M. Yasumoto
Nagoya Math. J.
Vol. 105 (1987), 33-37

NONSTANDARD ARITHMETIC OF POLYNOMIAL RINGS

MASAHIRO YASUMOTO

Dedicated to Professor Toshiyuki Tugué on his 60th birthday

Let $f(X, T_1, \cdots, T_m)$ be a polynomial over an algebraic number field K of finite degree. In his paper [2], T. Kojima proved

THEOREM. *Let $K = \boldsymbol{Q}$. If for every m integers $t_1, \cdots, t_m$, there exists an $r \in K$ such that $f(r, t_1, \cdots, t_m) = 0$, then there exists a rational function $g(T_1, \cdots, T_m)$ over $\boldsymbol{Q}$ such that*

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

Later, A. Schinzel [6] proved

THEOREM. *If for every m arithmetic progressions $P_1, \cdots, P_m$ in $\boldsymbol{Z}$ there exist integers $t_i \in P_i$ $(i \leqq m)$ and an $r \in K$ such that $f(r, t_1, \cdots, t_m) = 0$ then there exists a rational function $g(T_1, \cdots, T_m)$ over K such that*

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

In his thesis [7], S. Tung applied these theorems to solve some dicidability and definability problems. In this paper, we are concerned with geometric progressions of values of $T_1, \cdots, T_m$. We prove

THEOREM 1. *Assume that there exists $a_1, \cdots, a_m \in K$ other than 0 and roots of unity such that for any m integers $t_1, \cdots, t_m$, there exists an $r \in K$ with $f(r, a_1^{t_1}, \cdots, a_m^{t_m}) = 0$. Then there exist a rational function $g(T_1, \cdots, T_m)$ over K and m integers $k_1, \cdots, k_m$ not more than k such that*

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

where k is the X-degree of $f(X, T_1, \cdots, T_m)$.

§1.

In case of $m = 1$, Theorem 1 is an easy consequence from Theorem of P. Roquette (Theorem 2.1 [4]) as follows.

Received July 8, 1985.

Let $\omega \in {}^*N - N$ be a nonstandard natural number which is divisible by all natural number where ${}^*N$ is an enlargement of N. By the assumption of Theorem 1, there exists a $\delta \in {}^*K$ such that

$$f(\delta, a^{\omega}) = 0 .$$

Let $k_1 = [K(\delta, a^{\omega}); K(a^{\omega})]$. Since the X-degree of $f(X, T)$ is k,

$$k_1 \leqq k .$$

According to Theorem 2.1 in [4], we have

THEOREM 2. *For each natural number n, there is one and only one extension $F_n = K(a^{\omega/n})$ of $K(a^{\omega})$ within ${}^*K$ such that*

$$[F_n; K(a^{\omega})] = n$$

where ${}^*K$ is an enlargement of K.

Hence, $K(\delta, a^{\omega}) = K(a^{\omega/k_1})$. Therefore there exists a rational function $g(T)$ over T such that $\delta = g(a^{\omega/k_1})$. Now we have

$$f(g(a^{\omega/k_1}), a^{\omega}) = 0 .$$

Since a^{ω/k_1} is transcendental over K,

$$f(g(T), T^{k_1}) = 0$$

as contended.

§ 2.

In this section we prove Theorem 1 for the case $m = 2$. To prove it, we need iterated enlargements. Iterated enlargements are very useful method but sometime they may cause confusion. So first we discuss basic properties of iterated enlargements. Let ${}^\circ K$ be an enlargement of K. We consider the structure $({}^\circ K, K)$ and its enlargement ${}^*({}^\circ K, K) = ({}^{*\circ}K, {}^*K)$. Then ${}^{*\circ}K$ is an elementary extension of ${}^*K$ but not an enlargement of ${}^*K$. By Theorem of Roquette, for each $n \in N$ and $a \in K$ other than 0 and roots of unity, the following statement is valid for $({}^\circ K, K)$;

"*For each $\omega \in {}^\circ N - N$, there is one and only one extension F_n of $K(a^{\omega})$ within ${}^\circ K$ such that $[F_n; K(a^{\omega})] = n$.*"

By nonstandard principle, the above statement holds for $({}^{*\circ}K, {}^*K)$;

"*For each* $\omega \in {}^{*\circ}N - {}^{*}N$, *there is one and only one extension* F_n *of* L *within* ${}^{*\circ}K$ *such that* $[F_n; L] = n$."

where $L = \{h(a^\omega) \mid h(X) \in {}^*(K(X))\}$. It should be noted that the rational function field over ${}^*K$ in the sence of the enlargement generated by a^ω must be L, not ${}^*K(a^\omega)$.

Remark. ${}^{*\circ}K$ is an enlargement of ${}^\circ K$, but Theorem 2 (replacing ${}^\circ K$ and K by ${}^{*\circ}K$ and ${}^\circ K$ respectively) does not hold, because ${}^{*\circ}N$ is not an end extension of ${}^\circ N$, namely there exist a $c \in {}^{*\circ}N - {}^\circ N$ and a $d \in {}^\circ N$ with $c < d$. In fact, let $c \in {}^{*\circ}N$ be an element which satisfies the set of formulas $T = \{c < d \mid d \in {}^\circ N - N\} \cup \{n < c \mid n \in N\}$. Since any finite subset of T is satisfiable and ${}^{*\circ}N$ is an enlargement of ${}^\circ N$, such c exists. On the other hand, ${}^\circ N$ is an end extension of N, so ${}^{*\circ}N$ is also an end extension of ${}^*N$, therefore ${}^{*\circ}K$ is not an enlargement of ${}^*K$.

The following Lemma 1 has been proved in [4] but we include its proof for the convenience of the reader.

LEMMA 1. *Let* M *be any field. Then* ${}^*M(X)$ *is relatively algebraically closed in* ${}^*(M(X))$.

Proof. Let $u(X)/v(X)$ be any element of ${}^*(M(X)) - {}^*M(X)$ where $u(X)$, $v(X) \in {}^*(M[X])$ and g.c.d. $(u(X), v(X)) = 1$ and assume that $u(X)/v(X)$ is algebraic over ${}^*M(X)$. Then there exist $c_0, c_1, \cdots, c_n \in {}^*M[X]$ with $c_0 \neq 0$ and $c_0(u/v)^n + c_1(u/v)^{n-1} + \cdots + c_n = 0$. Since $u/v \notin {}^*M(X)$, the degree of u or v is infinitely large. We may assume without loss of generality that the degree of v is infinitely large. Then

$$c_0u^n + c_1u^{n-1}v + \cdots + c_nv^n = 0$$
$$c_0u^n \equiv 0 \qquad \mathrm{mod}\,(v)\,.$$

Since g.c.d. $(u, v) = 1$,

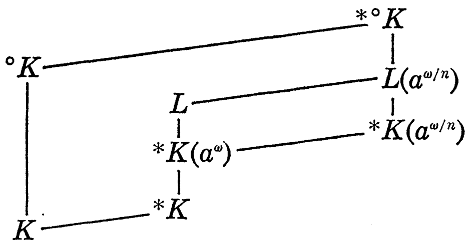
$$c_0 \equiv 0 \qquad \mathrm{mod}\,(v)\,.$$

Since the degree of v is infinitely large and the degree of c_0 is finite, $c_0 = 0$. This is a contradiction.

LEMMA 2. *Let* $a \in K$ *be not* 0 *nor roots of unity and* $\omega \in {}^{*\circ}N - {}^*N$ *be divisible by all natural number. Then* ${}^*K(a^{\omega/n})$ *is the unique extension of* ${}^*K(a^\omega)$ *of degree* n *within* ${}^{*\circ}K$.

Proof. Let $x \in {}^{*\circ}K$ be algebraic over ${}^*K(a^\omega)$ of degree n. Then $x \in L(a^{\omega/n})$ because $L(a^{\omega/n})$ is the unique extension of L of degree n within ${}^{*\circ}K$

and ${}^*K(a^\omega)$ is relatively algebraically closed in $L = \{h(a^\omega) \mid h(X) \in {}^*(K(X))\}$ by Lemma 1.

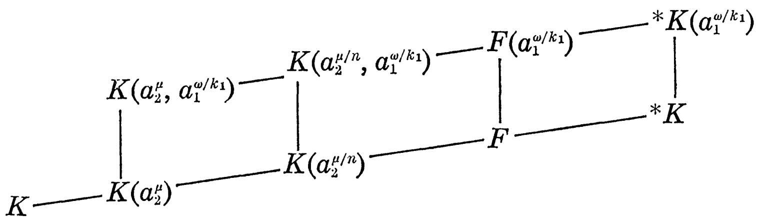


Again by Lemma 1, ${}^*K(a^{\omega/n})$ is relatively algebraically closed in $L(a^{\omega/n}) = \{h(a^{\omega/n}) \mid h(X) \in {}^*(K(X))\}$. Hence $x \in {}^*K(a^{\omega/n})$, as contended.

Let $\omega \in {}^{*\circ}N - {}^*N$ and $\mu \in {}^*N - N$ be divisible by all natural numbers. By the assumption of Theorem 1, there exists a $\delta \in {}^{*\circ}K$ with

$$f(\delta, a_1^\omega, a_2^\mu) = 0 .$$

Since $a_2^\mu \in {}^*K$, δ is algebraic over ${}^*K(a_1^\omega)$ of degree $k_1 \leqq k$. Hence by Lemma 2, $\delta \in {}^*K(a_1^{\omega/k_1})$. Let F be the relative algebraic closure of $K(a_2^\mu)$ within ${}^*K$. Then $\delta \in F(a_1^{\omega/k_1})$ because $F(a_1^{\omega/k_1})$ is relatively algebraically closed in ${}^*K(a_1^{\omega/k_1})$. By Theorem 2, $K(a_2^\mu)$ has the unique extension $K(a_2^{\mu/n})$ of degree n within F. Since a_1^{ω/k_1} is transcendental over F, $K(a_1^{\omega/k_1}, a_2^\mu)$ has the unique extension $K(a_1^{\omega/k_1}, a_2^{\mu/n})$ of degree n within $F(a_1^{\omega/k_1})$.



Let $k_2 = [K(\delta, a_2^\mu, a_1^{\omega/k_1}); K(a_2^\mu, a_1^{\omega/k_1})]$. Then $k_2 \leqq k$ and

$$K(\delta, a_2^\mu, a_1^{\omega/k_1}) = K(a_2^{\mu/k_2}, a_1^{\omega/k_1}) .$$

Hence there exists a rational function $g(T_1, T_2) \in K(T_1, T_2)$ such that

$$f(g(a_1^{\omega/k_1}, a_2^{\mu/k_2}), a_1^\omega, a_2^\mu) = 0 .$$

Since $a_1^{\omega/k_1} \in {}^{*\circ}K - {}^*K$ and $a_2^{\mu/k_2} \in {}^*K - K$ are algebraically independent over K,

$$f(g(T_1, T_2), T_1^{k_1}, T_2^{k_2}) = 0 .$$

§ 3.

Proof of Theorem for $m > 2$ is essentially the same as that in Section 2. By induction on $i \in N$, we define iterated enlargements $K_i = ({}^{*i\cdots*2*1}K, {}^{*i\cdots*3*2}K, \cdots, {}^{*i}K)$ as follows. Let $K_1 = ({}^{*1}K)$. K_{i+1} is an enlargement of $(K_i, K) = ({}^{*i\cdots*2*1}K, {}^{*i\cdots*3*2}K, \cdots, {}^{*i}K, K)$, i.e. $K_{i+1} = {}^{*i+1}(K_i, K) = ({}^{*i+1}K_i, {}^{*i+1}K)$. Let $\omega_j \in {}^{*m\cdots*j+1*j}N - {}^{*m\cdots*j+1}N$ be divisible by all natural numbers. Let $\delta \in {}^{*m\cdots*1}K$ satisfy

$$f(\delta, a_1^{\omega_1}, a_2^{\omega_2}, \cdots, a_m^{\omega_m}) = 0 .$$

Then by the same way as in Section 2, there exist natural numbers $k_1, k_2, \cdots, k_m$ not more than k such that $\delta \in K(a_1^{\omega_1/k_1}, \cdots, a_m^{\omega_m/k_m})$. Since $a_1^{\omega_1/k_1}, \cdots, a_m^{\omega_m/k_m}$ are algebraically independent over K, there is a rational function $g(T_1, \cdots, T_m) \in K(T_1, \cdots, T_m)$ such that

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

References

[1] H. Davenport, D. J. Lewis and A. Schinzel, Polynomials of certain special types, Acta Arith., **9** (1964), 107–116.

[2] T. Kojima, Note on number theoretic properties of algebraic functions, Tohoku Math. J., **8** (1915), 24–37.

[3] A. Robinson and P. Roquette, On the finiteness theorem of Siegel and Mahler concerning diophantine equations, J. Number Theory, **7** (1975), 121–176.

[4] P. Roquette, Nonstandard aspects of Hilbert's irreducible theorem, Lecture Notes in Math., **498**, 231–274.

[5] A. Schinzel, On Hilbert's irreducible theorem, Ann. Polon. Math., **16** (1965), 333–340.

[6] ——, Selected topics on polynomials, Michigan 1982.

[7] S. Tung, On weak number theories, Thesis Illinois 1983.

[8] T. Skolem Einige Satze uber Polynome, Avhandlinger Norske Vid. Akad. Oslo, I Mat-Naturv. Kl. No. 4.

Department of Mathematics
Faculty of Science
Nagoya University
Chikusa-ku, Nagoya 464
Japan