Toyama Math. J.
Vol. 31(2008), 59-67

Accuracy of powers of accurate elements

Nobuharu Onoda and Takasi Sugatani

Abstract. Let R be an integral domain with quotient field K and α an element of the algebraic closure of K. We show that (i) if α is accurate over R and satisfies the monic minimal polynomial $X^d - \eta$ over K, then α^n is accurate over R for any integer n; and (ii) if α is super-primitive over R, then α^n is super-primitive over R for every positive integer n such that $K(\alpha) = K(\alpha^n)$.

1. Introduction

Let R be an integral domain with quotient field K and let L be the algebraic closure of K. For an element $\alpha \in L$ we denote by $\varphi_\alpha(X)$ the monic minimal polynomial of α over K. Let $\Phi_\alpha: R[X] \to R[\alpha]$ be the natural R-algebra homomorphism sending X to α. Then we say that α is *accurate* (synonymously anti-integral) over R if $\ker \Phi_\alpha = I_{R,[\alpha]}\varphi_\alpha(X)R[X]$, where $I_{R,[\alpha]} = R[X] :_R \varphi_\alpha(X)$. Write

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

Let $R(\alpha) = R[\alpha] \cap R[\alpha^{-1}]$ and $R\langle\alpha\rangle = R \oplus I_{R,[\alpha]}\zeta_1 \oplus \cdots \oplus I_{R,[\alpha]}\zeta_{d-1}$, where

$$\zeta_i = \alpha^i + \eta_1\alpha^{i-1} + \cdots + \eta_i$$

for $i = 1, \ldots, d-1$.

It is known that (i) $R\langle\alpha\rangle$ is a subring of $R(\alpha)$ [6, Section 4 and Remark 5.1]; (ii) α is accurate over R if and only if $R\langle\alpha\rangle = R(\alpha)$ [6, Theorem

2000 *Mathematics Subject Classification.* Primary 13B02; Secondary 13G05.
Key words and phrases. accurate element, super-primitive element.

4.6 and Remark 5.1]; and (iii) α is accurate over R if and only if for any $g(X) \in \ker \Phi_\alpha$, the leading coefficient of $g(X)$ is in $I_{R,[\alpha]}$ [6, Lemma 2.2]. In particular, if $d = 1$, i.e., $\alpha \in K$, then α is accurate over R if and only if $R(\alpha) = R$ [1, Theorem 2.5]. From this it follows that if R is integrally closed, then every $\alpha \in K$ is accurate over R ([2, (11.13)] and [7, Corollary 7]). Moreover we know ([1, Theorem 3.3] and [5, Theorem 3.3]) that R is integrally closed if and only if every $\alpha \in K$ is accurate over R if and only if every $\alpha \in L$ is accurate over R.

Using [1, Theorem 2.5] above one can easily prove that if $\alpha \in K$ is accurate over R, then so is α^n for every integer n (cf. Lemma 2.1). In view of this it is natural to ask whether we can generalize this result to the case where $d > 1$. In section 2, we will prove that the answer is affirmative if $\varphi_\alpha(X)$ is of the form $\varphi_\alpha(X) = X^d - \eta$ with $\eta \in K$. In section 3, we will turn to super-primitive elements (for the definition, see below) and will show that if α is super-primitive over R, then α^n is super-primitive over R for every positive integer n such that $K(\alpha) = K(\alpha^n)$.

Let $J_{R,[\alpha]}$ be the ideal of R defined by

$$J_{R,[\alpha]} = I_{R,[\alpha]}(1, \eta_1, \eta_2, \ldots, \eta_d).$$

After [8], we put

$$T(R) = \{P \in \mathrm{Spec}(R) \mid P \text{ is minimal over } I_{R,[\beta]} \text{ for some } \beta \in K\}.$$

It is shown [4, Proposition 6] that for $P \in T(R)$, $\mathrm{grade}(P) = 1$ holds. Also, note that if R is Noetherian, then by considering a primary decomposition of a principal ideal, one sees $T(R) = \{P \in \mathrm{Spec}(R) \mid \operatorname{depth} R_P = 1\}$.

An element $\alpha \in L$ is called *super-primitive* over R if $J_{R,[\alpha]} \not\subset P$ for any $P \in T(R)$. It is known [6, Theorem 5.5] that if α is super-primitive over R, then α is accurate over R. The converse *does* hold if R is Noetherian and satisfies S_2-condition [3, Proposition 4]. However in general this is not the case even if R is an integrally closed 1-dimensional quasilocal domain : Let F be a field and s, t be indeterminates. Consider the valuation domain $V = F(s)[[t]]$. Now let $R = F + tV$. Then [2, (11.13)] implies that s is accurate over R, since R is integrally closed. Now observe that tV is the conductor from V to R. It then follows that s is not super-primitive over R. For such examples of Noetherian case, see [6, Example 5.12].

Throughout this paper we keep the above notation and assumptions.

2. Powers of accurate elements

Our first result includes a bit more about the powers of an accurate element, mentioned above.

Lemma 2.1. *Suppose that $d = 1$, i.e., $\alpha \in K$. If α is accurate over R and $f(X)$ is a monic polynomial in $R[X]$, then $f(\alpha)$ is accurate over R.*

Proof. Let $\beta = f(\alpha)$. It suffices to show that if c is the leading coefficient of some polynomial $g(X)$ such that $g(X) \in \ker \Phi_\beta$, then $c \in I_{R,[\beta]}$ by [6, Lemma 2.2]. Let $n = \deg f(X)$ and write $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$. We will show that $c\alpha^i \in R$ for every i with $1 \leq i \leq n$; if this is the case, then $c\beta = cf(\alpha) \in R$, as desired. We use induction on i. Let $h(X) = g(f(X))$. Then $h(\alpha) = g(\beta) = 0$, and hence $h(X) \in \ker \Phi_\alpha$. Note that c is the leading coefficient of $h(X)$ because $f(X)$ is monic. Since α is accurate over R, it thus follows from [6, Lemma 2.2] that $c \in I_{R,[\alpha]}$. Hence $c\alpha \in R$, and the assertion holds when $i = 1$.

Suppose that $c\alpha^j \in R$ for $j = 1, \ldots, i$ with $i < n$. Then we have

$$c\beta = cf(\alpha) = c'\alpha^{n-i} + c'a_1\alpha^{n-i-1} + \cdots + c'a_{n-i-1}\alpha + b,$$

where $c' = c\alpha^i \in R$ and $b = c(a_{n-i}\alpha^i + a_{n-i+1}\alpha^{i-1} + \cdots + a_n) \in R$. Let

$$u(X) = c'X^{n-i} + c'a_1X^{n-i-1} + \cdots + c'a_{n-i-1}X + b$$

and write $g(X) = cX^m + g_1(X)$, where $m = \deg g(X)$ and $\deg g_1(X) < m$. Set

$$h_1(X) = u(X)(f(X))^{m-1} + g_1(f(X)).$$

Then

$$h_1(\alpha) = u(\alpha)\beta^{m-1} + g_1(\beta) = c\beta^m + g_1(\beta) = g(\beta) = 0,$$

because $u(\alpha) = cf(\alpha) = c\beta$. Thus $h_1(X) \in \ker \Phi_\alpha$. Since

$$\deg u(X)(f(X))^{m-1} = (n - i) + n(m - 1) > \deg g_1(f(X)),$$

c' is the leading coefficient of $h_1(X)$. Thus $c' \in I_{R,[\alpha]}$ by [6, Lemma 2.2], so that $c\alpha^{i+1} = c'\alpha \in R$. This completes the proof. □

From this line to the end of this section, we assume that $\varphi_\alpha(X)$ is of the form $\varphi_\alpha(X) = X^d - \eta$ with $\eta \in K$. Note that in this case $I_{R,[\alpha]} = R :_R \eta$. Note also that $\zeta_i = \alpha^i$ for each i, so that

$$R\langle\alpha\rangle = R \oplus I_{R,[\alpha]}\alpha \oplus I_{R,[\alpha]}\alpha^2 \oplus \cdots \oplus I_{R,[\alpha]}\alpha^{d-1}. \tag{2.1}$$

Lemma 2.2. *α is accurate over R if and only if η is accurate over R.*

Proof. First suppose that α is accurate over R. Then $R(\alpha) = R\langle\alpha\rangle$ by [6, Theorem 4.6]. Note that $R(\eta) \subset R(\alpha)$ because $\eta = \alpha^d$. Hence, from the equation (2.1), we have

$$R(\eta) \subset R \oplus I_{R,[\alpha]}\alpha \oplus I_{R,[\alpha]}\alpha^2 \oplus \cdots \oplus I_{R,[\alpha]}\alpha^{d-1},$$

which implies $R(\eta) = R$, because $R(\eta) \subset K$. Therefore η is accurate over R by [1, Theorem 2.5].

Conversely suppose that η is accurate over R. Then $R(\eta) = R$ by [1, Theorem 2.5]. Since $\alpha^d = \eta$, we have

$$R[\alpha] = R[\eta] + R[\eta]\alpha + \cdots + R[\eta]\alpha^{d-1}$$

and

$$R[\alpha^{-1}] = R[\eta^{-1}] + R[\eta^{-1}]\alpha^{-1} + \cdots + R[\eta^{-1}]\alpha^{-(d-1)}.$$

Hence, for an element $\theta \in R(\alpha)$, we can write

$$\begin{aligned} \theta &= f_0 + f_1\alpha + \cdots + f_{d-1}\alpha^{d-1} \\ &= g_0 + g_1\alpha^{-1} + \cdots + g_{d-1}\alpha^{-(d-1)} \end{aligned}$$

for some $f_0, \ldots, f_{d-1} \in R[\eta]$ and $g_0, \ldots, g_{d-1} \in R[\eta^{-1}]$. From this it follows that

$$f_0\alpha^{d-1} + f_1\eta + f_2\eta\alpha + \cdots + f_{d-1}\eta\alpha^{d-2} = g_0\alpha^{d-1} + g_1\alpha^{d-2} + \cdots + g_{d-1},$$

which implies $f_0 = g_0$ and $f_i = g_{d-i}\eta^{-1}$ for $i \geq 1$. Thus

$$f_i \in R[\eta] \cap R[\eta^{-1}] = R(\eta) = R,$$

for each $i = 0, \ldots, d-1$. Moreover for $i \geq 1$ we have

$$f_i \eta = g_{d-i} \in R(\eta) = R,$$

which means $f_i \in R :_R \eta = I_{R,[\alpha]}$. Hence

$$\theta \in R + I_{R,[\alpha]}\alpha + \cdots + I_{R,[\alpha]}\alpha^{d-1} = R\langle\alpha\rangle,$$

and therefore $R(\alpha) \subset R\langle\alpha\rangle$. Since $R\langle\alpha\rangle \subset R(\alpha)$ in general, we have $R(\alpha) = R\langle\alpha\rangle$. Thus α is accurate over R by [6, Theorem 4.6]. $\square$

Lemma 2.3. *Let n be a positive integer and let $\beta = \alpha^n$. Then, setting $m = \gcd\{d, n\}$, we have $\varphi_\beta(X) = X^{d/m} - \eta^{n/m}$.*

Proof. Let $f(X) = X^{d/m} - \eta^{n/m}$. Then $f(\beta) = 0$, so that

$$[K(\beta) : K] \leq d/m. \tag{2.2}$$

On the other hand, for integers r, s with $rd + sn = m$, we have $\alpha^m = \alpha^{rd+sn} = \eta^r\beta^s \in K(\beta)$, which implies

$$[K(\alpha) : K(\beta)] \leq m. \tag{2.3}$$

It follows from (2.2) and (2.3) that

$$d = [K(\alpha) : K] = [K(\alpha) : K(\beta)][K(\beta) : K] \leq m(d/m) = d,$$

so that the equalities must hold both in (2.2) and (2.3). Therefore $f(X) = \varphi_\beta(X)$. $\square$

Theorem 2.4. *Let R be an integral domain with quotient field K and let α be an element of the algebraic closure of K such that $\varphi_\alpha(X)$, the minimal polynomial of α over K, is of the form $\varphi_\alpha(X) = X^d - \eta$ with $\eta \in K$. If α is accurate over R, then α^n is accurate over R for every integer n.*

Proof. By [6, Theorem 4.6], we may assume that n is positive. Suppose that α is accurate over R. Then η is accurate over R by Lemma 2.2. Hence $\eta^{n/m}$ is also accurate over R by Lemma 2.1, where $m = \gcd\{d, n\}$. Therefore, by Lemmas 2.2 and 2.3, we know that α^n is accurate over R. This completes the proof. $\square$

3. Powers of super-primitive elements

Lemma 3.1. *Let $t_1, \dots, t_d$ be indeterminates, and n a positive integer. For each $i = 1, \dots, d$, let s_i be the i-th elementary symmetric polynomial of $t_1, \dots, t_d$ and u_i the i-th elementary symmetric polynomial of $t_1^n, \dots, t_d^n$. Then we can write*

$$u_i = s_i^n + \sum c_{i_1 \cdots i_r} s_{i_1}^{j_1} \cdots s_{i_r}^{j_r}, \tag{3.1}$$

where $c_{i_1 \cdots i_r} \in \mathbb{Z}$, $j_1 > 0, \dots, j_r > 0$, $i_1 j_1 + \cdots + i_r j_r = in$, $j_1 + \cdots + j_r \le n$, $(i_1, \dots i_r) \ne (i, \dots, i)$ and $\max\{i_1, \dots, i_r\} > i$.

Proof. Since u_i is a symmetric polynomial of $t_1, \dots, t_d$, there exists a polynomial $F(X_1, \dots, X_d) \in \mathbb{Z}[X_1, \dots, X_d]$ such that $u_i = F(s_1, \dots, s_d)$. Let m be the total degree of $F(X_1, \dots, X_d)$. We will show that $m = n$. Let $F_m(X_1, \dots, X_d)$ be the leading form of F. Note that

$$s_i = s'_{i-1} t_d + s'_i \tag{3.2}$$

for $i = 1, \dots, d$, where s'_i is the i-th elementary symmetric polynomial of $t_1, \dots, t_{d-1}$ with $s'_0 = 1$ and $s'_d = 0$. Hence we can write

$$u_i = F(s_1, \dots, s_d) = F_m(1, s'_1, \dots, s'_{d-1}) t_d^m + H, \tag{3.3}$$

where H is a polynomial in $t_1, \dots, t_d$ over $\mathbb{Z}$ with $\deg_{t_d} H < m$. Since $\deg_{t_d} u_i = n$, it thus follows from (3.3) that $m \ge n$. If $m > n$, then $F_m(1, s'_1, \dots, s'_{d-1}) = 0$ again by (3.3), which implies $F_m(1, X_2, \dots, X_d) = 0$ because $s'_1, \dots, s'_{d-1}$ are algebraically independent over $\mathbb{Z}$. This means $F_m(X_1, \dots, X_d)$ is divisible by $X_1 - 1$, so that $F_m(X_1, \dots, X_d) = 0$ because $F_m(X_1, \dots, X_d)$ is homogeneous. This is a contradiction. We have thus proved $m = n$. On the other hand, u_i is a homogeneous polynomial in $t_1, \dots, t_d$ of degree in. Therefore we can write

$$u_i = c s_i^n + \sum c_{i_1 \cdots i_r} s_{i_1}^{j_1} \cdots s_{i_r}^{j_r}, \tag{3.4}$$

where $i_1 j_1 + \cdots + i_r j_r = in$, $j_1 + \cdots + j_r \le n$, $(i_1, \dots i_r) \ne (i, \dots, i)$ and $c, c_{i_1 \cdots i_r} \in \mathbb{Z}$. Let $i_k = \max\{i_1, \dots, i_r\}$. If $i_k \le i$, then

$$in = i_1 j_1 + \cdots + i_r j_r \le i(j_1 + \cdots + j_r) \le in,$$

and so

$$(i_1, \ldots, i_r) = (i, \ldots, i),$$

a contradiction. Thus $i_k > i$. Substituting $t_d = 0$ in (3.4) and using (3.2), we have an equality corresponding to (3.4) for the case of $d-1$ indeterminates $t_1, \ldots, t_{d-1}$. It now follows $c = 1$ by induction on d. □

Lemma 3.2. *Suppose that R is a quasilocal ring with maximal ideal P, and let n be a positive integer satisfying $K(\alpha) = K(\beta)$, where $\beta = \alpha^n$. If $J_{R,[\alpha]} = R$, then $J_{R,[\beta]} = R$.*

Proof. First we show that we may assume that α is separable over K. Let p be the characteristic of K and let p^e be the minimal integer such that $\alpha' := \alpha^{p^e}$ is separable over K. Then $\varphi_\alpha(X) \in K[X^{p^e}]$ and $\varphi_{\alpha'}(X) = \varphi_\alpha(X^{1/p^e})$. In particular we have $I_{R,[\alpha]} = I_{R,[\alpha']}$ and $J_{R,[\alpha]} = J_{R,[\alpha']}$. On the other hand, since $K(\alpha) = K(\beta)$, it follows that $K(\alpha') = K(\beta')$, where $\beta' = \beta^{p^e}$. Thus $\deg \varphi_{\alpha'}(X) = \deg \varphi_{\beta'}(X)$. Let $\psi(X) = \varphi_{\beta'}(X^{p^e})$. Then $\psi(\beta) = 0$, so that $\psi(X) = \varphi_\beta(X)$, because $\deg \psi(X) = p^e \deg \varphi_{\beta'}(X) = d$. From this we have $I_{R,[\beta]} = I_{R,[\beta']}$ and $J_{R,[\beta]} = J_{R,[\beta']}$. Since $\beta' = \alpha'^n$, replacing α by α', we may assume that α is separable over K.

Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ be the conjugates of α over K and write

$$\varphi_\beta(X) = X^d + \xi_1 X^{d-1} + \cdots + \xi_d.$$

Then $\alpha_1^n = \beta, \alpha_2^n, \ldots, \alpha_d^n$ are the conjugates of β over K. In fact if γ is a conjugate of β, then we have a K-isomorphism $\sigma : K(\beta) \to K(\gamma)$. But $K(\beta) = K(\alpha)$, and so $\gamma = \sigma(\alpha)^n$. Hence ξ_i is the i-th elementary symmetric polynomial of $\alpha_1^n, \ldots, \alpha_d^n$. It then follows from Lemma 3.1 that

$$\xi_i = \eta_i^n + \sum c_{i_1 \cdots i_r} \eta_{i_1}^{j_1} \cdots \eta_{i_r}^{j_r}, \tag{3.5}$$

where $c_{i_1 \cdots i_r} \in$ the prime ring of R , $i_1 j_1 + \cdots + i_r j_r = in$, $j_1 + \cdots + j_r \le n$, $(i_1, \ldots i_r) \ne (i, \ldots, i)$ and $\max\{i_1, \ldots, i_r\} > i$. It thus follows that $I_{R,[\alpha]}^n \subset I_{R,[\beta]}$. Now, since

$$J_{R,[\alpha]} = I_{R,[\alpha]} + I_{R,[\alpha]}\eta_1 + \cdots + I_{R,[\alpha]}\eta_d = R$$

and R is quasilocal, setting $\eta_0 = 1$, we have $I_{R,[\alpha]}\eta_j = R$ for some j. Let i be the maximal integer satisfying $I_{R,[\alpha]}\eta_i = R$. Thus $I_{R,[\alpha]}\eta_i = R$ and $I_{R,[\alpha]}\eta_j \subset P$ for $j > i$. It then follows that

$$I^n_{R,[\alpha]}\eta^{j_1}_{i_1} \cdots \eta^{j_r}_{i_r} \subset P,$$

because $\max\{i_1, \ldots, i_r\} > i$. Since $I^n_{R,[\alpha]}\eta^n_i = R$, from (3.5) it follows that $I^n_{R,[\alpha]}\xi_i = R$. Hence $I_{R,[\beta]}\xi_i = R$, which implies $J_{R,[\beta]} = R$. This completes the proof. □

Theorem 3.3. *Let R be an integral domain with quotient field K and let α be an element of the algebraic closure of K. Suppose that α is super-primitive over R. Then α^n is super-primitive over R for every positive integer n such that $K(\alpha) = K(\alpha^n)$.*

Proof. Note that α is super-primitive over R if and only if $J_{R,[\alpha]}R_P = R_P$ for every $P \in T(R)$. Note also that $I_{R,[\alpha]}R_P = I_{R_P,[\alpha]}$ since $I_{R,[\alpha]} = R :_R (\eta_1, \ldots, \eta_d)$, so that $J_{R,[\alpha]}R_P = J_{R_P,[\alpha]}$. Now let n be a positive integer such that $K(\alpha) = K(\alpha^n)$, and set $\beta = \alpha^n$. Then, for $P \in T(R)$, we have $J_{R_P,[\alpha]} = R_P$, and hence $J_{R_P,[\beta]} = R_P$ by Lemma 3.2. Thus $J_{R,[\beta]} \not\subset P$ for any $P \in T(R)$, which implies that β is super-primitive over R. This completes the proof. □

References

[1] A. Mirbagheri and L. J. Ratliff, Jr., On the intersection of two over-rings, *Houston J. Math.*, 8(1982), 525-535.

[2] M. Nagata, *Local rings*, Interscience Tracts, no. 13, Interscience Publ., New York, 1962.

[3] N. Onoda, T. Sugatani and K. Yoshida, Note on LCM-stability of simple extensions of Noetherian domains, *Math. J. Toyama Univ.*, 21(1998), 111-115.

[4] N. Onoda, T. Sugatani and K. Yoshida, Some remarks on Richman simple extensions of an integral domain, *Comm. Algebra*, 29(2001), 2013-2019.

[5] N. Onoda and T. Sugatani, A remark on Noetherian property of certain type of algebras, *Arab. J. Sci. Eng. Sect. C Theme Issues*, 26(2001), 161-169.

[6] N. Onoda, T. Sugatani and K. Yoshida, Accurate elements and super-primitive elements over rings, *J. Algebra*, 245(2001), 370-394.

[7] L. J. Ratliff, Jr., Conditions for Ker($R[X] \to R[c/b]$) to have a linear base, *Proc. Amer. Math. Soc.*, 39(1973), 509-514.

[8] H. T. Tang, Gauss' lemma, *Proc. Amer. Math. Soc.*, 35(1972), 372-376.

Nobuharu Onoda
Department of Mathematics
University of Fukui
Fukui 910-8507, JAPAN
e-mail: onoda@apphy.fukui-u.ac.jp

Takasi Sugatani
Department of Mathematics
University of Toyama
Toyama, 930-8555, JAPAN
e-mail: sugatani@sci.u-toyama.ac.jp

(Received September 29, 2008)