PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 108, Number 1, January 1990

P-ADIC TRANSCENDENTAL NUMBERS

KUMIKO NISHIOKA

(Communicated by William Adams)

ABSTRACT. Explicit sets of cardinality $2^{\aleph_0}$ of p-adic numbers which are algebraically independent over Q_p are constructed.

Let $\mathbf{Q}_p$ be the p-adic completion of $\mathbf{Q}$ for a prime p. Let $\overline{\mathbf{Q}}_p$ be the algebraic closure of $\mathbf{Q}_p$, and $\mathbf{C}_p$ be its p-adic completion which is an algebraically closed field of cardinality $2^{\aleph_0}$. Let $\mathbf{Q}_p^{\mathrm{unram}}$ be the maximum unramified extension field of $\mathbf{Q}_p$. Then $\mathbf{Q}_p^{\mathrm{unram}} = \mathbf{Q}_p(W)$, where W is the set of all roots of unity whose orders are prime to p. Let $\mathbf{C}_p^{\mathrm{unram}}$ be the p-adic closure of $\mathbf{Q}_p^{\mathrm{unram}}$ in $\mathbf{C}_p$. Koblitz [1] asked whether $\mathbf{C}_p^{\mathrm{unram}}$ has uncountably infinite transcendence degree over $\mathbf{Q}_p$ and $\mathbf{C}_p$ has uncountably infinite transcendence degree over $\mathbf{C}_p^{\mathrm{unram}}$. Lampert [2] answered that the transcendence degree of $\mathbf{C}_p^{\mathrm{unram}}$ over $\mathbf{Q}_p$ is $2^{\aleph_0}$ and the transcendence degree of $\mathbf{C}_p$ over $\mathbf{C}_p^{\mathrm{unram}}$ is $2^{\aleph_0}$ by constructing sets of algebraically independent numbers of cardinality $2^{\aleph_0}$. Here we will give more explicit examples of such sets which cannot be obtained by the method in [2].

Theorem. *Let K be an intermediate field between $\mathbf{Q}_p$ and $\mathbf{C}_p$. Let $\alpha_1, \dots, \alpha_m$ be in $\mathbf{C}_p$ and $\alpha_1, \dots, \alpha_{m-1}$ be algebraically independent over K. Suppose that for $i = 1, \dots, m-1$ there exist sequences $\{\beta_{ik}\}_{k\geq 1}$ in $\mathbf{C}_p$ converging to α_i and a sequence $\{S_k\}_{k\geq 1}$ of finite subsets of* $\mathrm{Aut}(\mathbf{C}_p/K(\{\beta_{ik}\}_{1\leq i\leq m-1}))$ *which satisfies*

$$(1)\qquad \lim_{k\to\infty} |S_k| = \infty \quad \text{and} \quad \alpha_m^\sigma \neq \alpha_m^\tau \text{ for any } \sigma, \tau \in S_k \text{ with } \sigma \neq \tau,$$

$$(2)\qquad \max_{1\leq i\leq m-1} |\alpha_i - \beta_{ik}|_p = o\left(\min_{\substack{\sigma,\tau\in S_k\\ \sigma\neq\tau}} |\alpha_m^\sigma - \alpha_m^\tau|_p\right) \quad \text{as } k\to\infty,$$

where we define the left-hand side of (2) *to be* 0 *if $m = 1$. Then $\alpha_1, \dots, \alpha_m$ are algebraically independent over K.*

To prove the theorem we need the following lemma which is proved in Koblitz [1].

Received by the editors March 13, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11J61.

Lemma (Koblitz [1], p. 70). Let $f(X) \in \mathbf{C}_p[X]$ have degree n,

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0.$$

Suppose that $f(X)$ has no multiple root. Then there exists a positive constant c such that if $g(X) = \sum_{i=0}^{n} b_i X^i \in \mathbf{C}_p[X]$ has degree n, and if $\max_{0\le i\le n} |a_i - b_i|_p$ is sufficiently small, then for every root β of $g(X)$ there is precisely one root α of $f(X)$ such that

$$|\alpha - \beta|_p \le \max_{1\le i\le n} |a_i - b_i|_p.$$

Proof of theorem. Suppose that $\alpha_1, \dots, \alpha_m$ are algebraically dependent over K. Then there exists a polynomial $f(X)$ of degree n with coefficients in $K[\alpha_1, \dots, \alpha_{m-1}]$,

$$f(X) = Q_n(\alpha_1, \dots, \alpha_{m-1}) X^n + \cdots + Q_0(\alpha_1, \dots, \alpha_{m-1})$$

such that $f(\alpha_m) = 0$ and $f(X)$ has no multiple root. If $\sigma \in S_k$, then

$$\begin{aligned}
&|Q_i(\alpha_i^\sigma, \dots, \alpha_{m-1}^\sigma) - Q_i(\alpha_1, \dots, \alpha_{m-1})|_p \\
&\quad\le \max\{|Q_i(\alpha_1^\sigma, \dots, \alpha_{m-1}^\sigma) - Q_i(\beta_{1k}, \dots, \beta_{m-1,k})|_p, \\
&\qquad\qquad |Q_i(\beta_{1k}, \dots, \beta_{m-1,k}) - Q_i(\alpha_1, \dots, \alpha_m)|_p\} \\
&\quad\le c_1 \max_{1\le i\le m-1} |\alpha_i - \beta_{ik}|_p,
\end{aligned}$$

where c_1 is a positive constant. If k is sufficiently large, then $|S_k| > n$ and by the lemma, there exists a root α of $f(X)$ and two distinct elements σ, τ of S_k such that

$$|\alpha - \alpha_m^\sigma|_p, \ |\alpha - \alpha_m^\tau|_p \le c_2 \max_{1\le i\le m-1} |\alpha_i - \beta_{ik}|_p,$$

where c_2 is a positive constant, and so

$$\min_{\substack{\sigma,\tau\in S_k \\ \sigma\ne\tau}} |\alpha_m^\sigma - \alpha_m^\tau|_p \le c_2 \max_{1\le i\le m-1} |\alpha_i - \beta_{ik}|_p.$$

This contradicts condition (2) and the theorem is proved.

It is well known that every element α of $\mathbf{C}_p^{\text{unram}}$ is uniquely represented as $\alpha = \sum_{n\ge q} \zeta_n p^n$ where $\zeta_n \in W$ and $q \in \mathbf{Z}$. The number α is transcendental over $\mathbf{Q}_p$ if and only if the extension degree $[\mathbf{Q}_p(\zeta_n) : \mathbf{Q}_p]$, $n \ge q$, is unbounded. By using the theorem, we obtain a set of cardinality $2^{\aleph_0}$ whose elements are in $\mathbf{C}_p^{\text{unram}}$ and algebraically independent over $\mathbf{Q}_p$.

Example 1. Let $\zeta(n)$ be a primitive nth root of unity for every natural number n. Let P be the set of all prime numbers. Then the numbers

$$\sum_{n=1}^{\infty} \zeta(l^{[\lambda n]}) p^n, \qquad (l \in P - \{p\}, \lambda \in \mathbf{R}^+)$$

are algebraically independent over $\mathbf{Q}_p$.

Proof. Let $l_1, \dots, l_s \in P - \{p\}$ and K be the p-adic closure of $\mathbf{Q}_p(\{\zeta(l_i^n)\}_{1\le i\le s, n\ge 0})$. Let $l \in P - \{p, l_1, \dots, l_s\}$ and $0 < \lambda_1 < \cdots < \lambda_m$. Put

$$\alpha_i = \sum_{n=0}^{\infty} \zeta(l^{[\lambda_i n]})p^n, \qquad 1 \le i \le m.$$

It is enough to prove that $\alpha_1, \dots, \alpha_m$ are algebraically independent over K. We prove it by induction on m. Assume that $\alpha_1, \dots, \alpha_{m-1}$ are algebraically independent over K. Put

$$\beta_{ik} = \sum_{n=1}^{k+[\log k]} \zeta(l^{[\lambda_i n]})p^n, \qquad 1 \le i \le m-1, \; k \ge 1,$$

and

$$d_k = [K(\zeta(l^{[\lambda_m k]})) : K(\zeta(l^{[\lambda_{m-1}(k+[\log k])]}))].$$

Then

$$|\alpha_i - \beta_{ik}|_p = p^{-k-[\log k]-1}$$

and $\lim_{k\to\infty} d_k = \infty$. Let S_k be a set of d_k isomorphisms of $\mathbf{C}_p$ which is obtained by extending $\mathrm{Gal}(K(\zeta(l^{[\lambda_m k]}))/K(\zeta(l^{[\lambda_{m-1}(k+[\log k])]})))$. Then

$$\min_{\substack{\sigma,\tau\in S_k \\ \sigma\ne\tau}} |\alpha_m^\sigma - \alpha_m^\tau|_p \ge p^{-k}.$$

Hence by the theorem, $\alpha_1, \dots, \alpha_m$ are algebraically independent over K.

In a similar way, we obtain a set of cardinality $2^{\aleph_0}$ whose elements are in $\mathbf{C}_p$ and algebraically independent over $\mathbf{C}_p^{\mathrm{unram}}$.

Example 2. The numbers

$$\sum_{n=1}^{\infty} p^{n+l^{-[\lambda n]}}, \qquad (l \in P - \{p\}, \; \lambda \in \mathbf{R}^+)$$

are algebraically independent over $\mathbf{C}_p^{\mathrm{unram}}$.

REFERENCES

1. N. Koblitz, *P-adic number theory, p-adic analysis and zeta functions*, G. T. M. Vol. 58, Springer-Verlag, New York, 1977.
2. D. Lampert, *Algebraic P-adic expansions*, J. Number Theory **23** (1986), 279–284.

NARA WOMEN'S UNIVERSITY, DEPARTMENT OF MATHEMATICS, KITA-UOYA NISHIMACHI, NARA 630, JAPAN