数理解析研究所講究録
第 657 巻 1988 年 39-44

Nonstandard Arithmetic of Iterated Polynomials

Masahiro Yasumoto (Nagoya university)

Let $^*Q$ be an enlargement of the rational number field Q, where by an enlargement, we mean an elementary extension which satisfies ω_1-saturation property. Let $t \in {}^*Q - Q$ be a nonstandard rational number. Then t is transcendental over Q. In this paper, we are concerned with algebraic extensions of a rational function field $Q(t)$ in $^*Q$ Structures of such extensions are closely related to diophantine problems.

Let us begin with some definitions about such extensions. We denote by Ω_t the relative algebraic closure of $Q(t)$ in $^*Q$.

$$\Omega_t = \overline{Q(t)} \cap {}^*Q$$

For each $d \in N$, we define $Y(t,d)$ to be the number of algebraic extensions of $Q(t)$ of degree d in $^*Q$.

$$Y(t,d) = {}^{\#}\{F \subset {}^*Q \mid [F : Q(t)] = d\}.$$

It is well known [2] that there is a nonstandard integer t such that $Y(t,d) = 0$ for all $d > 1$, in other words, $\Omega_t = Q(t)$. This fact is equivalent to the following Hilbert's irreducibility theorem.

Theorem. *For any irreducible polynomial $f(X,Y) \in Q[X,Y]$, there are infinitely many integers n such that $f(X,n)$ is also irreducible.*

In his paper [4], P.Roquette proved

Theorem. *If $t \in {}^*Q - Q$ is composed of standard primes only, i.e.*

$$t = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$$

where $p_1, \ldots, p_n$ are standard primes, $n \in N$ and $\alpha_1, \ldots \alpha_n \in {}^*Z$, then

$$\Omega_t = \bigcup_{d \in N} Q(p_1^{[\alpha_1/d]} \ldots p_n^{[\alpha_n/d]})$$

where $[x]$ denotes the largest integer not more than x.

This theorem can be applied to prove the following theorem [5] in standard number theory.

Theorem. *Let $f(X, T_1, \ldots, T_m)$ be a polynomial over Q. Assume there exist $c_1, \ldots, c_m \in Q$ other than 0 and ± 1 such that for any m integers $n_1, \ldots, n_m$, there exists an $r \in Q$ with*

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

Then there exist a rational function $g(T_1, \ldots, T_m)$ over Q and m integers $k_1, \ldots, k_m$ not more than the X-degree of $f(X, T_1, \ldots, T_m)$ such that

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

In case of $m = 1$, Prof. Fried pointed out that the theorem can be proved without nonstandard method but in case of $m \geq 2$, no proof of the theorem without nonstandard method is known.

Next we consider another type of nonstandard integers. Let $\varphi(X) \in Z[X]$, $a \in Z$ and $\alpha \in {}^*N - N$. Let

$$t = \varphi^\alpha(a) \in {}^*Z$$

t may be standard. We have to exclude such trivial cases. t is standard if and only if $\varphi^m(a) = \varphi^n(a)$ for some $m \neq n$. Since $\varphi(X)$ is a polynomial, there are only finitely many integers a satisfying the above condition. So in the following, we always assume that a is an integer which does not satisfy the condition.

Let $\varphi(X) = cX + d$ be a linear polynomial where c is a rational number other than 0 and ± 1. Then

$$\varphi^{\alpha}(a) = \left(a - \frac{d}{c-1}\right) c^{\alpha} - \frac{d}{c-1}$$

Hence

$$Q(\varphi^{\alpha}(a)) = Q(c^{\alpha})$$

Therefore by the theorem of Roquette,

$$\Omega_{\varphi^{\alpha}(a)} = \bigcup_{d \in N} Q(c^{[\alpha/d]})$$

Next we consider a polynomial $\varphi(X) \in Z[X]$ of degree at least 2. Then it is easily shown that $Q(\varphi^{\alpha}(a))$ has a tower of algebraic extensions,

$$Q(\varphi^{\alpha}(a)) \subset Q(\varphi^{\alpha-1}(a)) \subset Q(\varphi^{\alpha-2}(a)) \subset \dots$$

$$\subset Q(\varphi^{\alpha-i}(a)) \subset \dots \subset \Omega_{\varphi^{\alpha}(a)}.$$

So the problem is wether

$$\Omega_{\varphi^{\alpha}(a)} = \bigcup_{i \in N} Q(\varphi^{\alpha-i}(a)). \tag{1}$$

But unfortunately there is a counter example of the equation (1). For example, let $\varphi(X) = X^2$, then $\varphi^{\alpha}(2) = 2^{2^{\alpha}}$. Hence

$$\bigcup_{i \in N} Q(\varphi^{\alpha-i}(2)) = \bigcup_{i \in N} Q(2^{2^{\alpha-i}})$$

On the other hand, by the theorem of Roquette,

$$\Omega_{2^{2^\alpha}} = \bigcup_{d\in N} Q(2^{[2^\alpha/d]})$$

Since $2^{[2^\alpha/3]}$ is algebraic over $Q(2^{2^\alpha})$ of degree 3 but $Q(2^{2^{\alpha-i}})$ is algebraic over $Q(2^{2^\alpha})$ of degree 2^i, then $2^{[2^\alpha/3]}$ is not an element of $Q(2^{2^{\alpha-i}})$ Therefore the equation does not hold for $\varphi(X) = X^2$. Our aim is to give a condition for a polynomial $\varphi(X)$ to satisfy the equation (1). First let us 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.$(\deg(\varphi), \deg(\psi(X)) = 1, \deg(\psi) \geq 2$ and $\varphi(\Phi(X)) = \psi(\Psi(X))$.
Ritt[2] and Fried[1] gave a characterization of polynomials satisfying the condition (I). Now we can state our main theorem.

Theorem 1. *Let $\varphi(X) = cX^d + h(X) \in Z[X]$ be a polynomial of degree at least 3 which does not satisfy the condition (I) where $c \neq 0$ and $deg(h) \leq d-3$. Let a be an integer such that $\varphi^m(a) \neq \varphi^n(a)$ for every $m \neq n$. Then for every $\alpha \in {}^*N - N$,*

$$\Omega_{\varphi^\alpha(a)} = \bigcup_{i\in N} Q(\varphi^{\alpha-i}(a)).$$

For proof of Theorem 1, refer to [8]. This theorem can be applied to prove the following theorem in standard number theory.

Theorem 2. *Let $\varphi(X)$ and a be as in Theorem 1 and let $f(X,T)$ be a polynomial over Q. If for any $n \in N$ there exists an $r \in Q$ such that*

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

then there exist a rational function $g(X)$ over Q and $k \in N$ such that

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

Proof: By assumption of the theorem, there exist $\alpha \in {}^*N - N$ and $x \in {}^*Q$ such that

$$f(x, \varphi^{\alpha}(a)) = 0$$

By Theorem 1, for some $k \in N$

$$x \in Q(\varphi^{\alpha-k}(a))$$

Let $g(T)$ be a rational function over Q with

$$x = g(\varphi^{\alpha-k}(a)).$$

Then

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

Since $\varphi^{\alpha-k}(a) \in {}^*Z - Z$, $\varphi^{\alpha-k}(a)$ is transcendental over Q, therefore

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

as contended. ◇

This is a new theorem proved by nonstandard method. It is not known wether Theorem 2 can be generalized for polynomials of many variables.

References

1. Fried, M., *On a theorem of Ritt and related diophantine problems*, J. Reine Angew. Math. **264** (1974), 40-55.
2. Gilmore, P. C. and Robinson, A., *Metamathematical considerations on the relative irreducibility of polynomials*, Canad. J. Math. **7** (1955), 483-489.
3. Ritt, J. F., *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51-66.
4. Roquette, P., *Nonstandard aspects of Hilbert's irreducibility theorem*, L.N.M. **498** (1975), 231-275.
5. Yasumoto, M., *Nonstandard arithmetic of polynomial rings*, Nagoya Math. J. **105** (1987), 33-37.

6. Yasumoto, M., *Hilbert's irreducibility sequences and nonstandard arithmetic*, J. Number Theory **26** (1987).
7. Yasumoto, M., *Algebraic extensions in nonstandard models and Hilbert's irreducibility theorem*, to appear in J. Symbolic Logic.
8. Yasumoto, M., *Nonstandard arithmetic of iterated polynomials*, preprint.