THE INVERTIBILITY OF AN ELEMENT $\alpha^2 - a$ OF A SUPER-PRIMITIVE EXTENSION $R[\alpha]/R$ AND A LINEAR FORM OF A LAURENT EXTENSION $R[\alpha,\ \alpha^{-1}]$

MITSUO KANEMITSU, KIYOSHI BABA AND KEN-ICHI YOSHIDA

Received March 6, 2000; revised June 3, 2000

Abstract. Let R be an integral domain and α a super-primitive element of degree $d \geq 2$ over R. In the preceding paper [1] we have discussed the invertibility of an element $\alpha - a$ and the flatness of $R[\alpha]/R$. In this paper we will give some conditions for an element $\alpha^2 - a$ to be a unit of $R[\alpha]$ and give a sufficient condition for the extension $R[\alpha]/R$ to be a flat extension. Furthermore, we will prove an analogous result to Theorem 7 in [1]. Finally we will give some results on the invertibility of a linear form $a\alpha - b$ of a Laurent extension $R[\alpha,\ \alpha^{-1}]$.

Introduction

Let R be an integral domain with the quotient field K and $R[X]$ a polynomial ring over R in an indeterminate X. Let α be an element of an algebraic field extension of K and $\pi : R[X] \longrightarrow R[\alpha]$ the R-algebra homomorphism defined by $\pi(X) = \alpha$. Let $\varphi_\alpha(X)$ be the minimal polynomial of α over K with deg $\varphi_\alpha(X) = d$ and write

$$\varphi_\alpha(X) = X^d + \eta_1 X^{d-1} + \cdots + \eta_d,\ (\eta_1,\ \cdots,\ \eta_d \in K).$$

We will define

$$I_{[\alpha]} := \cap_{i=1}^{d} (R\ :_R\ \eta_i)$$

and

$$J_{[\alpha]} := I_{[\alpha]}(1,\ \eta_1,\ \cdots,\ \eta_d)$$

where $(R\ :_R\ \eta_i) = \{c \in R \mid c\eta_i \in R\}$ and $(1,\ \eta_1,\ \cdots,\ \eta_d)$ is an R-module generated by $1,\ \eta_1,\ \cdots,\ \eta_d$. An element α is called an *anti-integral element* of degree d over R if Ker $\pi = I_{[\alpha]}\varphi_\alpha(X)R[X]$. We say that the extension $R[\alpha]/R$ is an *anti-integral extension* if α is an anti-integral element of degree d over R. An element α is said to be a *super-primitive element* of degree d over R if $J_{[\alpha]} \not\subset p$ for every $p \in \mathrm{Dp}_1(R)$ where $\mathrm{Dp}_1(R) = \{\ p \in \mathrm{Spec}(R) \mid \text{depth } R_p = 1\ \}$. The extension $R[\alpha]/R$ is called a *super-primitive extension* if α is a super-primitive element of degree d over R.

Let a be an element of R satisfying $\mathrm{rad}(a) \notin K$, where $\mathrm{rad}(a) = \{\ b \in R \mid nb \in (a) \text{ for } n > 0\}$. Assume that $[K(\mathrm{rad}(a))(\alpha)\ :\ K(\mathrm{rad}(a))] = d$. Then the minimal polynomial of α over $K(\mathrm{rad}(a))$ coincides with $\varphi_\alpha(X)$. We will set $B = R[\mathrm{rad}(a)]$ and define

$$I_{B,\ [\alpha]} := \cap_{i=1}^{d} (B\ :_B\ \eta_i),$$

1991 *Mathematics Subject Classification.* 13B02.
Key words and phrases. flat extension, anti-integral extension, Laurent extension.

$$J_{B,\ [\alpha]} := I_{B,\ [\alpha]}(1,\ \eta_1,\ \cdots,\ \eta_d)$$

where $(B\ :_B\ \eta_i) = \{\ b \in B\ \mid\ b\eta_i \in B\ \}$ and $(1,\ \eta_1,\ \cdots,\ \eta_d)$ is a B-module generated by $1,\ \eta_1,\ \cdots,\ \eta_d$. Since rad $(a)\ \notin K$ and $a \in R$, we know that $B = R + R\ \mathrm{rad}(a)$ and B is a free R-module of rank 2. Hence B/R is a flat extension. This implies that

$$\begin{aligned} I_{B,\ [\alpha]} &:= \cap_{i=1}^{d}(B\ :_B\ \eta_i) = \cap_{i=1}^{d}(R\ :_R\ \eta_i)B \\ &= \{\ \cap_{i=1}^{d}(R\ :_R\ \eta_i)\}B = I_{[\alpha]}B \end{aligned}$$

and

$$J_{B,\ [\alpha]} := I_{B,\ [\alpha]}(1,\ \eta_1,\ \cdots,\ \eta_d) = I_{[\alpha]}(1,\ \eta_1,\ \cdots,\ \eta_d)B = J_{[\alpha]}B.$$

Assume that α is a super-primitive element of degree d over R. Then grade $J_{[\alpha]} > 1$. Since B/R is a flat extension, we get grade $J_{[\alpha]}B > 1$. This shows that α is also a super-primitive element of degree d over B. Hence α is an anti-integral element of degree d over B by [4, Theorem 1.12].

Our notation is standard and unexplained one is referred to [3].

We will list some facts which use later for reference sake.

Lemma 1 ([1, Proposition 2]). *Let B be an integral domain and α an anti-integral element of degree $d\ \geq 2$ over B. Let a be an element of B. If $\alpha - a$ is not a unit of $B[\alpha]$, there exists an element b of $I_{[\alpha]}$ such that $b\varphi_\alpha(a) = 1$, that is, $I_{[\alpha]}\varphi_\alpha(a) = B$.*

Lemma 2 ([1, Proposition 8]). *Let B be an integral domain and α an anti-integral element of degree d over B. Let a be an element of B. If $I_{[\alpha]}\varphi_\alpha(a) = B$, then $\alpha - a$ is a unit of $B[\alpha]$.*

We will give a condition for an element $\alpha^2 - a$ to be a unit of B.

Proposition 3. *Let R be an inetgral domain with the quotient field K. Let a be an element of R such that* rad $(a) \notin K$. *Let α be a super-primitive element of degree $d \geq 2$ over R. Assume that $[K(\mathrm{rad}\ (a))(\alpha)\ :\ K(\mathrm{rad}\ (a))] = d$. Set $A = R[\alpha]$ and $B = R[\mathrm{rad}(a)]$.*
Then the following conditions are equivalent to each other.
(i) *$\alpha^2 - a$ is a unit of A.*
(ii) *$I_{[\alpha]}\varphi_\alpha(\mathrm{rad}(a))B = B$ and $I_{[\alpha]}\varphi_\alpha(-\mathrm{rad}(a))B = B$.*

Proof. (i) $\Longrightarrow$ (ii). By the condition (i) and $\alpha^2 - a = (\alpha - \mathrm{rad}(a))(\alpha + \mathrm{rad}(a))$, we know that both $\alpha - \mathrm{rad}(a)$ and $\alpha + \mathrm{rad}(a)$ are units of $B[\alpha]$. Therefore Lemma 1 implies the condition (ii).

(ii) $\Longrightarrow$ (i). By Lemma 2 we see that $\alpha - \mathrm{rad}(a)$ and $\alpha + \mathrm{rad}(a)$ are units of $B[\alpha]$. Then $\alpha^2 - a$ is also a unit of $B[\alpha]$. Besides, $\alpha^2 - a$ is an element of A. Then $\alpha^2 - a$ is a unit of A because $B[\alpha]/A$ is an integral extension. ☐

We will make two equalities of the condition (ii) in Proposition 3 into one. We will need some definitions.

If d is even, then set $d = 2\ell$,

$$\varphi_{\alpha,\ 0}(X) = X^{2\ell} + \eta_2 X^{2(\ell-1)} + \ \cdots\ + \ \eta_{d-2}X^2 + \eta_d$$

and

$$\varphi_{\alpha,\ 1}(X) = (\eta_1 X^{2\ell-1} + \eta_3 X^{2\ell-3} + \cdots + \eta_{d-1}X)X^{-1}.$$

If d is odd, then set $d = 2\ell + 1$,

$$\varphi_{\alpha,\ 0}(X) = \eta_1 X^{2\ell} + \eta_3 X^{2\ell-2} + \cdots + \eta_{d-2}X^2 + \eta_d$$

and

$$\varphi_{\alpha,\ 1}(X) = (X^{2\ell+1} + \eta_2 X^{2\ell-1} + \cdots + \eta_{d-1}X)X^{-1}.$$

Note that $\varphi_\alpha(X) = \varphi_{\alpha,\ 0}(X) + X\varphi_{\alpha,\ 1}(X)$ and $\varphi_{\alpha,\ 0}(X),\ \varphi_{\alpha,\ 1}(X) \in K[X^2]$. Hence $I_{[\alpha]}\varphi_{\alpha,\ 0}(\mathrm{rad}(a))$ and $I_{[\alpha]}\varphi_{\alpha,1}(\mathrm{rad}(a))$ are ideals of R.

Theorem 4. *Let R be an inetgral domain with the quotient field K. Let a be an element of R such that* rad $(a) \notin K$. *Let α be a super-primitive element of degree $d \geq 2$ over R. Assume that $[K(\mathrm{rad}\ (a))(\alpha) : K(\mathrm{rad}\ (a))] = d$. Then the following conditions are equivalent to each other.*

(i) *$\alpha^2 - a$ is a unit of $R[\alpha]$.*

(ii) $I^2_{[\alpha]}(\varphi_{\alpha,\ 0}(\mathrm{rad}(a))^2 - a\varphi_{\alpha,\ 1}(\mathrm{rad}(a))^2) = R$.

Proof. Set $B = R[\mathrm{rad}(a)]$ and $A = R[\alpha]$.

(i) $\Longrightarrow$ (ii). By Proposition 3, we have $I_{[\alpha]}\varphi_\alpha(\mathrm{rad}(a))B = B$ and $I_{[\alpha]}\varphi_\alpha(-\mathrm{rad}(a))B = B$. On the other hand we get

$$\varphi_\alpha(\mathrm{rad}(a)) = \varphi_{\alpha,\ 0}(\mathrm{rad}(a)) + \mathrm{rad}(a)\ \varphi_{\alpha,\ 1}(\mathrm{rad}(a))$$

and

$$\begin{aligned}\varphi_\alpha(-\mathrm{rad}(a)) &= \varphi_{\alpha,\ 0}(-\mathrm{rad}(a)) - \mathrm{rad}(a)\varphi_{\alpha,\ 1}(-\mathrm{rad}(a)) \\ &= \varphi_{\alpha,\ 0}(\mathrm{rad}(a)) - \mathrm{rad}(a)\varphi_{\alpha,\ 1}(\mathrm{rad}(a)).\end{aligned}$$

Hence $\varphi_\alpha(\mathrm{rad}(a))\varphi_\alpha(-\mathrm{rad}(a)) = \varphi_{\alpha,\ 0}(\mathrm{rad}(a))^2 - a\varphi_{\alpha,\ 1}(\mathrm{rad}(a))^2$.
Therefore

$$B = I^2_{[\alpha]}\varphi_\alpha(\mathrm{rad}(a))\varphi_\alpha(-\mathrm{rad}(a))B = I^2_{[\alpha]}(\varphi_{\alpha,0}(\mathrm{rad}(a))^2 - a\ \varphi_{\alpha,1}(\mathrm{rad}(a))^2)B.$$

We will prove that $I^2_{[\alpha]}(\varphi_{\alpha,\ 0}(\mathrm{rad}(a))^2 - a\varphi_{\alpha,\ 1}(\mathrm{rad}(a))^2) = R$. Suppose the contrary. Then there exists a prime ideal p of R such that $I^2_{[\alpha]}(\varphi_{\alpha,\ 0}(\mathrm{rad}(a))^2 - a\varphi_{\alpha,\ 1}(\mathrm{rad}(a))^2) \subset p$. Since B is integral over R, we can take a prime ideal P of B lying over p. Then $I^2_{[\alpha]}(\varphi_{\alpha,\ 0}(\mathrm{rad}(a))^2 - a\varphi_{\alpha,\ 1}(\mathrm{rad}(a))^2)B \subset P$. This is a contradiction.

(ii) $\Longrightarrow$ (i). The condition (ii) implies that $I^2_{[\alpha]}\varphi_\alpha(\mathrm{rad}(a))\varphi_\alpha(-\mathrm{rad}(a))B = B$. Hence $I_{[\alpha]}\varphi_\alpha(\mathrm{rad}(a))B = B$ and $I_{[\alpha]}\varphi_\alpha(-\mathrm{rad}\ (a))B = B$ because $I_{[\alpha]}\varphi_\alpha(\mathrm{rad}(a))B$ and $I_{[\alpha]}\ \varphi_\alpha(-\mathrm{rad}(a))B$ are ideals of B. So we get the required result by Proposition 3. □

Theorem 5. *Let R be an inetgral domain with the quotient field K. Let a be an element of R such that* rad $(a) \notin K$. *Let α be a super-primitive element of degree $d \geq 2$ over R. Assume that $[K(\mathrm{rad}\ (a))(\alpha) : K(\mathrm{rad}\ (a))] = d$. If $\alpha^2 - a$ is a unit of $R[\alpha]$, then the extension $R[\alpha]/R$ is a flat extension.*

Proof. Since α is an anti-integral element of degree d over R, it suffices to prove that $J_{[\alpha]} = R$ by [4, Proposition 2.6]. Assume that $J_{[\alpha]} \neq R$. Then there exists an element p of Spec(R) such that $J_{[\alpha]} \subset p$. Hence $I_{[\alpha]}\varphi_{\alpha,\ 0}(\mathrm{rad}(a)) \subset p$ and $I_{[\alpha]}\varphi_{\alpha,\ 1}(\mathrm{rad}(a)) \subset p$. Therefore

$$I_{[\alpha]}^2(\varphi_{\alpha,\ 0}(\mathrm{rad}(a))^2 - a\varphi_{\alpha,\ 1}(\mathrm{rad}(a))^2) \subset p.$$

On the other hand $I_{[\alpha]}^2(\varphi_{\alpha,\ 0}(\mathrm{rad}(a))^2 - a\varphi_{\alpha,\ 1}(\mathrm{rad}(a))^2 = R$ by Theorem 4 because $\alpha^2 - a$ is a unit of $R[\alpha]$. This is absurd. □

Remark 6. Under the assumptions in Theorem 5 $I_{[\alpha]}$ is an invertible ideal of R because $R = J_{[\alpha]} = I_{[\alpha]}(1,\ \eta_1,\ \cdots,\ \eta_d)$.

Proposition 7. *Let R be an inetgral domain with the quotient field K. Let a and b be elements of R such that* rad (a), rad $(b) \notin K$. *Let α be a super-primitive element of degree $d \geq 2$ over R. Assume that* $[K(\mathrm{rad}\ (a))(\alpha)\ :\ K(\mathrm{rad}\ (a))] = d$ *and* $[K(\mathrm{rad}\ (b))(\alpha)\ :\ K(\mathrm{rad}\ (b))] = d$. *If both $\alpha^2 - a$ and $\alpha^2 - b$ are units of $R[\alpha]$, then*

$$(\varphi_{\alpha,\ 0}(\mathrm{rad}(a))^2 - a\varphi_{\alpha,\ 1}(\mathrm{rad}(a))^2)/(\varphi_{\alpha,\ 0}(\mathrm{rad}(b))^2 - b\varphi_{\alpha,\ 1}(\mathrm{rad}(b))^2)$$

is a unit of R.

Proof. By Theorem 4 we know that

$$I_{[\alpha]}^2(\varphi_{\alpha,\ 0}(\mathrm{rad}(a))^2 - a\varphi_{\alpha,\ 1}(\mathrm{rad}(a))^2) = R = I_{[\alpha]}^2(\varphi_{\alpha,\ 0}(\mathrm{rad}(b))^2 - b\varphi_{\alpha,\ 1}(\mathrm{rad}(b))^2).$$

Since $I_{[\alpha]}$ is an invertible ideal of R, we get

$$(\varphi_{\alpha,\ 0}(\mathrm{rad}(a))^2 - a\varphi_{\alpha,\ 1}(\mathrm{rad}(a))^2)R = (\varphi_{\alpha,\ 0}(\mathrm{rad}(b))^2 - b\varphi_{\alpha,\ 1}(\mathrm{rad}(b))^2)R$$

and concludes the assertion. □

Remark 8. Assume that R contains a field whose characteristic is other than 2. Then the quadratic expression $\alpha^2 - b\alpha + c$ of α can be written of the from

$$\alpha^2 - b\alpha + c = (\alpha - \frac{1}{2}b)^2 + c - \frac{1}{4}b^2.$$

Note that $R[\alpha] = R[\alpha - \frac{1}{2}b]$. We will replace $\alpha - \frac{1}{2}b$ by α and set $a = c - \frac{1}{4}b^2$. We can get the same results as above for quadratic expressions under the following assertions.

(1) rad $(a) \notin K$.

(2) α is a super-primitive element of degree $d \geq 2$ over R (cf. [4, Proposition 1.12]).

(3) $[K(\mathrm{rad}\ (a))(\alpha)\ :\ K(\mathrm{rad}\ (a))] = d$.

We will proceed to the Laurent extensions $R[\alpha,\ \alpha^{-1}]$.

Proposition 9. *Let R be an integral domain and α an anti-integral element of degree d over R. Let a be an element of R. Then the following are equivalent to each other.*

(i) *$\alpha - a$ is a unit of $R[\alpha,\ \alpha^{-1}]$.*

(ii) *$a \in \mathrm{rad}(I_{[\alpha]}\varphi_\alpha(a))$.*

Proof. (i) $\Longrightarrow$ (ii). Since $\alpha-a$ is a unit of $R[\alpha,\ \alpha^{-1}]$, there exist an element $g(X)$ of $R[X]$ and a positive integer m such that $(\alpha-a)g(\alpha)a^{-m}=1$. Then $X^m-(X-a)g(X)\in \mathrm{Ker}\ \pi$. Hence $X^m-(X-a)g(X)\in I_{[\alpha]}\varphi_\alpha(X)R[X]$ because α is an anti-integral element of degree d over R. Then there exists an element $h(X)$ of $I_{[\alpha]}R[X]$ such that $X^m-(X-a)g(X)=\varphi_\alpha(X)h(X)$. Substituting a for X, we have $a^m=\varphi_\alpha(a)h(a)$ and $h(a)\in I_{[\alpha]}$. This implies that a is in rad $(I_{[\alpha]}\varphi_\alpha(a))$.

(ii) $\Longrightarrow$ (i). We will prove that there exists an element $g(X)$ of $R[X]$ and a positive integer m sucht that $(\alpha-a)g(X)\alpha^{-m}=1$. Set $A=R[\alpha]$. Then we have only to prove that rad $((\alpha-a)A)\supset$ rad (αA). Let P be an element of Spec(A) satisfying $\alpha-a\in P$. By the condition (ii) there exist an element c of $I_{[\alpha]}$ and a positive integer n such that $a^n=c\varphi_\alpha(a)$. Write $\varphi_\alpha(X)$ as

$$\varphi_\alpha(X)=(X-a)^d+\lambda_1(x-a)^{d-1}+\cdots+\lambda_d, \qquad (\lambda_1,\ \cdots,\ \lambda_d\in K).$$

Then $\lambda_1,\ \cdots,\ \lambda_d$ are in $(1,\ \eta_1,\ \cdots,\ \eta_d)$ and $\lambda_d=\varphi_\alpha(a)$. Set $c_i=c\lambda_i$ for $1\le i\le d$. Then $c_1,\ \cdots,\ c_d$ are in R and

$$c(\alpha-a)^d+c_1(\alpha-a)^{d-1}+\ \cdots\ +\ c_{d-1}(\alpha-a)+\ c\varphi_\alpha(a)=0.$$

Therefore $a^n=c\varphi_\alpha(a)$ is in P because $\alpha-a$ is in P. This shows that rad$((\alpha-a)A)\supset$ rad (aA). □

Corollary 10. *Let R be a Noetherian domain and α an anti-integral element of degree d over R. Let a be an element of R. Then $a\alpha-1$ is a unit of $R[\alpha,\ \alpha^{-1}]$ if and only if a is in* rad $(I_{[\alpha^{-1}]}\ \varphi_{\alpha^{-1}}(a))$.

Proof. Note that α is an anti-integral element of degree d over R if and only if so is α^{-1} by [2, Theorem 6]. Also note that $a\alpha-1$ is a unit of $R[\alpha,\ \alpha^{-1}]$ if and only if $\alpha^{-1}-a$ is a unit of $R[\alpha,\ \alpha^{-1}]$. It is immediate from Proposition 9. □

We will give a criterion for a linear form of α to be a unit of $R[\alpha,\ \alpha^{-1}]$.

Theorem 11. *Let R be a Noetherian domain and α an anti-integral element of degree d over R. Let a and b be elements of R. Assume that*

(1) *$R[\alpha]/R$ is a flat extension.*

(2) grade $(a,\ b)R\le 1$.

Then the following are equivalent to each other.

(i) *$a\alpha-b$ is a unit of $R[\alpha,\ \alpha^{-1}]$.*

(ii) *Let p be an element of* $\mathrm{Dp}_1(\mathrm{R})$.

If $a\notin p$, then b/a is in rad $(I_{[\alpha]}\varphi_\alpha(b/a)R_p)$.

If $b\notin p$, then a/b is in rad $(I_{[\alpha^{-1}]}\varphi_{\alpha^{-1}}(a/b)R_p)$.

Proof. (i) $\Longrightarrow$ (ii). If a is not in p, then $\alpha-b/a$ is a unit of $R_p[\alpha,\ \alpha^{-1}]$. Hence b/a is in rad $(I_{[\alpha]}\varphi_\alpha(b/a)R_p)$ by Proposition 9. If b is not in p, then $(a/b)\alpha-1$ is a unit of $R_p[\alpha,\ \alpha^{-1}]$. Therefore a/b is in rad $I_{[\alpha^{-1}]}\varphi_{\alpha^{-1}}(a/b)R_p$ by Corollary 10.

(ii) $\Longrightarrow$ (i). Set $A=R[\alpha]$ and $C=R[\alpha,\ \alpha^{-1}]$. Since $C=\cap_{P\in \mathrm{Dp}_1(C)}\ C_P$, it sufficies to prove that $(a\alpha-b)^{-1}$ is in C_P for $P\in \mathrm{Dp}_1(C)$. Set $p=P\cap R$. Then depth $R_p=1$ because C/A and A/R are flat extensions. We will prove that $a\alpha-b$ is a unit of $R_p[\alpha,\ \alpha^{-1}]$. Since grade $(a,\ b)R>1$, we see that a is not in p or b is not in p. If a is not in p, then by the condition (ii) we have $b/a\in$ rad $(I_{[\alpha]}\varphi_\alpha(b/a)R_p)$. Hence Proposition 9 asserts that $\alpha-b/a$

is a unit of $R_p[\alpha,\ \alpha^{-1}]$. So $a\alpha - b$ is a unit of $R_p[\alpha,\ \alpha^{-1}]$ because a is a unit of R_p. If b is not in p, then $(a/b)\alpha - 1$ is a unit of $R_p[\alpha,\ \alpha^{-1}]$ by the condition (ii) and Corollary 10. Hence $a\alpha - b$ is also a unit of $R_p[\alpha,\ \alpha^{-1}]$. This shows that $(a\alpha - 1)^{-1}$ is in $R_p[\alpha,\ \alpha^{-1}] \subset C_P$. □

References

[1] K. Baba, S. Oda and K.Yoshida, Anti-inetgral extensions and co-monic elements, *to appear.*

[2] M. Kanemitsu and K. Yoshida, Some properties of extensions $R[\alpha] \cap R[\alpha^{-1}]$ over Noetherian domains R, *Communications in Algebra*, **23** No. 12 (1995), 4501-4507.

[3] H. Matsumura, *Commutative Algebra* (2nd ed.), Benjamin, New York, 1980.

[4] S. Oda, J. Sato and K. Yoshida, High degree anti-integral extensions of Noetherian domains, *Osaka J. Math.*, **30** (1993), 119-135.

Mitsuo Kanemitsu
Department of Mathematics
Aichi University of Education
Igaya-cho, Kariya-shi, 448-8542, JAPAN
e-mail:mkanemit@auecc.aichi-edu.ac.jp

Kiyoshi Baba
Department of Mathematics
Faculty of Education and Welfare Science
Oita University
Oita 870-1192, JAPAN

and

Ken-ichi Yoshida
Department of Applied Mathematics
Okayama University of Science
Ridai-cho 1-1, Okayama 700-0005, JAPAN.