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 $Q$ be the $p$-adic completion of $Q$ for a prime $p$. Let $Q_p$ be the algebraic closure of $Q_p$, and $C_p$ be its $p$-adic completion which is an algebraically closed field of cardinality $2^\aleph_0$. Let $Q^{unram}_p$ be the maximum unramified extension field of $Q_p$. Then $Q^{unram}_p = Q_p(W)$, where $W$ is the set of all roots of unity whose orders are prime to $p$. Let $C^{unram}_p$ be the $p$-adic closure of $Q^{unram}_p$ in $C_p$. Koblitz [1] asked whether $C^{unram}_p$ has uncountably infinite transcendence degree over $Q_p$ and $C_p$ has uncountably infinite transcendence degree over $C^{unram}_p$. Lampert [2] answered that the transcendence degree of $C^{unram}_p$ over $Q_p$ is $2^\aleph_0$ and the transcendence degree of $C_p$ over $C^{unram}_p$ 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 $Q_p$ and $C_p$. Let $\alpha_1, \ldots, \alpha_m$ be in $C_p$ and $\alpha_1, \ldots, \alpha_{m - 1}$ be algebraically independent over $K$. Suppose that for $i = 1, \ldots, m - 1$ there exist sequences $\{\beta_{ik}\}_{k \geq 1}$ in $C_p$ converging to $\alpha_i$ and a sequence $\{S_k\}_{k \geq 1}$ of finite subsets of $\text{Aut}(C_p/K(\{\beta_{ik}\}_{1 \leq i \leq m - 1}))$ which satisfies

1. $\lim_{k \to \infty} |S_k| = \infty$ and $\alpha_\sigma^\sigma \neq \alpha_\tau^\tau$ for any $\sigma, \tau \in S_k$ with $\sigma \neq \tau$,

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

where we define the left-hand side of (2) to be $0$ if $m = 1$. Then $\alpha_1, \ldots, \alpha_m$ 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.

Lemma (Koblitz [1], p. 70). Let \( f(X) \in \mathbb{C}_p[X] \) 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 \( g(X) = \sum_{i=0}^{n} b_i X^i \in \mathbb{C}_p[X] \) has degree \( n \), and if \( \max_{0 \leq i \leq n} |a_i - b_i|_p \) is sufficiently small, then for every root \( \beta \) of \( g(X) \) there is precisely one root \( \alpha \) of \( f(X) \) such that
\[
|\alpha - \beta|_p \leq \max_{1 \leq i \leq n} |a_i - b_i|_p.
\]

Proof of theorem. Suppose that \( \alpha_1, \ldots, \alpha_m \) are algebraically dependent over \( K \). Then there exists a polynomial \( f(X) \) of degree \( n \) with coefficients in \( K[\alpha_1, \ldots, \alpha_{m-1}] \),
\[
f(X) = Q_n(\alpha_1, \ldots, \alpha_{m-1}) X^n + \cdots + Q_0(\alpha_1, \ldots, \alpha_{m-1})
\]
such that \( f(\alpha_m) = 0 \) and \( f(X) \) has no multiple root. If \( \sigma \in S_k \), then
\[
|Q_i(\alpha_1^\sigma, \ldots, \alpha_{m-1}^\sigma) - Q_i(\alpha_1, \ldots, \alpha_{m-1})|_p
\leq \max\{|Q_i(\alpha_1^\sigma, \ldots, \alpha_{m-1}^\sigma) - Q_i(\beta_1, \ldots, \beta_{m-1}, k)|_p, |Q_i(\beta_1, \ldots, \beta_{m-1}, k) - Q_i(\alpha_1, \ldots, \alpha_{m})|_p\}
\leq c_1 \max_{1 \leq i \leq m-1} |\alpha_i - \beta_{ik}|_p,
\]
where \( c_1 \) is a positive constant. If \( k \) is sufficiently large, then \( |S_k| > n \) and by the lemma, there exists a root \( \alpha \) of \( f(X) \) and two distinct elements \( \sigma, \tau \) of \( S_k \) such that
\[
|\alpha - \alpha_m^\sigma|_p, |\alpha - \alpha_m^\tau|_p \leq c_2 \max_{1 \leq i \leq m-1} |\alpha_i - \beta_{ik}|_p,
\]
where \( c_2 \) is a positive constant, and so
\[
\min_{\sigma, \tau \in S_k} |\alpha_m^\sigma - \alpha_m^\tau|_p \leq c_2 \max_{1 \leq i \leq m-1} |\alpha_i - \beta_{ik}|_p.
\]
This contradicts condition (2) and the theorem is proved.

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

Example 1. Let \( \zeta(n) \) be a primitive \( n \)th root of unity for every natural number \( n \). Let \( P \) be the set of all prime numbers. Then the numbers
\[
\sum_{n=1}^{\infty} \zeta(l^{\lambda n})p^n, \quad (l \in P - \{p\}, \lambda \in \mathbb{R}^+)
\]
are algebraically independent over \( \mathbb{Q}_p \).
Proof. Let $l_1, \ldots, l_s \in P - \{p\}$ and $K$ be the $p$-adic closure of
$\mathbb{Q}_p(\{(l_i^n)_{1 \leq i \leq s, n \geq 0}\})$. Let $l \in P - \{p, l_1, \ldots, l_s\}$ and $0 < \lambda_1 < \cdots < \lambda_m$.
Put
$$\alpha_i = \sum_{n=0}^{\infty} \zeta(l_i^n)p^n, \quad 1 \leq i \leq m.$$ 
It is enough to prove that $\alpha_1, \ldots, \alpha_m$ are algebraically independent over $K$.
We prove it by induction on $m$. Assume that $\alpha_1, \ldots, \alpha_{m-1}$ are algebraically
independent over $K$. Put
$$\beta_{ik} = \sum_{n=1}^{k + [\log k]} \zeta(l_i^n)p^n, \quad 1 \leq i \leq m - 1, \ k \geq 1,$$
and
$$d_k = [K(\zeta(l_{m-k})): K(\zeta(l_{m-1-k+\log k}))].$$ 
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 $\mathbb{C}_p$ which is
obtained by extending $\text{Gal}(K(\zeta(l_{m-k}))/K(\zeta(l_{m-1-k+\log k})))$. Then
$$\min_{\sigma, \tau \in S_k} |\alpha_m - \sigma \alpha_m|_p \geq p^{-k}.$$ 
Hence by the theorem, $\alpha_1, \ldots, \alpha_m$ are algebraically independent over $K$.

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

Example 2. The numbers
$$\sum_{n=1}^{\infty} p^{n+\lambda-l} , \quad (l \in P - \{p\}, \ \lambda \in \mathbb{R}^+)$$
are algebraically independent over $\mathbb{C}_p^{\text{unram}}$.

REFERENCES

1. N. Koblitz, *P-adic number theory, p-adic analysis and zeta functions*, G. T. M. Vol. 58,


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

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use