Journal of Pure and Applied Algebra 13 (1978) 41–47.
© North-Holland Publishing Company

ON THE ALGEBRAIC INDEPENDENCE OF CERTAIN LIOUVILLE NUMBERS

William W. ADAMS
Department of Mathematics, University of Maryland, College Park, MD 20742, U.S.A.

Received 24 June 1977

Dedicated to the memory of George Cooke

1. Introduction

The purpose of this paper is to prove that certain sets of Liouville numbers are algebraically independent. For this purpose we define α to be a *Liouville series* provided α has a representation as an infinite series of the form

$$\alpha = \sum_{\nu=1}^{\infty} p^{-k_\nu}$$

where $p > 1$ is an integer and k_ν is a strictly increasing sequence of positive integers such that

$$\lim_{N\to\infty} \frac{k_{N+1}}{k_N} = \infty.$$

The following theorem is proved.

Theorem 1. *Let $\alpha_1 = \sum_{\nu=1}^{\infty} p_1^{-k_\nu}$, $\alpha_2 = \sum_{\nu=1}^{\infty} p_2^{-k_\nu}$ and $\alpha_3 = \sum_{\nu=1}^{\infty} p_3^{-k_\nu}$ be Liouville series, where we assume that $p_1 \neq p_2$ and that $P > 2$ is a prime such that*

$$P \mid p_3, \qquad P \nmid p_1, \qquad P \nmid p_2 \quad \text{and} \quad P - 1 \mid k_\nu$$

for all ν large.

Finally we assume there is a strictly increasing sequence N_j of positive integers such that N_j has an infinite number of limit points in the P-adic integers $\mathbb{Z}_P$ and such that

$$\text{ord}_P k_{N_j} < \text{ord}_P k_\nu \quad \text{for all } \nu > N_j$$

and

$$k_{N_j-1}/\text{ord}_P k_{N_j} \to \infty \quad (j \to \infty).$$

Then α_1, α_2, α_3 are algebraically independent.

Example. The integers $k_\nu = \nu\,!$ satisfy the hypotheses with $N_j = -1 + jP$. Thus we see that

$$\sum_{\nu=1}^{\infty} 2^{-\nu!}, \quad \sum_{\nu=1}^{\infty} 4^{-\nu!}, \quad \sum_{\nu=1}^{\infty} 3^{-\nu!}$$

are algebraically independent.

It was pointed out to me by David Cantor that with a stronger hypothesis on the p_i, the restriction to 3 variables is easily lifted. Namely the following is true.

Theorem 2. *Let $\alpha_i = \sum_{\nu=1}^{\infty} p_i^{-k_\nu}$ be Liouville Series $(1 \leq i \leq n)$ where $p_1, \ldots, p_n$ are multiplicatively independent integers larger than 1. Then $\alpha_1, \ldots, \alpha_n$ are algebraically independent.*

The proof proceeds in two stages. First we generalize the usual Liouville criterion for transcendence [2, p. 121] in the most naive possible way (Section 2). This generalization requires an hypothesis concerning the non-vanishing of polynomials in more than one variable at certain rational points. This hypothesis is easily verified to prove Theorem 2. In Section 3 we give a P-adic argument to verify the hypothesis in order to prove Theorem 1.

There are many other results on the algebraic independence of Liouville numbers (c.f. [3, 4]). They all concentrate on having approximation hypotheses strong enough to guarantee in advance that the polynomials involved cannot vanish at the appropriate rational points. These theorems do not seem to be strong enough to prove the results of this paper.

2. A generalized Liouville theorem

Proposition 3. *Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ be a vector of real numbers which is algebraically dependent. Let $f(x)$ be any non-zero polynomial in n-variables, with integer coefficients and degree d_i in x_i $(x = (x_1, \ldots, x_n))$ such that $f(\alpha) = 0$. Then there exists a constant $c = c(\alpha, f)$ such that for all rational n-tuples $a/b = (a_1/b_1, \ldots, a_n/b_n)$ $(b_i > 0)$ we have either*

$$f\left(\frac{a}{b}\right) = 0 \tag{1}$$

or

$$\left\|\frac{a}{b} - \alpha\right\| \geq \frac{c}{b_1^{d_1} b_2^{d_2} \cdots b_n^{d_n}}. \tag{2}$$

Proof. Assuming $f(a/b) \neq 0$ we have

$$\frac{1}{b_1^{d_1} \cdots b_n^{d_n}} \leq \left|f\left(\frac{a}{b}\right)\right| = \left|f\left(\frac{a}{b}\right) - f(\alpha)\right|$$

$$\leq \sup_{\substack{\xi \text{ on line} \\ \text{between } a/b \text{ and } \alpha}} |\nabla f(\xi)| \left\|\frac{a}{b} - \alpha\right\|.$$

Either $\|a/b-\alpha\|\geqslant 1$ or there exists $C=C(\alpha,f)$ such that

$$\sup_{\xi}|Df(\xi)|\leqslant C,$$

and we are done.

Corollary 4. *Let $\alpha=(\alpha_1,\ldots,\alpha_n)$ be real. Suppose that for all positive integer n-tuples $d_1,\ldots,d_n$ and that for all non-zero polynomials $f(x)$ with integer coefficients in n variables, there is a rational $a/b=(a_1/b_1,\ldots,a_n/b_n)$ such that*

$$f\left(\frac{a}{b}\right)\neq 0 \tag{3}$$

and

$$\left\|\frac{a}{b}-\alpha\right\|\leqslant\frac{1}{b_1^{d_1}\cdots b_n^{d_n}}. \tag{4}$$

Then $\alpha=(\alpha_1,\ldots,\alpha_n)$ is algebraically independent.

Now suppose that

$$\alpha_i=\sum_{\nu=1}^{\infty}p_i^{-k_\nu}\quad(1\leqslant i\leqslant n)$$

are Liouville series. Set

$$\frac{a_i}{b_i}=\sum_{\nu=1}^{N}p_i^{-k_\nu}$$

so that $b_i=p_i^{k_N}$. Then

$$\left\|\frac{a}{b}-\alpha\right\|\leqslant\sqrt{n}\max_{1\leqslant i\leqslant n}\left\{\left|\frac{a_i}{b_i}-\alpha_i\right|\right\}\leqslant\sqrt{n}\frac{2}{p_1^{k_{N+1}}},$$

where we assume $p_1\leqslant p_i$ $(2\leqslant i\leqslant n)$. It is then easily verified that (4) is satisfied for some N sufficiently large, depending on $d_1,\ldots,d_n$.

Thus we arrive at the following.

Lemma 5. *Let $p_1,\ldots,p_n$ be integers. In order to show that Liouville series*

$$\sum_{\nu=1}^{\infty}p_1^{-k_\nu},\ldots,\sum_{\nu=1}^{\infty}p_n^{-k_\nu}$$

are algebraically independent, it suffices to show that for all non-zero polynomials $f(x)$ in n-variables with integer coefficients, there exist infinitely many N such that

$$f\left(\sum_{\nu=1}^{N}p_1^{-k_\nu},\ldots,\sum_{\nu=1}^{N}p_n^{-k_\nu}\right)\neq 0.$$

$$|p_1^{-k_\nu} - p_2^{-k_\nu}|_P = \frac{1}{p}|(a_1 - a_2)k_\nu|_P \tag{8}$$

where a_1, a_2 are given in (6).

To prove (a) in Lemma 6, we see that we may take $p_1 = p$ and $p_2 = 1$ in (8) to conclude that

$$|p^{-k_\nu} - 1|_P \leq |k_\nu|_P \xrightarrow[\nu\to\infty]{} 0,$$

since the hypothesis of Theorem 1 guarantees that $\mathrm{ord}_P k_\nu \to \infty$ $(\nu \to \infty)$.

To prove (b) in Lemma 6 we see immediately from (8) that the first term dominates the sum and has the desired form.

4. Proof of Theorem 2

We must show that the hypotheses of Lemma 5 are valid. So assume that $p_1, \ldots, p_n$ are multiplicatively independent and that $f(x_1, \ldots, x_n)$ is a polynomial such that for all N large

$$f\left(\sum_{\nu=1}^{N} p_1^{-k_\nu}, \ldots, \sum_{\nu=1}^{N} p_n^{-k_\nu}\right) = 0. \tag{9}$$

Setting $\alpha_i = \sum_{\nu=1}^{\infty} p_i^{-k_\nu}$ $(1 \leq i \leq n)$ we also have

$$f(\alpha_1, \ldots, \alpha_n) = 0.$$

Consider the Taylor Expansion of f about $\alpha_1, \ldots, \alpha_n$,

$$f(x_1, \ldots, x_n) = \sum_{(i)} C_{(i)}(x - \alpha_i)^{i_1} \cdots (x - \alpha_n)^{i_n},$$

for $(i) = (i_1, \ldots, i_n)$.

Since $p_1, \ldots, p_n$ are multiplicatively independent, the integers $a_{(i)} = p_1^{i_1} \cdots p_n^{i_n}$ are all different. Choose (i_0) such that $a_{(i_0)}$ is least with $C_{(i_0)} \neq 0$. We observe that

$$p_i^{-k_{N+1}} \leq \sum_{\nu=N+1}^{\infty} p_i^{-k_\nu} \leq 2p_i^{-k_{N+1}}.$$

Thus from (9) we see that, for d = total degree of f,

$$|C_{(i_0)}| \leq \sum_{(i)\neq(i_0)} |C_{(i)}| 2^d \left(\frac{a_{(i_0)}}{a_{(i)}}\right)^{k_{N+1}} \to 0 \quad (N \to \infty).$$

Hence $C_{(i_0)} = 0$ and we see $f \equiv 0$, as desired.

The proof of Lemma 6 will be deferred until we show the impossibility of (5).

Set $X_N = (\sum_{\nu=1}^{N} p^{-k_\nu}, \sum_{\nu=1}^{N} p_2^{-k_\nu})$. Then by Lemma 6(a)

$$X_N = (N + \alpha_{1N}, N + \alpha_{2N})$$

where $\lim_{N\to\infty} \alpha_{iN} = \alpha_i$ exists in $\mathbf{Q}_P$. Set

$$R(x_1, x_2) = x_1 - x_2 - \alpha_1 + \alpha_2.$$

There is an integer l such that

$$Q(x_1, x_2) = R(x_1, x_2)^l Q_1(x_1, x_2)$$

such that $R \nmid Q_1$. From (5)

$$|Q(X_N)|_P = |R(X_N)|_P^l |Q_1(X_N)|_P \leq P^{-k_N}.$$

By Lemma 6(b), for $N = N_j - 1$

$$|R(X_N)|_P = |(\alpha_{1N} - \alpha_1) - (\alpha_{2N} - \alpha_2)|_P$$

$$= \left| \sum_{\nu=N_j}^{\infty} (p_1^{-k_\nu} - p_2^{-k_\nu}) \right|_P$$

$$= C |k_{N_j}|_P.$$

Hence $|Q_1(X_N)|_P \leq (1/C) P^{-k_{N_j-1}} |k_{N_j}|_P^{-l} \to 0$ $(j \to \infty)$.

Now, by hypothesis, the sequence $X_N = (N + \alpha_{1N}, N + \alpha_{2N})$ $(N = N_j - 1)$ has an infinite number of distinct limit points. If X is one of them, then $R(X_N) \to 0$ and $Q_1(X_N) \to 0$ $(j \to \infty)$ implies $R(X) = Q_1(X) = 0$. Hence the polynomials R and Q_1 have an infinite number of distinct zeros in common. Since R is linear, hence irreducible, this implies that $R \mid Q_1$ violating the definition of Q_1. Thus (5) is impossible.

It remains only to prove Lemma 6.

Proof of Lemma 6. By Fermat's little theorem we may write

$$p_i^{P-1} = 1 + a_i P \quad (i = 1, 2). \tag{6}$$

For ν large write $k_\nu = (P-1)k'_\nu$. Then

$$|p_1^{-k_\nu} - p_2^{-k_\nu}|_P = |p_1^{k_\nu} - p_2^{k_\nu}|_P$$

$$= |(1 + a_1 P)^{k'_\nu} - (1 + a_2 P)^{k'_\nu}|_P$$

$$= \left| \sum_{\mu=1}^{k'_\nu} \binom{k'_\nu}{\mu} (a_1^\mu - a_2^\mu) P^\mu \right|_P. \tag{7}$$

Using the well-known [1; page 46] result that

$$|\mu!|_P = P^{-(\mu - s(\mu))/(P-1)}$$

where, if $\mu = s_0 + s_1 P + \cdots + s_t P^t$ with $0 \leq s_i < P$, $s(\mu) = s_0 + \cdots + s_t$; it is not hard to show that the first term in (7) dominates. Thus we conclude that

3. Proof of Theorem 1

We restrict ourselves to $n = 3$. So suppose that for all N sufficiently large

$$f\left(\sum_{\nu=1}^{N} p_1^{-k_\nu}, \sum_{\nu=1}^{N} p_2^{-k_\nu}, \sum_{\nu=1}^{N} p_3^{-k_\nu}\right) = 0$$

where f is a non-zero polynomial with integer coefficients. Write

$$f(x_1, x_2, x_3) = \sum_{j=0}^{d_3} Q_j(x_1, x_2)x_3^j$$

with $Q_j(x_1, x_2)$ polynomials with integer coefficients and $Q_{d_3}(x_1, x_2) \neq 0$, and $d_3 \geq 0$. As before, write $a_i/b_i = \sum_{\nu=1}^{N} p_i^{-k_\nu}$, $b_i = p_i^{k_N}$. Then

$$\begin{aligned}
0 &= p_3^{d_3 k_N} f\left(\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}\right) \\
&= \sum_{j=0}^{d_3} Q_j\left(\frac{a_1}{b_1}, \frac{a_2}{b_2}\right) a_3^j p_3^{(d_3-j)k_N} \\
&\equiv Q_{d_3}\left(\frac{a_1}{b_1}, \frac{a_2}{b_2}\right) a_3^{d_3} \pmod{P^{k_N}}.
\end{aligned}$$

Since $P \nmid a_3$ we obtain

$$Q_{d_3}\left(\frac{a_1}{b_1}, \frac{a_2}{b_2}\right) \equiv 0 \pmod{P^{k_N}}.$$

Set $Q = Q_{d_3}$. Thus we have a non-zero polynomial $Q(x_1, x_2)$ with integer coefficients such that for all N sufficiently large

$$Q\left(\sum_{\nu=1}^{N} p_1^{-k_\nu}, \sum_{\nu=1}^{N} p_2^{-k_\nu}\right) \equiv 0 \pmod{P^{k_N}}. \tag{5}$$

We will show that (5) is impossible. We will now work in the P-adic field $\mathbf{Q}_P$. Denote the P-adic integers by $\mathbf{Z}_p$ and the P-adic valuation by $|\cdots|_P$. We will require the following lemma.

Lemma 6.

(a) *For any integer p prime to P the series*

$$\sum_{\nu=1}^{\infty} (p^{-k_\nu} - 1)$$

converges in $\mathbf{Z}_P$.

(b) *For N_j as in Theorem 1 we have*

$$\left|\sum_{\nu=N_j}^{\infty} \left(p_1^{-k_\nu} - p_2^{-k_\nu}\right)\right|_P = C|k_{N_j}|_P$$

where C is a non-zero constant depending on p_1, p_2 and P.

References

[1] G. Bachman, Introduction to p-adic Numbers and Valuation Theory (Academic Press, New York, 1964).
[2] W.J. LeVeque, Topics in Number Theory (Addison Wesley, Reading MA, 1956).
[3] O. Perron, Über mehrfach transzendente Erwüterungen des natürlichen Rationalitütsbereichs. S.-B. Bayer. Akad. Wiss. H. 2 (1932) 79–86.
[4] W.M. Schmidt, Simultaneous approximation and algebraic independence of numbers, Bull. Amer. Math. Soc. 68 (1962) 475–478.