manuscripta
mathematica
© Springer-Verlag 1990

NONSTANDARD ARITHMETIC OF ITERATED POLYNOMIALS

MASAHIRO YASUMOTO

Let K be an algebraic number field of finite degree and $f(X,T)$ a polynomial over K. For each $\varphi(X) \in \mathbf{Z}[X]$, we denote by $E(\varphi)$ the set of all integers a with $\varphi^m(a) = \varphi^n(a)$ for some $m \neq n$. In this paper, we give a condition for a polynomial $\varphi(X) \in \mathbf{Z}[X]$ to satisfy the following; If for $n \in N$, there exist $r \in K$ and $a \in \mathbf{Z} - E(\varphi)$ such that $f(r, \varphi^n(a)) = 0$, then there exists a rational function $g(X)$ over K and $k \in \mathbf{N}$ such that $f(g(T), \varphi^k(T)) = 0$.

1. Introduction

Let $\varphi(X)$ be a polynomial with integer coefficientsand a an integer. In this paper, we are concerned with the sequence of integers,

$$a, \varphi(a), \varphi(\varphi(a)), \varphi(\varphi(\varphi(a))), \dots, \varphi^n(a), \dots \quad (n \in \mathbf{N}).$$

Let $\varphi(X) = X + k$ where k is an integer, then the sequence $\varphi^n(a) = nk+a$ $(n \in \mathbf{N})$ is an arithmetical progression. In this case, the following theorem is known.([1],[6],[7])

THEOREM. *Let K be an algebraic number field of finite degree and $f(X, T_1, \dots, T_m)$ be a polynomial over K. If for every m arithmetical progressions P_i $(1 \leq i \leq m)$ of integers, there exist integers $t_i \in P_i$ $(1 \leq i \leq m)$ and an $r \in K$ such that*

$$f(r, t_1, \dots, t_m) = 0,$$

then there exists a rational function $g(T_1, \ldots, T_m)$ *over* K *such that*

$$f(g(T_1, \ldots, T_m), T_1, \ldots, T_m) = 0.$$

If $\varphi(X) = cX$, then the sequence $\varphi^n(a) = ac^n$ $(n \in \mathbf{N})$ is a geometrical progression. In the previous paper [8], we proved the following theorem by using iterated enlargements.

THEOREM. *Let* K *be an algebraic number field of finite degree and* $f(X, T_1, \ldots, T_m)$ *be a polynomial over* K. *Assume there exist* $c_1, \ldots, c_m \in K$ *other than* 0 *and roots of unity such that for any* m *integers* $n_1, \ldots, n_m$, *there exists an* $r \in K$ *with*

$$f(r, c_1^{n_1}, \ldots, c_m^{n_m}) = 0.$$

Then there exists a rational function $g(T_1, \ldots, T_m)$ *over* K *and* m *integers* $k_1, \ldots, k_m$ *not more than* d *such that*

$$f(g(T_1, \ldots, T_m), T_1^{k_1}, \ldots, T_m^{k_m}) = 0$$

where d *is the* X*-degree of* $f(X, T_1, \ldots, T_m)$.

Next we consider a polynomial $\varphi(X)$ of degree at least 2 which does not satisfy the following condition.

(I) *There exist polynomials* $\psi(X), \Phi(X)$ *and* $\Psi(X)$ *over* K *such that* g.c.d.$(\deg(\varphi), \deg(\psi)) = 1$, $\deg(\psi) \geq 2$ *and* $\varphi(\Phi(X)) = \psi(\Psi(X))$.

Polynomials satisfying the condition (I) are characterized by Ritt[4] and Fried[2, Theorem 3]. Our purpose of this paper is to prove the the following theorem similar to above theorems.

THEOREM 1. *Let* $f(X, T)$ *be a polynomial over an algebraic number field* K *of finite degree. Assume that* $\varphi(X) = cX^d + h(X) \in \mathbf{Z}[X]$ *is a polynomial of degree at least* 3 *which does not satisfy the condition* (I) *where* $\deg(h) \leq d - 3$ *and* $c \neq 0$. *If for any* $n \in \mathbf{N}$, *there exists an* $a \in \mathbf{Z} - E(\varphi)$ *and* $r \in K$ *such that*

$$f(r, \varphi^n(a)) = 0,$$

then there exist a rational function $g(T)$ *over* K *and* $k \in \mathbf{N}$ *such that*

$$f(g(T), \varphi^k(T)) = 0.$$

In Theorem 1, the assumption that $\varphi(X)$ does not satisfy the condition (I) cannot be eliminated. For example, let us consider $\varphi(X) = X^3$ and $f(X,T) = X^2 - T$. Then $\varphi(X^2) = X^6 = \varphi(X)^2$ satisfies the condition (I). On the other hand, for any $n \in \mathbf{N}$, $f(a^{3^n}, \varphi^n(a^2)) = (a^{3^n})^2 - (a^2)^{3^n} = 0$. But for any $k \in \mathbf{N}$, there is no rational function $g(X)$ such that $f(g(X), \varphi^k(X)) = g(X)^2 - X^{3^k} = 0$. We will prove Theorem 1 by using nonstandard method and no proof of Theorem 1 without nonstandard method is known. It is also not known wether Theorem 1 can be generalized for polynomials $f(X, T_1, \dots, T_m)$ of many variables.

2. Proof of Theorem 1

Let $^*K$ be an enlargement of an algebraic number field K of finite degree and $t \in {}^*K - K$. We assume the reader is familiar with nonstandard arithmetic(c.f.[5]). Let Ω_t denote the algebraic closure of $K(t)$ within $^*K$. First we state a proposition which will be proved later and show how Theorem 1 follows from it.

PROPOSITION 1. *Let $\varphi(X)$ be as in Theorem 1. Then for every $s \in {}^*\mathbf{N} - \mathbf{N}$ and every $a \notin E(\varphi)$,*

$$\Omega_{\varphi^s(a)} = \bigcup_{i \in \mathbf{N}} K(\varphi^{s-i}(a)).$$

[*Proof of Theorem 1*] By the assumption of Theorem 1, there exists $s \in {}^*\mathbf{N} - \mathbf{N}$, $a \in {}^*\mathbf{Z} - {}^*E(\varphi)$ and $x \in {}^*K$ such that

$$f(x, \varphi^s(a)) = 0.$$

By Proposition 1, $x \in K(\varphi^{s-k}(a))$ for some $k \in \mathbf{N}$. Let $g(X)$ be a rational function over K with $x = g(\varphi^{s-k}(a))$. Then

$$f(g(\varphi^{s-k}(a)), \varphi^k(\varphi^{s-k}(a))) = 0.$$

Since $s - k \in {}^*\mathbf{N} - \mathbf{N}$ and $a \notin E(\varphi)$, then $\varphi^{s-k}(a) \in {}^*\mathbf{Z} - \mathbf{Z}$, hence $\varphi^{s-k}(a)$ is transcendental over K, therefore

$$f(g(T), \varphi^k(T)) = 0$$

as contended.

3. Algebraic extensions in $^*K$

Now we turn to the proof of Proposition 1. In the following, we assume as in Theorem 1 that $\varphi(X) = cX^d + h(X) \in \mathbf{Z}[X]$ is a polynomial of degree at least 3 which does not satisfy the condition (I) where $\deg(h) \leq d-3$ and $c \neq 0$. First let us recall the nonstandard proof of the theorem of Siegel and Mahler.([5]) A prime divisor of K is defined to be an equivalence class of nontrivial valuations of K. Let V be the set of all prime divisors of K and $^*V$ its enlargement. An element $\mathfrak{p} \in^* V$ is called an arithmetical prime. Let F be an algebraic function field of one variable over K which is included in $^*K$. By a functional prime P, we mean an equivalence class of nontrivial valuations of F which is trivial on K. A functional prime P is called exceptional if there exists an $x \in F \subset {}^*K$ such that P is a pole of x and x admits standard arithmetical primes only in its denominator. For example, let x be a nonstandard algebraic integer. Then x admits archimedean primes only in its denominator. Since the set of all archimedean primes in V is finite, it is not enlarged, in other words, every archimedean prime in $^*V$ is standard. Therefore every functional prime which is a pole of x is exceptional. In their paper[5], A. Robinson and P. Roquette proved the following nonstandard equivalent of the theorem of Siegel and Mahler.

THEOREM 2 ([5, Theorem 1.1,5.4 and Remark 5.6]). *Assume that there is a nonstandard $x \in F$ which admits standard primes only in its denominator. Then F is a rational function field. If P_i $(1 \leq i \leq m)$ are distinct exceptional functional primes, then*

$$\sum_{i=1}^{m} \deg(P_i) \leq 2.$$

The next lemma is easy to prove and has been proved in [10], so we omit its proof.

LEMMA 1 ([10, Lemma 2]). *Let Q (resp. R) be the polar prime (resp. the zero prime) of x in a rational function field $K(x)$. Let $t \in K(x)$.*
(1) If $[t]_\infty = dQ$ for some $d \in \mathbf{N}$, then $t = \psi(x)$ for some polynomial $\psi(X) \in K[X]$ of degree d where $[t]_\infty$ denotes the polar divisor of t.

(2) Let $d > m > 0$. If $[t]_\infty = mR + (d-m)Q$, then there is a polynomial $\psi(X) \in K[X]$ of degree d such that $t = \psi(x)/x^m$ and $\psi(0) \neq 0$.

The following well known theorem is used to prove Proposition 1.

THEOREM 3. *Let K be a field and let $\Phi(X)$ be a polynomial over K such that* $\text{g.c.d.}(\text{char}(K) = 0, \deg(\Phi(X))) = 1$ *or* $\text{char}(K){=}0$*. If L and M are fields intermediate between $K(X)$ and $K(\Phi(X))$, then*

$$[L \cap M : K(\Phi(X))] = \text{g.c.d.}([L : K(\Phi(X))] , [M : K(\Phi(X))]$$

and

$$[K(X) : L \cdot M] = \text{g.c.d.}([K(X) : L] , [K(X) : M]).$$

For the proof of Theorem 3, refer to [3, Theorem 3.6] or [7, Theorem 5].

[*Proof of Proposition 1*] Let $s \in {}^*\mathbf{N} - \mathbf{N}$ and $a \notin E(\varphi)$. Let $y \in {}^*K$ be algebraic over $K(\varphi^s(a))$. We are going to prove $y \in K(\varphi^{s-i}(a))$ for some $i \in \mathbf{N}$. Assume otherwise, then

$$[\bigcup_{i \in \mathbf{N}} K(y, \varphi^{s-i}(a)) : \bigcup_{i \in \mathbf{N}} K(\varphi^{s-i}(a))] > 1.$$

Let d_y be the left side of the above inequality and let $k \in \mathbf{N}$ be such that $d_y = [K(y, \varphi^{s-k}(a)) : K(\varphi^{s-k}(a)))]$. Let $t_i = \varphi^{s-k-i}(a)$ and let P_i be the polar prime of t_i in the rational function field $K(t_i)$. Since $\varphi(X)$ is a polynomial of degree d, we have $P_i = [t_i]_\infty = [\varphi(t_{i+1})]_\infty = d[t_{i+1}]_\infty = dP_{i+1}$.

$$\begin{tikzcd}
{} & {} \\
K(t_{n+1}) \arrow[u, dash] \arrow[r, dash, "d_y"] \arrow[d, dash, "d^n"'] & K(t_{n+1}, y) = K(z) \arrow[u, dash] \arrow[d, dash, "d^n"] \\
K(t_1) \arrow[r, dash, "d_y"] \arrow[d, dash, "d"'] & K(t_1, y) = K(x_1) \arrow[d, dash, "d"] \\
K(t_0) \arrow[r, dash, "d_y"] & K(t_0, y) = K(x_0)
\end{tikzcd}$$

Since $\varphi(X) \in \mathbf{Z}[X]$ and $a \notin E(\varphi)$, we get $t_i \in {}^*\mathbf{Z} - \mathbf{Z}$, hence P_i is exceptional. Let F be a finite algebraic extension of $K(t_i)$ within ${}^*K$.

Then every extension of P_i in F is also exceptional([5, Lemma 6.1]). Therefore by Theorem 2, we have to consider the following three cases;

(i) P_0 has a unique extension Q_1 of degree 1 in $K(t_1, y)$.

(ii) P_0 has two extensions Q_1, R_1 of degree 1 in $K(t_1, y)$.

(iii) P_0 has a unique extension of degree 2 in $K(t_1, y)$.

First we consider the case (i). Let Q_0 be the restriction of Q_1 to $K(t_0, y)$. Then Q_0 is an exceptional prime of degree 1 and a unique extension of P_0 in $K(t_0, y)$. Hence $P_0 = d_yQ_0 = dP_1 = dd_yQ_1$. By Theorem 2 and Lemma 1, there exist $x_0 \in K(t_0, y)$, $x_1 \in K(t_1, y)$ and polynomials $\psi(X), \Phi(X)$ and $\Psi(X)$ of degree d_y, d_y and d respectively such that $[x_0]_\infty = Q_0$, $[x_1]_\infty = Q_1$, $K(t_0, y) = K(x_0)$, $K(t_1, y) = K(x_1)$, $t_0 = \psi(x_0)$, $x_0 = \Psi(x_1)$ and $t_1 = \Phi(x_1)$. Hence we have $t_0 = \psi(\Psi(x_1)) = \varphi(\Phi(x_1))$. Since x_1 is transcendental over K, we get $\psi(\Psi(X)) = \varphi(\Phi(X))$. Since $\deg(\psi) = d_y > 1$ and we are assuming that φ does not satisfy the condition (I),

$$\text{g.c.d.}(\deg(\varphi), \deg(\psi)) > 1.$$

Then by Theorem 3,

$$[K(t_0, y) \cap K(t_1) : K(t_0)] = \text{g.c.d.}(\deg(\varphi), \deg(\psi)) > 1.$$

Therefore,

$$\begin{aligned} d_y &= [\bigcup_{i \in \mathbf{N}} K(\varphi^{s-i}(a), y) : \bigcup_{i \in \mathbf{N}} K(\varphi^{s-i}(a))] \\ &= [\bigcup_{i \in \mathbf{N}} K(t_i, y) : \bigcup_{i \in \mathbf{N}} K(t_i)] \\ &\leq [K(t_0, y) : K(t_0, y) \cap K(t_1)] \\ &< [K(t_0, y) : K(t_0)] = [K(\varphi^{s-k}(a), y) : K(\varphi^{s-k}(a))] = d_y, \end{aligned}$$

this is a contradiction.

Next we consider the case (ii). Since P_1 is a unique extension of P_0 in $K(t_1)$, Q_1 and R_1 are extensions of P_1. Then

$$P_1 = (d_y - m)Q_1 + mR_1$$

for some $m \in \mathbf{N}$ with $0 < m < d_y$. Without loss of generality, we may assume $d_y - m \geq m$. Let $n \in \mathbf{N}$ be such that $d^n > d_y$. Since Q_1 and R_1

are exceptional, by Theorem 2 Q_1 (resp. R_1) has a unique extension Q' (resp. R') of degree 1 in $K(t_{n+1}, y)$. Then P_{n+1} is the restriction of Q' and R' to $K(t_{n+1})$. Since $P_1 = d^n P_{n+1}$, $Q_1 = d^n Q'$ and $R_1 = d^n R'$, we have

$$P_{n+1} = (d_y - m)Q' + mR'.$$

By Theorem 2, there exists a $z \in K(t_{n+1}, y)$ such that $K(z) = K(t_{n+1})$ and $[z] = R' - Q'$ where $[z]$ denotes the principal divisor of z. Since $[t_1]_\infty = P_1$ and $[t_1]_\infty = P_{n+1}$, there exist, by Lemma 1, polynomials $\psi_1(X)$ and $\psi(X)$ of degree d_y such that

$$t_1 = \frac{\psi_1(x_1)}{x_1^m}, \qquad t_{n+1} = \frac{\psi(z)}{z^m}.$$

On the other hand, since $[x_1] = R_1 - Q_1 = d^n(R' - Q') = d^n[z]$, there is a $b \in K$ such that $x_1 = bz^{d^n}$ and $b \neq 0$, hence

$$t_1 = \varphi^n(t_{n+1}) = \varphi^n\left(\frac{\psi(z)}{z^m}\right) = \frac{\psi_1(x_1)}{x_1^m} = \frac{\psi_1(bz^{d^n})}{b^m z^{md^n}}.$$

Since z is transcendental over K, we have

$$b^m X^{md^n} \varphi^n\left(\frac{\psi(X)}{X^m}\right) = \psi_1(bX^{d^n}) \qquad (1)$$

Let $\psi(X) = rX^{d_y} + \lambda(X)$ where $\lambda(X)$ is a polynomial of degree less than d_y. Let $k = \deg(\lambda(X))$. Since $\varphi(X) = cX^d + h(X)$ with $\deg(h) \leq d - 3$, we have $\varphi^n(X) = c^n X^{d^n} + \mu(X)$ for some polynomial $\mu(X)$ with $\deg(\mu) \leq d^n - 3$. Let $j = \deg(\mu)$. Then

$$\deg\left(X^{md^n}\mu\left(\frac{rX^{d_y} + \lambda(X)}{X^m}\right)\right) = md^n + d_y j - mj.$$

On the other hand,

$$X^{md^n}\left(\frac{rX^{d_y} + \lambda(X)}{X^m}\right)^{d^n} = r^{d^n} X^{d_y d^n} + \theta(X)$$

for some polynomial $\theta(X)$ with $\deg(\theta) = d_y(d^n - 1) + k$. Since $d^n - 2 > j$ and $d_y - m > m$, we get

$$\begin{aligned}\deg(\theta) &= d_y(d^n - 1) + k > \frac{d_y(d^n + j)}{2} \geq \frac{d_y(d^n - j)}{2} + d_y j \\ &\geq md^n + d_y j - mj.\end{aligned}$$

Hence

$$b^m X^{md^n} \varphi^n \left(\frac{\psi(X)}{X^m}\right) = b^m r^{d^n} c^n X^{d_y d^n} + \xi(X) \qquad (2)$$

for some polynomial $\xi(X)$ with $\deg(\xi) = deg(\theta) = d_y(d^n - 1) + k$. Since $d^n > d_y$ and $k < d_y$, we have

$$(d_y - 1)d^n < \deg(\xi) < d_y d^n.$$

Combining equations (1) and (2), we get a contradiction because any monomial in $\psi_1(bX^{d^n})$ is of degree id^n for some $i \in \mathbf{N}$.

The case (iii) can be reduced to the case (ii) by taking a quadratic extension of K. This completes the proof of Proposition 1.

Remark. In order to generalize Theorem 1 for polynomials $f(X, T_1, \ldots, T_m)$ of many variables it is necessary to prove that the number k in Theorem 1 is bounded by a constant which is determined by the degree of $f(X,T)$ and independent from its coefficients. For example, if we can prove $k \leq \deg(f)$, then Theorem 1 can be generalized by the same way as in [8]. But the proof of Theorem 1 gives no information about the number k.

REFERENCES

1. DAVENPORT, H., LEWIS, D.J., SCHINZEL, A., *Polynomials of certain special types*, Acta Arith. **9** (1964), 107-116
2. FRIED, M., *On a theorem of Ritt and related diophantine problems*, J. Reine Angew. Math. **264** (1974), 40-55
3. FRIED, M., MACRAE, R. E., *On the invariance of chains of fields*, Illinois J. Math. **13** (1969), 165-171
4. RITT, J. F., *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51-66
5. ROBINSON, A., ROQUETTE, P., *On the finiteness theorem of Siegel and Mahler concerning diophantine equation*, J. Number Theory **7** (1975), 121-176

6. SCHINZEL, A., *On Hilbert's irreducibility theorem*, Ann. Polon. Math. **16** (1965), 333-340

7. ______________, "Selected topics on polynomials," Michigan, 1982.

8. YASUMOTO, M., *Nonstandard arithmetic of polynomial rings*, Nagoya Math. J. **105** (1987), 33-37

9. ______________, *Hilbert's irreducibility sequences and nonstandard arithmetic*, J. Number Theory **26** (1987), 274-285

10. ______________, *Algebraic extensions in nonstandard models and Hilbert's irreducibility theorem*, J. Symbolic Logic **53** (1988), 470-480

Department of Mathematics
College of General Education
Chikusa-ku
Nagoya 464-01
JAPAN

(Received September 23, 1987;
in revised form November 27, 1989)