that f is separable. Then, the (left)A-(right)A-homomorphism

$$\phi:\ A\otimes_B A\to A\quad(\textstyle\sum_i a_i\otimes b_i\to\sum_i a_ib_i)$$

splits. Hence there exists an element e in $A\otimes_B A$ such that $\phi(e)=1$ and $(c\otimes 1)e=e(1\otimes c)$ for all $c\in A$. Since $A\otimes_B A=(x\otimes x)B+(x\otimes 1)B+(1\otimes x)B+(1\otimes 1)B$, we may write

$$e=(x\otimes x)b_1+(x\otimes 1)b_2+(1\otimes x)b_3+(1\otimes 1)b_4$$

where $b_i\in B$, $i=1,\cdots,4$. Then, we have that $x^2b_1+xb_2+xb_3+b_4=1$ and $(x\otimes 1)e=e(1\otimes x)$. Since $\{x\otimes x,\ x\otimes 1,\ 1\otimes x,\ 1\otimes 1\}$ is a right free B-basis of $A\otimes_B A$, one will easily see that

(4) $$1=bb_1+b_4$$

(5) $$ab_2+b_4=b\rho(b_1).$$

Now, in virtue of (1 — 5), we can prove the assertion (b) which is as follows:

$\rho(a)=\rho(a(bb_1+b_4))=\rho(abb_1)+\rho(ab_4)$ (by (4))
$=\rho(a)b\rho(b_1)+\rho(a)\rho(b_4)$ (by (1))
$=ba\rho(b_1)+\rho(a)\rho(b\rho(b_1)-ab_2)$ (by (2, 5))
$=ba\rho(b_1)+\rho(a)b\rho^2(b_1)-\rho(a)\rho(a)\rho(b_2)$ (by (1))
$=bb_1a+ba\rho^2(b_1)-aa\rho(b_2)$ (by (1, 2, 3))
$=(1-b_4)a+b\rho(b_1)a-ab_2a$ (by (4, 1))
$=(1-b_4)a+b\rho(b_1)a-(b\rho(b_1)-b_4)a=a$ (by (5)).

This completes the proof.

By Th. 1 and [3, Th. 2. 5], we have the following theorem, which has been noted also in [5].

Theorem 2. *For $f\in B[X;\ \rho]_2$, f is Galois if and only if $\delta(f)$ is inversible in B.*

Next, we consider the following conditions.

(C_1) 2 is inversible in B.
(C_2) $\rho|Z$ (the restriction ρ to Z)$=1$.
(C_3) $B[X;\ \rho]_2$ contains a Galois polynomial.
(C_4) $B[X;\ \rho]_2$ contains a separable polynomial X^2-Xa.

Then, by Ths. 1, 2, [3, Th. 2. 7] and [4, Th. 1], we obtain the following

Theorem 3. *Assume one of the conditions* (C_1 — C_4). *Then, for $f\in B[X;\ \rho]_2$, the following conditions are equivalent.*

(a) *f is Galois.*
(b) *f is separable.*
(c) *$\delta(f)$ is inversible in B.*

2. On $B[X;\ \rho,\ D]_2$. Now, we shall begin our study with the following lemma.

Lemma 4. *Let $f=X^2-Xa-b\in B[X;\ \rho,\ D]_2$ and set $d=ba-ab$. Then*

(v) $$\alpha\delta(f)=\delta(f)\rho^2(\alpha) \quad \textit{for any } \alpha\in B.$$

(vi) $$\delta(f)\rho(a)=\delta(f)a-2d.$$

(vii) $$\delta(f)D(a)=ad+2d(a-\rho(a)).$$

Proof. By (i, ii), we have that for any $\alpha \in B$,

$$\begin{aligned}
\alpha(a^2+4b) &= \alpha a^2+4\alpha b \\
&= (a\rho(\alpha)+2D(\alpha))a+4(b\rho^2(\alpha)+D^2(\alpha)-D(\alpha)a) && \text{(by (i, ii))} \\
&= a\rho(\alpha)a+2D(\alpha)a+4b\rho^2(\alpha)+4D^2(\alpha)-4D(\alpha)a \\
&= a(a\rho^2(\alpha)+2D\rho(\alpha))+2(a\rho D(\alpha)+2D^2(\alpha))+4b\rho^2(\alpha)+4D^2(\alpha)-4D(\alpha)a \\
&= a^2\rho^2(\alpha)+2aD\rho(\alpha)+2a\rho D(\alpha)+4D^2(\alpha)+4b\rho^2(\alpha)+4D^2(\alpha)-4D(\alpha)a \\
&= (a^2+4b)\rho^2(\alpha)+4aD\rho(\alpha)+8D^2(\alpha)-4D(\alpha)a \\
&= (a^2+4b)\rho^2(\alpha)+4(aD\rho(\alpha)+2D^2(\alpha)-D(\alpha)a) \\
&= (a^2+4b)\rho^2(\alpha)+4(2D(D(\alpha))-I_{a,\rho}(D(\alpha))) = (a^2+4b)\rho^2(\alpha) && \text{(by (i))}.
\end{aligned}$$

Moreover, by (i, iii, iv), we have

$$\begin{aligned}
(a^2+4b)\rho(a) &= a^2\rho(a)+4b\rho(a) = a(a\rho(a))+4b\rho(a) \\
&= a(a^2-2D(a))+4(ba-D(b)) && \text{(by (i, iii))} \\
&= (a^2+4b)a-2(aD(a)+2D(b)) \\
&= (a^2+4b)a-2(a(\rho(b)-b)+2D(b)) && \text{(by (iv))} \\
&= (a^2+4b)a-2(-ab+a\rho(b)+2D(b)) \\
&= (a^2+4b)a-2(-ab+ba) && \text{(by (i))} \\
&= (a^2+4b)a-2d, \text{ and} \\
(a^2+4b)D(a) &= a^2D(a)+4bD(a) = a^2D(a)+2b(a^2-a\rho(a)) && \text{(by (i))} \\
&= a^2D(a)+2ba(a-\rho(a)) = a^2D(a)+2(ab+d)\ (a-\rho(a)) \\
&= a^2D(a)+2ab(a-\rho(a))+2d(a-\rho(a)) \\
&= a^2D(a)+2aD(b)+2d(a-\rho(a)) && \text{(by (iii))} \\
&= a^2(\rho(b)-b)+a(ba-a\rho(b))+2d(a-\rho(a)) && \text{(by (iv, i))} \\
&= -a^2b+aba+2d(a-\rho(a)) \\
&= ad+2d(a-\rho(a)).
\end{aligned}$$

This completes the proof.

Next, we shall prove the following

Lemma 5. *Let* $g = X^2-Xu-v \in B[X;\ \rho,\ D]_{(2)}$, *and* $X^2-Xa-b \in B[X;\ \rho,\ D]_2$. *Then*

(viii) $\rho(u)=u,\ \rho(v)=v,\ D(u)=D(v)=0$, *and* $uv=vu$.

(ix) $qp=pq$ *for any* $q \in \{u,\ v\}$ *and* $p \in \{a,\ b\}$.

(x) *If* $\delta(g)$ *is inversible in* B *then* $\rho^2(a)=a$ *and* $\rho^2(b)=b$.

Proof. Since $\rho(u)=u$ and $D(u)=0$, it follows from (iii, iv) that $D(v)=0$ and $\rho(v)=v$. From this and (i, ii), we have that for any $q \in \{u, v\}$, $qa-aq=I_{a,\rho}(q)=2D(q)=0=I_{u,\rho}(q)=qu-uq$, and $qb-bq=I_{b,\rho^2}(q)=D^2(q)-D(q)a=0$. This implies (viii, ix). If $\delta(g)$ is inversible in B then $\delta(g)^{-1}\alpha\delta(g)=\rho^2(\alpha)$ $(\alpha \in B)$ by (v). Hence (x) follows immediately

from (ix), completing the proof.

In virtue of (vi, vii, viii), we obtain the following

Corollary 6. *Let* $f=X^2-Xa-b\in B[X;\ \rho,\ D]_2$ *whose discriminant is inversible in* B. *Then,* $f\in B[X;\ \rho,\ D]_{(2)}$ *if and only if* $ab=ba$.

Now, we shall prove the following theorem which is useful in our study and contains the result of K. Kishimoto [1, Th. 1. 2].

Theorem 7. *Let* 2 *be inversible in* B. *Then, for* $f=X^2-Xa-b\in B[X;\ \rho,\ D]_2$, *the following conditions are equivalent.*

(a) f *is Galois.*
(b) f *is separable.*
(c) $(a-\rho(a))^2+4\delta(f)$ *is inversible in* B.

In this case, there holds that $\rho(a-\rho(a))=a-\rho(a)$.

Proof. We consider $B[x;\ a,\ b]$ and set $s=2^{-1}a$. Then, we have that for any $\alpha\in B$,

$$\begin{aligned}\alpha(x-s)&=\alpha x-\alpha s=x\rho(\alpha)+D(\alpha)-\alpha s=x\rho(\alpha)+\alpha s-s\rho(\alpha)-\alpha s\\&=x\rho(\alpha)-s\rho(\alpha)=(x-s)\rho(\alpha),\ \text{and}\\(x-s)^2&=x^2-xs-sx+s^2=xa+b-xs-(x\rho(s)+D(s))+s^2\\&=xa+b-xs-x\rho(s)-s^2+s\rho(s)+s^2\\&=xa+b-xs-(x-s)\rho(s)\\&=(x-s)a+sa+b-(x-s)s-s^2-(x-s)\rho(s)\\&=(x-s)\ (a-s-\rho(s))+sa+b-s^2.\end{aligned}$$

Hence, for the polynomial $h=Y^2-Y(a-s-\rho(s))-(sa+b-s^2)\in B[Y;\ \rho]_2$, we obtain the B-ring isomorphism

$$B[X;\ \rho,\ D]/fB[X;\ \rho,\ D]\simeq B[Y;\ \rho]/hB[Y;\ \rho].$$

This implies that f is Galois (resp. separable) if and only if h is Galois (resp. separable). Moreover, it is easily seen that $\delta(h)=(a-s-\rho(s))^2+4(sa+b-s^2)=4^{-1}(a-\rho(a))^2+(a^2+4b)$. By Th. 3, h is Galois if and only if h is separable, which is equivalent to that $\delta(h)$ is inversible in B. Thus, it follows that the conditions (a), (b) and (c) are equivalent. Now, let f be separable. Then h is separable, and hence by Th. 1, we have $h\in B[Y;\ \rho]_{(2)}$, that is, $\rho(a-s-\rho(s))=a-s-\rho(s)$. Since $s=2^{-1}a$, we obtain $\rho(a-\rho(a))=a-\rho(a)$. This completes the proof.

Corollary 8. *Let* 2 *be inversible in* B. *Then, for a polynomial*

$f = X^2 - Xa - b$ of $B[X; \rho, D]_2$ with $a\rho(a) = \rho(a)a$, the following conditons are equivalent.

(a) *f is Galois.*

(b) *f is separable.*

(c) *$\delta(f)$ is inversible in B.*

Proof. By the assumption and (i), we have $(a-\rho(a))^2 = a^2 - a\rho(a) - (a\rho(a) - \rho(a)\rho(a)) = 2D(a) - 2D(a) = 0$. Hence the assertion follows immediately from Th. 7.

Corollary 9. *Let 2 be inversible in B. Let $f = X^2 - Xa - b$ be a polynomial in $B[X; \rho, D]_2$ which satisfies one of the conditions* (1), (2), (3) *and* (4):

(1) *$D(a) = 0$ and $D(b) = 0$.*

(2) *$D(a) = 0$ and $ab = ba$.*

(3) *$a\rho(a) = \rho(a)a$ and $ab = ba$.*

(4) *$\rho^2(a) = a$.*

Then, the following conditions are equivalent.

(a) *f is Galois.*

(b) *f is separable.*

(c) *$\delta(f)$ is inversible in B.*

(d) *$\delta(f)$ is inversible in B and $f \in B[X; \rho, D]_{(2)}$*

Proof, In case (1), we have $\rho(b) = b + D(a) = b$ (by (v)), and so, $ba - ab = ba - a\rho(b) = 2D(b) = 0$. Moreover, in case (4), there holds that $0 = a\delta(f) - \delta(f)\rho^2(a) = 4(ab - ba)$ (by (v)). Hence, by Cor. 6 and Th. 7, it suffices to prove that (b) implies (c). Assume (b). Case (1) is contained in case (2). In case (2), it follows from (i) and Th. 7 that

$$\begin{aligned}(a-\rho(a))^2 &= (a-\rho(a))a - (a-\rho(a))\rho(a) \\ &= (a-\rho(a))a - a(a-\rho(a)) \\ &= (a-\rho(a))a - a\rho(a-\rho(a)) \\ &= 2D(a-\rho(a)) = 2D(a) - 2\rho D(a) = 0,\end{aligned}$$

whence $\delta(f)$ is inversible in B. In case (3), the assertion is a direct consequence of Cor. 8. In case (4), we have that $2(a-\rho(a)) = a - \rho(a) + \rho(a-\rho(a)) = 0$ (by Th. 7), whence $\delta(f)$ is inversible in B. Thus we obtain (c), completing the proof.

Lemma 10. *Let $B = dB + cB$ with $c \in Z$. Then*

$$B = (d^m + c^n b)^r B + c^s B$$

for any $b \in B$ and any positive integers m, n, r, s.

Proof. By the assumption, we may write $1=dx+cy$ $(x,\ y\in B)$. Then we have

$$d=d^2x+dcy=d^2x+dc(dx+cy)y=d^2p_1+c^2q_1\ (p_1,\ q_1\in B)$$
$$c=cdx+c^2y=cd(dx+cy)x+c^2y=d^2p_2+c^2q_2\ (p_2,\ q_2\in B)$$

and hence

$$1=dx+cy=(d^2p_1+c^2q_1)x+(d^2p_2+c^2q_2)y=d^2x_2+c^2y_2\ (x_2,\ y_2\in B).$$

Therefore, it follows that $1=d^tx_k+c^ty_k$ $(x_k,\ y_k\in B)$ for $t=2^k$ where k is any positive integer. Moreover, if $2^k\geqq m$, $n(>0)$ then $B=d^mB+c^nB$. Thus we obtain that for any $b\in B$,

$$B=d^mB+c^nB=(d^m+c^nb)B+c^nB=(d^m+c^nb)B+cB$$
$$=(d^m+c^nb)^rB+c^sB$$

where m, n, r, s are any positive integers. This completes the proof.

By virtue of Th. 7 and Lemma 10, we can prove the following

Lemma 11. *Let* $f=X^2-Xa-b$ *be a separable polynomial in* $B[X;\ \rho,\ D]_2$. *Then* $2^r\rho(a-\rho(a))=2^r(a-\rho(a))$ *for some integer* $r\geq 0$. *If* $B=aB+2B$ *then*

$$B=\delta(f)B+2^m(a-\rho(a))^nB=B\delta(f)+B(a-\rho(a))^n2^m$$

for any integers $m,\ n\geq 0$.

Proof. If 2 is nilpotent then the assertion is obvious by Lemma 10. Hence we assume that 2 is not nilpotent. We set $M=\{2^n\mid n\geq 0\}\subset B$. By B_M, we denote the (quotient) ring of fractions formed with respect to M and we write $\alpha_M=\alpha/1\in B_M$ for any $\alpha\in M$. Since $\rho(2)=2$ and $D(2)=0$, we have the automorphism ρ_M (resp. the derivation D_M) of B_M induced by ρ (resp. by D). Now, we consider the ring extension $B[x;\ a,\ b]$ of B. Since this is a free B-module, there is a B_M-ring isomorphism

$$B[x;\ a,\ b]_M\simeq B_M[X;\ \rho_M,\ D_M]/(X^2-Xa_M-b_M)B_M[X;\ \rho_M,\ D_M].$$

Since X^2-Xa-b is separable, $B[x;\ a,\ b]$ is separable over B, whence $B[x;\ a,\ b]_M$ is separable over B_M. From this, it follows that $X^2-Xa_M-b_M$ $(\in B_M[X;\ \rho_M,\ D_M])$ is separable. Hence, by Th. 7, we have that $2^r\rho(a-\rho(a))=2^r(a-\rho(a))$ for some integer $r\geq 0$. Now, let $n\geq 0$ be an integer, and set $\delta=a^2+4b$. Since $\rho(a-\rho(a))_M=(a-\rho(a))_M$, it follows from (v) that $(a-\rho(a))_M\delta_M=\delta_M(a-\rho(a))_M$. This gives that

$$((a-\rho(a))^2+4\delta)_M^n=(a-\rho(a))_M^{2n}+\delta c_M$$

for some $c\in B$, which is inversible in B_M (by Th. 7). Hence there exists

an element c_1 in B_M such that

$$1_M=((a-\rho(a))_M^{2n}+\delta c_M)c_1=(a-\rho(a))_M^{2n}c_1+\delta c_M c_1.$$

We have therefore

$$2^s=(a-\rho(a))^{2n}c_2+\delta c_3$$

for some integer $s\geq 0$ and some elements c_2, $c_3\in B$. Now assume $B=aB+2B$. Then, it follows from Lemma 10 that for any integer $m\geq 0$,

$$\begin{aligned}B&=\delta B+2^{m+s}B=\delta B+2^m((a-\rho(a))^{2n}c_2+\delta c_3)B\\&=\delta B+2^m(a-\rho(a))^{2n}B=\delta B+2^m(a-\rho(a))^nB.\end{aligned}$$

Evidently $B=aB+2B=Ba+B2$ (by (i)). Hence, by a similar way, we have $B=B\delta+B(a-\rho(a))^n2^m$ for any integers m, $n\geq 0$. This completes the proof.

In virtue of Lemma 11, we obtain the following corollary whose proof proceeds just as in the proof of Cor. 9((b)$\Longrightarrow$(c)), and it may be omitted.

Corollary 12. *Let $f=X^2-Xa-b$ be a separable polynomial in $B[X;\ \rho,\ D]_2$ which satisfies one of the conditions* (1)–(3):

(1) $2^sD(a)=0$ *for some integer* $s\geq 0$.

(2) $2^s(a\rho(a)-\rho(a)a)=0$ *for some integer* $s\geq 0$.

(3) $2^s(\rho^2(a)-a)=0$ *for some integer* $s\geq 0$.

If $B=aB+2B$ then $\delta(f)$ is inversible in B.

Now, we shall prove the following theorem which contains the result of Y. Miyashita [2, Th. 2. 4 (ii$\Longleftrightarrow$v)].

Theorem 13. *Let $f=X^2-Xa-b$ be a polynomial in $B[X;\ \rho,\ D]_2$ which satisfies one of the conditions* (1)–(5):

(1) $D(a)=0$ *and* $2\rho^2(a)=2a$.

(2) $D(a)=0$ *and* $2D(b)=0$.

(3) $D(a)=0$ *and* $2ab=2ba$.

(4) $ab=ba$ *and* $2a\rho(a)=2\rho(a)a$.

(5) $ab=ba$ *and* $2\rho^2(a)=2a$.

Then, the following conditions are equivalent.

(a) *f is Galois and $B=aB+2B$*

(b) *f is separable and $B=aB+2B$*

(c) *$\delta(f)$ is inversible in B.*

(d) *$\delta(f)$ is inversible in B and $f\in B[X;\ \rho,\ D]_{(2)}$.*

Proof. By Lemma 5(viii) and [3, Lemma 1. 5], we see that (d)

implies (a). Evidently (a) implies (b). Moreover, it follows from Cor. 12 that (b) implies (c). Hence, it suffices to prove that (c) implies (d). Assume (c). In case (1) and (2), we have

$$2(ab-ba)=2(ab-b\rho^2(a))=2(D^2(a)-D(a)a)=0 \quad \text{(by (ii))},$$
$$2(ba-ab)=2(ba-a(\rho(b)-D(a))=4D(b)=0 \quad \text{(by (iv))}$$

respectively. Hence these cases are contained in case (3). In case (3), there holds $\rho(a)=a$ (by (vi)), which implies (d). In case (4) and (5), our assertions follow immediately from Cor. 6. This completes the proof.

Lemma 14. *Let* $2=0$ *and assume that* $B[X;\ \rho,\ D]_2$ *contains a polynomial* $g=X^2-Xu-v$ *such that* $\delta(g)$ *is inversible in* B *and* $D(u)=0$. *Then* $g\in B[X;\ \rho,\ D]_{(2)}$. *If* f *is a separable polynomial in* $B[X;\ \rho,\ D]_2$ *then* $\delta(f)$ *is inversible in* B, *and* $f\in B[X;\ \rho,\ D]_{(2)}$.

Proof. Since $\alpha u-u\rho(\alpha)=2D(\alpha)=0$ $(\alpha\in B)$, it follows that $\rho(\alpha)=u^{-1}\alpha u$ $(\alpha\in B)$, $\rho(u)=u$, and so, $g\in B[X;\ \rho,\ D]_{(2)}$. Let $X^2-Xa-b\in B[X;\rho,\ D]_2$. Then, by Lemma 5(ix), we have that $\rho(a)=u^{-1}au=a$, $D(a)=u^{-1}bu-b=0$ (by (iv)), which implies $X^2-Xa-b\in B[X;\ \rho,\ D]_{(2)}$, whence

$$\rho(r)=r,\ D(r)=0,\ rs=sr \text{ for any } r,\ s\in\{a,\ b,\ u,\ v\},$$
$$D(u^{-1})=u^{-1}(uD(u^{-1}))=u^{-1}(D(1)-D(u)u^{-1})=0.$$

Now, we consider $B[x;\ a,\ b]$, and set $y=xu^{-1}$. Then we have that for any $\alpha\in B$, $\alpha y=\alpha xu^{-1}=(x\rho(\alpha)+D(\alpha))u^{-1}=x\rho(\alpha)u^{-1}+D(\alpha)u^{-1}=y\alpha+D(\alpha)u^{-1}$, and $y^2=(xu^{-1})^2=x^2u^{-2}=xau^{-2}+bu^{-2}=yau^{-1}+bu^{-2}$. We denote $u_r^{-1}D$ by D_0. Since $D_0(au^{-1})=D(au^{-1})u^{-1}=aD(u^{-1})u^{-1}=0$, it follows that

$$Y^2-Yau^{-1}-bu^{-2},\ Y^2-Y-vu^{-2}\in B[Y;\ D_0]_{(2)}.$$

If $X^2-Xa-b(\in B[X;\ \rho,\ D]_2)$ is separable then $Y^2-Yau^{-1}-bu^{-2}$ is separable in $B[Y;\ D_0]$, and whence by [3, Th. 3. 4], $\delta(Y^2-Yau^{-1}-bu^{-2})=(au^{-1})^2$ is inversible in B. Thus a is inversible in B, completing the proof.

Lemma 15. *Assume that* $B[X;\ \rho,\ D]_{(2)}$ *contains a polynomial* g *such that* $\delta(g)$ *is inversible in* B. *If* f *is a separable polynomial in* $B[X;\ \rho,\ D]_2$ *then* $\delta(f)$ *is inversible in* B.

Proof. By Lemma 5(x) and Cor. 9, it suffices to prove the lemma in case $B\neq 2B$. Assume $B\neq 2B$. We consider here the factor ring $\bar{B}=B/2B$ and set $\bar{a}=a+2B$. Evidently $\rho(2B)=2B$ and $D(2B)\subset 2B$. Hence there exists the automorphism $\bar{\rho}$ (resp. the derivation $\bar{D}$) of $\bar{B}$ induced by ρ (resp. D). Now, let $X^2-Xa-b\in B[X;\ \rho,\ D]_2$. Then $X^2-X\bar{a}-\bar{b}\in\bar{B}[X;\ \bar{\rho},\ \bar{D}]_2$.

Since $B[x;\ a,\ b]$ is a free right (left) B-module, we have the $\bar{B}$-ring isomorphism

$$B[x;\ a,\ b]/2B[x;\ a,\ b] \simeq \bar{B}[X;\ \bar{\rho},\ \bar{D}]/(X^2-X\bar{a}-\bar{b})\bar{B}[X;\ \bar{\rho},\ \bar{D}].$$

Now, we assnme that X^2-Xa-b is separable, and write $g=X^2-Xu-v$. Then $X^2-X\bar{a}-\bar{b}$ $(\in B[X;\bar{\rho},\bar{D}]_2)$ is separable, $X^2-X\bar{u}-\bar{v}\in\bar{B}[X;\bar{\rho},\bar{D}]_{(2)}$, and $\bar{u}^2$ is inversible in $\bar{B}$ by our assumption. Since $\bar{2}=\bar{0}$ $(\in\bar{B})$, it follows from Lemma 14 that $\bar{a}$ is inversible in $\bar{B}$. Thus we obtain $B=aB+2B$. Therefore, by Lemma 5(x) and Cor. 12, a^2+4b is inversible in B. This completes the proof.

Now, we shall conclude the study with the following theorem which is our main result and this contains the results of [3, Th. 3. 4 (Case (C_1))] and [4, Th. 1].

Theorem 16. *Assume that $B[X;\ \rho,\ D]_{(2)}$ contains a polynomial g such that $\delta(g)$ is inversible in B. Then, for a polynomial $f\in B[X;\ \rho,\ D]_2$, the following conditions are equivalent.*

(a) *f is Galois.*
(b) *f is separable.*
(c) *$\delta(f)$ is inversible in B.*
(d) *$\delta(f)$ is inversible in B, and $f\in B[X;\ \rho,\ D]_{(2)}$.*

Proof. By virtue of Lemma 5 and [3, Lemma 1. 5], we see that (d) implies (a). Evidently (a) implies (b). Moreover, it follows from Lemma 15 that (b) implies (c). Hence it suffices to prove that (c) implies (d). We now set $g=X^2-Xu-v$ and let $f=X^2-Xa-b\in B[X;\ \rho,\ D]_2$ so that $\delta(f)$ is inversible in B. Then, by Lemma 5, we have that $\rho^2(a)=a$, $\rho^2(b)=b$, $au=ua$, and $bu=ub$. From this and (i, iv), it follows that

$$2D(a+\rho(a))=I_{\prime,\rho}(a+\rho(a))=0,\ \ 2D(b+\rho(b))=0$$

and

$$\begin{aligned}
4(ba-ab) &= 4(ba-ab)-4D(b+\rho(b)) \\
&= 4(ba-ab)-2((b+\rho(b))a-a(b+\rho(b))) && \text{(by (i))} \\
&= 4(ba-ab)-2((2b+D(a))a-a(2b+D(a))) && \text{(by (iv))} \\
&= -2D(a)a+2aD(a) \\
&= -(a^2-a\rho(a))a+a(a^2-a\rho(a)) && \text{(by (i))} \\
&= a\rho(a)a-a^2\rho(a)=a\rho(a)a-a(2D(a+\rho(a))+a\rho(a)) \\
&= a\rho(a)a-a((a+\rho(a))a-a(a+\rho(a))+a\rho(a)) && \text{(by (i))} \\
&= a\rho(a)a-a\rho(a)a=0.
\end{aligned}$$

Moreover, we have

$$
\begin{aligned}
u(ba-ab) &= u(a\rho(b)-ab+2D(b)) && \text{(by (i))}\\
&= a(u\rho(b)-bu)+2uD(b) && \text{(by (ix))}\\
&= a(-2D(b))+2uD(b)=(u-a)2D(b) && \text{(by (i))}\\
&= (u-a)b(2a-2\rho(a)) && \text{(by (iii))}\\
&= (u-a)b(a^2+4b)^{-1}(a^2+4b)\ (2a-2\rho(a))\\
&= (u-a)b(a^2+4b)^{-1}4(ba-ab) = 0 && \text{(by (vi)).}
\end{aligned}
$$

Hence we obtain $(u^2+4v)\ (ba-ab)=0$, which implies $ba=ab$. Thus, it follows from Cor. 6 that $f\in B[X;\ \rho,\ D]_{(2)}$. This shows that (c) implies (d), completing the proof.

REFERENCES

[1] K. KISHIMOTO : A classification of free quadratic extensions of rings, Math. J. Okayama Univ. **18** (1976), 139—148.

[2] Y. MIYASHITA : On a skew polynomial ring, J. Math. Soc. Japan **31**(1979), 317—330.

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

[4] T. NAGAHARA : Supplements to the previous paper "On separable polynomials of degree 2 in skew polynomial rings", Math. J. Okayama Univ. **19** (1977). 159—161.

[5] T. NAGAHARA and K. KISHIMOTO : On free cyclic extensions of rings. Proc. 10 th Symp. Ring Theory (Shinshu Univ., Matsumoto, 1977). 1978, 1—25.

DEPARTMENT OF MATHEMATICS

OKAYAMA UNIVERSITY

(Received March 15, 1979)