JOURNAL OF NUMBER THEORY 23, 279–284 (1986)

Algebraic p-adic Expansions

DAVID LAMPERT

Department of Mathematics, University of Michigan,
Ann Arbor, Michigan 48109

Communicated by H. L. Montgomery

Received January 1, 1984; revised December 20, 1984

We describe a theory p-adic expansions for algebraic p-adic numbers in which countable ordinal number index sets and p-adically nonconvergent expansions are needed. This theory is used to compute parts of the expansions of the p^nth roots of unity and to answer a question of Koblitz [1] about transcendence degrees.

We shall use the following notation. Let $\mathbb{Q}_p$ be the p-adic completion of $\mathbb{Q}$ for a prime p, a field of cardinality $2^{\aleph_0}$. Let $\bar{\mathbb{Q}}_p$ be the algebraic closure of $\mathbb{Q}_p$, and let $\mathbb{C}_p$ be its p-adic completion, which is an algebraically closed complete field with a valuation uniquely extended from $\mathbb{Q}_p$ and is also of cardinality $2^{\aleph_0}$. Let $D_p = \{z \in \mathbb{C}_p\colon |z| \leqslant 1\}$. Let $\mathbb{Q}_p^{\text{unram}}$ be the field consisting of the set of $x \in \overline{\mathbb{Q}_p}$ such that the ring extension $\mathbb{Q}_p \cap D_p \subset \mathbb{Q}_p(x) \cap D_p$ is unramified. Let $\mathbb{C}_p^{\text{unram}}$ be the p-adic completion of $\mathbb{Q}_p^{\text{unram}}$, considered as a subfield of $\mathbb{C}_p$. Let $1^{1/n}$ denote any primitive nth root of unity in $\mathbb{C}_p$.

We choose in $\mathbb{C}_p$ one of each rational power of p which together compose a multiplicative group $p^{\mathbb{Q}}$, and consider these choices to be fixed throughout this paper. We introduce the field of *p-adic ordinal series* (or "p-adic Malcev–Neumann series") which are formal sums $\sum \zeta_i p^{r_i}$, where the ζ_i's are roots of unity in $\mathbb{C}_p$ of order prime to p (i.e., among representatives for $\mathbb{F}_p^*$), and $\{r_i\}$ is a well-ordered subordered-set of $\mathbb{Q}$. We let an ordinal number i index the term whose preceding terms are ordered by i. If $x = \sum \zeta_j p^{r_j}$, then we let $x_i = \sum_{j<i} \zeta_j p^{r_j}$ denote an *initial sum*. One checks by transfinite induction that the field operations analogous to those of $\mathbb{Q}_p$ are well defined and that this field is complete non-archimedean valued.

We now define (using the axiom of choice) an embedding of $\overline{\mathbb{Q}_p}$ into the field of p-adic ordinal series which extends the inclusion of $p^{\mathbb{Q}}$ and the obvious embedding of $\mathbb{Q}_p$ given by p-adic expansion. We successively extend the embedding through a chain of finite field extensions; we continue the argument only for the first extension $\mathbb{Q}_p \subset \mathbb{Q}_p(x)$. Let $f(t)$ be the minimal polynomial of x over $\mathbb{Q}_p$. To determine the p-adic expansion of x,

0022-314X/86 $3.00

we inductively add terms $\zeta_i p^{r_i}$ so that $|f(x_i+\zeta_i p^{r_i})| < |f(x_i)|$, which implies that the initial sum x_{i+1} is closer than x_i to at least one root of $f(t)$ in the field of p-adic ordinal series. Thus, if an initial sum x_i of the p-adic expansion of x has been defined, then the next term in the expansion is determined by writing

$$f(x_i+\zeta p^r)=f(x_i)+(\zeta p^r)\,f'(x_i)+\cdots+(\zeta p^r)^d\,\frac{f^{(d)}(x_i)}{d!} \qquad (1)$$

and then choosing r_i and ζ_i for r and ζ so that the first term in the p-adic expansion of $f(x_i)$ is canceled modulo one higher power of p by the first terms in the p-adic expansions of the other summands on the right side of (1) which have lowest valuation. This method of determining expansions by using Taylor developments can be used to show that the field of p-adic ordinal series is algebraically closed.

We now illustrate this method by computing part of the 2-adic expansion of $1^{1/4}$. Then $f(t)=t^2+1$ in this illustration. Let $\zeta_0=1$, $r_0=0$, and $x_1=1$. Then $x_2=1+\zeta_1 2^{r_1}$, and

$$f(1+\zeta 2^r)=2+(\zeta 2^r)(2)+(\zeta 2^r)^2(1),$$

so we choose $r_1=1/2$, $\zeta_1=1$, whence $f(x_2)\equiv 2^{3/2}$ (modulo higher powers). Then $x_3=x_2+\zeta_2 2^{r_2}$, and $f(x_2+\zeta 2^r)\equiv 2^{3/2}+(\zeta 2^r)(2)+(\zeta 2^r)^2(1)$ (modulo higher powers), so we choose $r_2=3/4$, $\zeta_2=1$, whence $f(x_3)\equiv 2^{7/4}$ (modulo higher powers). Continuing, we see that $x_\omega=1+2^{1/2}+2^{3/4}+2^{7/8}+\cdots$, with $f(x_\omega)\equiv 2^2$ (modulo higher powers), where ω is the first infinite ordinal number. Then $x_{\omega+1}=x_\omega+\zeta_\omega 2^{r_\omega}$, and $f(x_\omega+\zeta 2^r)\equiv 2^2+\zeta 2^{1+r}+\zeta^2 2^{2r}$ (modulo higher powers), so we choose $r_\omega=1$ and $\zeta_\omega^2+\zeta_\omega+1=0$. Therefore, we have

$$1^{1/4}=1+2^{1/2}+2^{3/4}+2^{7/8}+\cdots+\zeta_\omega 2+\cdots,$$

where ζ_ω is a primitive cube root of unity. It follows that for $n\geqslant 2$,

$$1^{1/2^n}=1+2^{1/2^{n-1}}+2^{3/2^n}+2^{7/2^{n+1}}+\cdots.$$

Next we describe our results on the expansions of the p^nth roots of unity for $p>2$.

THEOREM 1. *For* $p>2$,

$$1^{1/p}\equiv 1+\zeta_1 p^{1/(p-1)}+\zeta_2 p^{2/(p-1)}+\cdots+\zeta_{p-2}p^{(p-2)/(p-1)}$$

(modulo p*), where* $\zeta_1=(-1)^{1/(p-1)}$, $\zeta_2\equiv\zeta_1^2/2 \pmod p$, *and* $\zeta_{k+1}=\zeta_k^2/\zeta_1$ *for* $2\leqslant k\leqslant p-3$. *Furthermore,*

$$1^{1/p^2}=1+\zeta_1 p^{r_1}+\zeta_2 p^{r_2}+\cdots,$$

where $r_1=1/p(p-1)$ *and* $r_{i+1}=(1+r_i)/p$ *for* $i\geqslant 1$.

Proof. To prove the first statement we use the Taylor developments of $f(t)=t^{p-1}+t^{p-2}+\cdots+1$ and its derivatives to keep track of the valuation of $f^{(k)}(x_i)/k!$ for all k, and the fact that $f^{(k)}(1)/k!=\binom{p-1}{k}+\binom{p-2}{k}+\cdots+\binom{k+1}{k}+1=\binom{p}{k+1}$.

To prove the second statement we again analyze Taylor developments of the minimal polynomial $f(t)=(t^{p^2}-1)/(t^p-1)$ and its derivatives. We use

LEMMA 1. *For $p>2$,*

$$\begin{array}{lrl}
\text{(i)} & \operatorname{ord}_p f^{(k)}(1)/k! = 1 & (k=0),\\
\text{(ii)} & >1 & (1\leqslant k<p),\\
\text{(iii)} & =1 & (k=p),\\
\text{(iv)} & \geqslant 1 & (p<k<p^2-p),\\
\text{(v)} & =0 & (k=p^2-p).
\end{array}$$

Proof. (Suggested by D. W. Masser). As $f(1)=p$ and $f^{(p^2-p)}(1)=(p^2-p)!$, both (i) and (v) are clear. Also we have

$$f(y+1)=\frac{(y+1)^{p^2}-1}{(y+1)^p-1}\equiv\frac{y^{p^2}}{y^p}\equiv y^{p^2-p}\ (\mathrm{mod}\ p),$$

wich gives (iv). Next we note that

$$\begin{aligned}
k!\binom{rp}{k}&=rp(rp-1)\cdots(rp-k+1)\\
&=(-1)^{k-1}(k-1)!\,rp+(-1)^{k-2}r^2\sigma_k p^2+0\ (\mathrm{mod}\ p^3),
\end{aligned}$$

where σ_k is the $(k-2)$th symmetric function of $1, 2, \dots, k-1$. For $1\leqslant k<p$ we get

$$\begin{aligned}
k!\sum_{r=0}^{p-1}\binom{rp}{k}&=(-1)^{k-1}(k-1)!\,p\sum_{r=0}^{p-1}r+0\ (\mathrm{mod}\ p^2)\\
&=\tfrac{1}{2}(-1)^{k-1}(k-1)!\,p^2(p-1)+0\ (\mathrm{mod}\ p^2)=0\ (\mathrm{mod}\ p^2),
\end{aligned}$$

so that

$$\frac{f^{(k)}(1)}{k!}=\sum_{r=0}^{p-1}\binom{rp}{k}=0\ (\mathrm{mod}\ p^2).$$

For $k=p$ the same calculation gives

$$\begin{aligned}
p!\sum_{r=0}^{p-1}\binom{rp}{p}&=\tfrac{1}{2}(-1)^{p-1}(p-1)!\,p^2(p-1)+(-1)^{p-2}p^2\sigma_p\sum_{r=0}^{p-1}r^2\\
&\quad+0\ (\mathrm{mod}\ p^3).
\end{aligned}$$

But $\sigma_p \equiv 0 \pmod{p}$ because $(x-1)(x-2)\cdots(x-(p-1)) \equiv x^{p-1}-1 \pmod{p}$, so we get $f^{(p)}(1)/p! = \sum_{r=0}^{p-1} \binom{rp}{p} = -\frac{1}{2}p + 0 \pmod{p^2}$. Thus Lemma 1 and Theorem 1 are proved.

It follows from Theorem 1 that the initial exponents in the expansion of $1^{1/p^n}$ for $n \geqslant 2$ are r_i/p^{n-2}.

We now note some properties of the expansions of algebraic p-adic numbers. If $x \in \bar{\mathbb{Q}}_p$ and $x = \sum \zeta_i p^{r_i}$, then since x has only finitely many conjugates over $\mathbb{Q}_p$, we have $\{r_i\} \subset (1/Np^{\infty})\mathbb{Z}$ for some N, and the residue classes of the ζ_i's lie in $\mathbb{F}_q$ for some q. If $x \in \bar{\mathbb{Q}}_p$ is such that the ring extension $\mathbb{Q}_p \cap D_p \subset \mathbb{Q}_p(x) \cap D_p$ is tamely ramified, then by induction on i, x is closer to x_i than are all conjugates of x_i, so that $x_i \in \mathbb{Q}_p(x)$ by Krasner's lemma. Hence all terms $\zeta_i p^{r_i}$ in the expansion of x belong to $\mathbb{Q}_p(x)$ and $\{r_i\} \subset (1/e)\mathbb{Z}$ where e is the ramification index of $\mathbb{Q}_p(x) \cap D_p$ over $\mathbb{Q}_p \cap D_p$. For example, $\mathbb{Q}_p(1^{1/p}) = \mathbb{Q}_p((-p)^{1/(p-1)})$. More generally, Krasner's lemma and Theorem 1 imply that for any $x \in \bar{\mathbb{Q}}_p$, all terms in the expansion of x, before the first one which has a wild exponent and is succeeded by a term whose exponent is $\leqslant 1/(p-1)$ plus that wild exponent, belong to $\mathbb{Q}_p(x)$.

We next show that the exponents in the expansion of $x \in \bar{\mathbb{Q}}_p$ can accumulate only at rational numbers. This follows from

THEOREM 2. *The field of all ordinal series $\sum \zeta_i p^{r_i}$ such that all accumulation values of $\{r_i\}$ are rational is algebraically closed.*

Proof. Let $f(t)$ be a polynomial over this field of degree d, and let $r_{A_1}, r_{A_2}, \ldots,$ be a bounded increasing sequence of exponents occurring in the expansion of a root of f. By induction on d, we may assume that for all $k \geqslant 1$, the first two terms in the expansion of $f^{(k)}(x_{A_i})$ are constant for large i, for otherwise the x_{A_i}'s (and hence the x_{A_i+1}'s) would be initial sums for a root of a polynomial of lower degree. We shall use the Taylor formula

$$f(x+\zeta p^r) = f(x) + (\zeta p^r)\, f'(x) + \cdots + (\zeta p^r)^d \frac{f^{(d)}(x)}{d!}.$$

If the r_{A_i}'s were to approach an irrational limit L, then the limits of the valuations of the terms $(\xi_{A_i} p^{r_{A_i}})^k (f^{(k)}(x_{A_i})/k!)$ for $k \geqslant 1$ would be distinct. Hence there would be exactly one such term, say the kth, which cancels the first term in the expansion of $f(x_{A_i})$ at the A_ith inductive expansion step for all large i. Thus we would have $\lim_{i\to\infty} |f(x_{A_i})| = \lim_{i\to\infty} |(\zeta_{A_i} p^{r_{A_i}})^k (f^{(k)}(x_{A_i})/k!)|$, and for all large i the valuation of $f(x_{A_i} + \zeta_{A_i} p^{r_{A_i}})$ would be that of the first uncanceled term in the expansion of $f(x_{A_i})$ because of the assumption that the first two terms in the expansion of $f^{(k)}(x_{A_i})$ remain constant for large i. Thus there would be an N such that for all $i \geqslant N$ the valuation of $f(x_{A_i} + \zeta_{A_i} p^{r_{A_i}})$ is one of the exponents in the expansion of $f(x_{A_N})$, and hence $\lim_{i\to\infty} \operatorname{ord}(f(x_{A_i}+\zeta_{A_i}p^{r_{A_i}}))= kL+\operatorname{ord}(f^{(k)}(x_{A_N})/k!)$ would belong to the set of accumulation values of the exponents in the expansion of $f(x_{A_N})$. By transfinite induction on $\sup A_i$, L would be rational, and this contradiction proves the theorem.

Moreover, if $x \in \bar{\mathbb{Q}}_p$ and A is a countable ordinal number, then there exist positive integers M and N such that $r_{A+i} \in 1/Np^{Mi}\,\mathbb{Z}$ for all finite numbers i, because the proof of Theorem 2 shows by induction on A that the denominators of r_{A+i} grow at most exponentially with i.

We now pose some open questions: Which countable ordinal number is needed to index the expansion of the p^nth root of unity? Which countable ordinal numbers are needed for all $x \in \bar{\mathbb{Q}}_p$?

The theory of algebraic T-adic expansions applies to $k((T))$. When k is a field of characteristic zero, the algebraic closure of $k((T))$ is the field of "Puiseux expansions" $\bigcup_{[L:k]<\infty} \bigcup_{n=1}^{\infty} L((T^{1/n}))$. This is true because $\bar{k}$ has primitive roots of unity of all orders, so that if the denominators of the exponents of an algebraic ordinal series were unbounded, then so would be its number of conjugates over $k((T))$ in the field of T-adic ordinal series over $\bar{k}$; similarly, the coefficients of an algebraic ordinal series lie in a finite extension of k. On the other hand, if k is a field of characteristic p, then the roots of $x^p-x-T^{-1}=0$ are $x=T^{-1/p}+T^{-1/p^2}+T^{-1/p^3}+\cdots+\zeta$, $\zeta\in\mathbb{F}_p$; the theory of algebraic expansions over $k((T))$ is then similar to the theory of algebraic p-adic expansions. The theory of algebraic expansions might also apply to other complete noetherian regular local rings, but the expansions would depend on the choice of a set of representatives for the residue field and on the choice of an ordered list $(x_1, ..., x_n)$ of generators of the maximal ideal (one successively expands x_k-adically).

We conclude this paper by proving the following theorem which answers a question of Koblitz [1].

THEOREM 3. *The transcendence degree of* $\mathbb{C}_p^{\text{unram}}$ *over* $\mathbb{Q}_p$ *is* $2^{\aleph_0}$, *and the transcendence degree of* $\mathbb{C}_p$ *over* $\mathbb{C}_p^{\text{unram}}$ *is* $2^{\aleph_0}$.

The following lemma will be useful.

LEMMA 2. *For all fields* F *and groups* G *such that* $\mathbb{F}_p \subset F \subset \bar{\mathbb{F}}_p$ *and* $\mathbb{Z} \subset G \subset \mathbb{Q}$, *there exists* $x \in \mathbb{C}_p$ *such that the valuation group of* $\mathbb{Q}_p(x)$ *is* G *and the residue field of* $\mathbb{Q}_p(x) \cap D_p$ *is* F.

Proof. Write F as an increasing union of finite fields, $F=\bigcup_{j=1}^{\infty} F_j$, and write G as an increasing union of subgroups of $\mathbb{Q}$ containing $\mathbb{Z}$ with finite index, $G=\bigcup_{j=1}^{\infty} G_j$. Then successively add terms ζp^r in the rapidly convergent p-adic expansion of x which have $\zeta \in F$ and $r \in G$, in such a way that the valuation group of $\mathbb{Q}_p(x)$ contains the next desired G_j, or that the residue field of $\mathbb{Q}_p(x) \cap D_p$ contains the next desired F_j. This can be done as follows: To ensure that the valuation group of $\mathbb{Q}_p(x)$ contains the next desired G_j, add a term of the form p^r with suitable r generating G_j; to ensure that the residue field of $\mathbb{Q}_p(x) \cap D_p$ contains the next desired F_j, add a term of the form ζp^r with suitable ζ generating F_j and $r \in \mathbb{Z}$. In either case r is chosen sufficiently large (and larger than one plus the previous exponent in the expansion of x) by the following procedure: Let f be the minimal polynomial over $\mathbb{Q}_p$ of the already defined initial sum x_i, and use the Taylor formula

$$\begin{aligned} f(x) = f(x_i + \zeta p^r + \cdots) &= f'(x_i)(\zeta p^r + \cdots) \\ &+ \frac{f''(x_i)}{2}(\zeta p^r + \cdots)^2 + \cdots \end{aligned}$$

to decide how small to make the next term ζp^r so that its r or ζ belongs to the valuation group or residue field of $\mathbb{Q}_p(x)$. Thus Lemma 2 is proved.

Proof of Theorem 3. By Lemma 2, for any subset S of the primes there exists $x_S \in \mathbb{C}_p^{\text{unram}}$ such that the residue field of $\mathbb{Q}_p(x_S) \cap D_p$ is the field generated by $\bigcup_{q \in S, n \geqslant 1} \mathbb{F}_{p^{q^n}}$. Let $\mathbb{N}$ be the set of positive integers, let ϕ: $\mathbb{N} \to \{\text{primes}\}$ be a bijection, let $\{n_i\}$ be any infinite subset of $\mathbb{N}$ listed in increasing order, and take correspondingly $S = \{\phi(\phi(n_1)), \phi(\phi(n_1)\,\phi(n_2)), \phi(\phi(n_1)\,\phi(n_2)\,\phi(n_3)), \ldots\}$. There are $2^{\aleph_0}$ such subsets $\{n_i\}$, hence $2^{\aleph_0}$ corresponding S. These x_S are algebraically independent over $\mathbb{Q}_p$, because the residue field extension corresponding to $\mathbb{Q}_p(x_{S_1}, \ldots, x_{S_m}) \subset \mathbb{Q}_p(x_{S_1}, \ldots, x_{S_{m+1}})$ is infinite when $S_1, \ldots, S_{m+1}$ are distinct since $S_{m+1} \not\subset S_1 \cup \cdots \cup S_m$. Thus tr. deg. $(\mathbb{C}_p^{\text{unram}}/\mathbb{Q}_p) \geqslant 2^{\aleph_0}$, and the reverse inequality follows from card. $(\mathbb{C}_p) = 2^{\aleph_0}$. The statement tr. deg. $(\mathbb{C}_p/\mathbb{C}_p^{\text{unram}}) = 2^{\aleph_0}$ is proved similarly by using valuation groups generated by $\bigcup_{q \in S, n \geqslant 1} (1/q^n)\,\mathbb{Z}$. Thus Theorem 3 is proved.

Reference

1. N. Koblitz, "*P*-adic Number Theory, *P*-adic Analysis, and Zeta Functions," G.T.M. Vol. 58, Springer-Verlag, New York, 1977.