Invent. math. 77, 1-23 (1984)

Inventiones mathematicae

The rationality of the Poincaré series associated to the *p*-adic points on a variety

J. Denef

Department of Mathematics, University of Leuven, Celestijnenlaan 200 B, B-3030 Heverlee, Belgium

§ 1. Introduction

Let p denote a fixed prime number, $\mathbb{Z}_p$ the ring of p-adic integers, and Q_p the field of p-adic numbers. We denote the set of m-tuples of elements of $\mathbb{Z}_p$ (resp. Q_p) by $\mathbb{Z}_p^m$ (resp. Q_p^m).

Let $f_1(x), \ldots, f_r(x)$ be polynomials in m variables $x=(x_1, \ldots, x_m)$ over $\mathbb{Z}_p$. For $n \in \mathbb{N}$, let $\tilde{N}_n$ be the number of elements in the set

$$\{x \bmod p^n \mid x \in \mathbb{Z}_p^m \text{ and } f_i(x) \equiv 0 \bmod p^n, \text{ for } i=1, \ldots, r\},$$

and let N_n be the number of elements in the set

$$\{x \bmod p^n \mid x \in \mathbb{Z}_p^m \text{ and } f_i(x)=0, \text{ for } i=1, \ldots, r\}.$$

To these data one can associate the following Poincaré series

$$\tilde{P}(T)=\sum_{n=0}^{\infty} \tilde{N}_n T^n, \qquad P(T)=\sum_{n=0}^{\infty} N_n T^n,$$

Borewicz and Šhafarevič [6, p. 63] conjectured that $\tilde{P}(T)$ is a rational function of T. This was proved by Igusa [15, 16], in the case $r=1$, using Hironaka's resolution of singularities. Subsequently Meuser [22] proved the conjecture for arbitrary r, by adapting Igusa's method. In this paper we will give a different proof (see § 7) of the rationality of $\tilde{P}(T)$, which does not use resolution of singularities.

Recently Serre [28, § 3] and Oesterlé [24] investigated the behaviour of N_n for $n \to \infty$, and they asked the question whether $P(T)$ is a rational function of T. In this paper we prove

1.1. Theorem. *$P(T)$ is a rational function of T.*

The proof of Theorem 1.1 runs as follows: First we express $P(T)$ as an integral over a certain subset D of $\mathbb{Z}_p^{m+1}$ (Lemma 3.1). From a theorem of

Macintyre [21], on the elimination of quantifiers for Q_p (see § 2) it follows that D is a boolean combination of rather simple subsets of $\mathbb{Z}_p^{m+1}$. The integral over such a subset is then evaluated (Theorem 3.2) by Igusa's method [16], using resolution of singularities.

In § 4 we consider some generalizations. In § 5 we prove the rationality of the two-variable Poincaré series $P(T, U)$ associated to the number of solutions mod p^n which can be lifted to solutions mod p^{n+j}. The denominator of $P(T, U)$ has a particular simple form.

Section 6 contains a result on the absolute value of a definable function, which will be used in § 7, and an application to the p-adic distance from a point to a variety.

In § 7 we give a different proof for the rationality of $\tilde{P}(T)$, $P(T)$ and $P(T, U)$ which does not use resolution of singularities. This proof (even for $\tilde{P}(T)$) heavily relies on Macintyre's Theorem [21] on the elimination of quantifiers for Q_p, and uses a partition (Theorem 7.3) which is similar to and completely inspired by P.J. Cohen's Cell Decomposition [7, p. 140].

The special case of a curve $f(x_1, x_2)$ has been investigated by Driggs [9], Igusa [17], Meuser [23], and Strauss [29] for $\tilde{P}(T)$, and by Bollaerts [5] for $P(T)$.

I am grateful to D.J. Lewis, D. Meuser, and N. Schappacher for stimulating conversations and for providing me with useful information. I also want to thank L. Bröcker for pointing out a simplification in the proofs.

§ 2. Elimination of quantifiers

We consider the following three kinds of subsets of Q_p^m:

A subset of Q_p^m of *type I* is of the form

$$\{x \in Q_p^m \mid f(x) = 0\},$$

for some $f \in \mathbb{Z}_p[x_1, \ldots, x_m]$.

A subset of Q_p^m of *type II* is of the form

$$\{x \in Q_p^m \mid \operatorname{ord}(f(x)) \geqq \operatorname{ord}(g(x))\},$$

for some $f, g \in \mathbb{Z}_p[x_1, \ldots, x_m]$. Here ord denotes the p-adic valuation on Q_p (using the convention that $\operatorname{ord}(0) = +\infty$).

A subset of Q_p^m of *type III* is of the form

$$\{x \in Q_p^m \mid \exists\, y \in Q_p\colon f(x) = y^n\},$$

for some $n \in \mathbb{N}$, $n \geqq 2$, and $f \in \mathbb{Z}_p[x_1, \ldots, x_m]$.

Lemma 2.1. *A subset of Q_p^m, which is of type I or II, is also of type III.*

Proof. We have that $f(x) = 0$ iff $p(f(x))^2$ is a square. Moreover, if $p \neq 2$, then $\operatorname{ord}(f(x)) \geqq \operatorname{ord}(g(x))$ iff

$$\exists\, y \in Q_p\colon (g(x))^2 + p(f(x))^2 = y^2.$$

If $p=2$, then $\operatorname{ord}(f(x)) \geqq \operatorname{ord}(g(x))$ iff

$$\exists\, y \in Q_p\colon\ (g(x))^2 + 8(f(x))^2 = y^2. \qquad \text{Q.E.D.}$$

A *boolean combination* of subsets of Q_p^m of type III is a subset which is obtained by taking intersections, unions and complements (a finite number of times) of subsets of Q_p^m of type III.

We can now state Macintyre's Theorem [21] on the elimination of quantifiers for Q_p:

2.2. Theorem. *Let S be a boolean combination of subsets of Q_p^{m+q} of type III. Then the set*

$$\{x \in Q_p^m \mid \exists\, y \in Q_p^q\colon (x, y) \in S\}$$

is a boolean combination of subsets of Q_p^m of type III.

Historical note. An elimination of quantifiers for Q_p was first obtained by Ax and Kochen [2, III]. Their result differs from Macintyre's in that it uses subsets of a more general type. Their proof is based on the model theory of valued fields which was developped by Ax and Kochen [2, 20] and Ersov [10, 11].

Subsequently P.J. Cohen [7] gave an elementary (but very ingenious) proof. Cohen's work has been generalized by Weispfenning [31]. Only much later came Macintyre's Theorem [21] which we stated above. Macintyre's proof is based on the results of Ax and Kochen and Ersov. Recently Prestel and Roquette [26, p. 91], have given a selfcontained proof of Macintyre's Theorem and generalized it to finite field extensions of Q_p. Their proof uses model theory. Currently Weispfenning is preparing a paper [32] which will contain an elementary proof of Macintyre's Theorem in a more general setting.

Remarks. It is known (see e.g. [21]) that Theorem 2.2 becomes false if one only works with boolean combinations of subsets of type I and II. Many of the results of Ax and Kochen, and Ersov fail for local fields of characteristic $p \neq 0$, but the situation there is not yet well understood (see Delon [8]).

§ 3. Proof of Theorem 1.1

For $a \in Q_p$, let $|a| = p^{-\operatorname{ord}(a)}$. Let $|dx| = |dx_1|\,|dx_2| \ldots |dx_m|$ be the Haar measure on Q_p^m such that the measure of $\mathbb{Z}_p^m$ is 1. Let $f_1(x), \ldots, f_r(x)$ with $x = (x_1, \ldots, x_m)$ be as in § 1.

For $s \in \mathbb{R}$, $s > 0$, we consider

$$I(s) = \int_D |w|^s\, |dx|\, |dw|,$$

where

$$D = \{(x, w) \in \mathbb{Z}_p^m \times \mathbb{Z}_p \mid \exists\, y \in \mathbb{Z}_p^m\colon x \equiv y \bmod w, \text{ and } f_i(y) = 0, \text{ for } i = 1, \ldots, r\}.$$

Let $P(T)$ be the Poincaré series of § 1.

3.1. Lemma. *With the above notation, we have*

$$I(s)=\frac{p-1}{p}P(p^{-m-1}p^{-s})$$

Proof.

$$\begin{aligned}
I(s)&=\sum_{n=0}^{\infty}\int_{\substack{D\\ \mathrm{ord}(w)=n}}p^{-ns}|dx|\,|dw|\\
&=\sum_{n=0}^{\infty}p^{-ns}\int_{\substack{(x,p^n)\in D\\ \mathrm{ord}(w)=n}}|dx|\,|dw|\\
&=\sum_{n=0}^{\infty}p^{-ns}\Big(\int_{(x,p^n)\in D}|dx|\Big)\Big(\int_{\mathrm{ord}(w)=n}|dw|\Big)\\
&=\sum_{n=0}^{\infty}p^{-ns}\frac{N_n}{p^{nm}}\left(\frac{1}{p^n}-\frac{1}{p^{n+1}}\right)\\
&=\frac{p-1}{p}\sum_{n=0}^{\infty}N_n(p^{-s}p^{-m-1})^n.\quad\text{Q.E.D.}
\end{aligned}$$

Thus to prove Theorem 1.1 we have to show that $I(s)$ is a rational function of p^{-s}. From Lemma 2.1 and Theorem 2.2 it follows that D is a boolean combination of subsets of Q_p^{m+1} of type III. Thus Theorem 1.1 reduces to

3.2. Theorem. *Let S be a boolean combination of subsets of Q_p^m of type III. Suppose that S is contained in a compact subset C of Q_p^m. Let $g\in Q_p[x]$, where $x=(x_1,\ldots,x_m)$. Then*

$$Z(s)=\int_S|g(x)|^s|dx|$$

is a rational function of p^{-s}.

In the special case that $S=\mathbb{Z}_p^m$, this is due to Igusa [15, 16]. A related integral in the archimedian case has been investigated by Atiyah [1], Bernstein-Gel'fand [4], and Bernstein [3].

Proof. We calculate $Z(s)$ by applying Igusa's method [16]. S can be written as a union of intersections of subsets which are of type III or the complement of one such.

Since $\int_{A\cup B}=\int_A+\int_B-\int_{A\cap B}$, we may suppose that S is the set of all $x\in Q_p^m$ satisfying the following conditions

(1) $\qquad f_j(x)$ is (is not) an n_j-th power in Q_p, $\quad j=1,2,\ldots,q$,

where $f_j\in\mathbb{Z}_p[x]\setminus\{0\}$, and $n_j\in\mathbb{N}$, $n_j\geqq 2$. Let $f=\left(\prod_{j=1}^{q}f_j\right)g$. Applying Hironaka's Embedded Resolution of Singularities [14, p. 176] to the locus $f=0$, one obtains a Q_p-analytic manifold Y, and a proper Q_p-analytic map $h\colon Y\to Q_p^m$, with the following properties: For every $b\in Y$ there exist local coordinates y

$=(y_1, \ldots, y_m)$ centered at b such that, locally around b, we have

$$f \circ h = \varepsilon \prod_{i=1}^{m} y_i^{N_i},$$

and

$$h^*(dx_1 \wedge \ldots \wedge dx_m) = \eta \left(\prod_{i=1}^{m} y_i^{\nu_i - 1} \right) dy_1 \wedge \ldots \wedge dy_m,$$

with N_i, $\nu_i \in \mathbb{N}$, $\nu_i \geqq 1$, and with ε, η invertible Q_p-analytic functions in a neighbourhood of b (see [18, p. 84–87]).

Since the ring of germs of Q_p-analytic functions around b is a unique factorization domain, we have

$$f_j \circ h = \varepsilon_j \prod_{i=1}^{m} y_i^{N_{ji}}, \quad \text{for } j = 1, \ldots, q,$$

and

$$g \circ h = \gamma \prod_{i=1}^{m} y_i^{M_i},$$

in an open neighbourhood U of b, with N_{ji}, $M_i \in \mathbb{N}$, and $\varepsilon_j, \gamma, \eta$ invertible Q_p-analytic functions on U.

By making U smaller, if necessary, we may assume that $|\varepsilon_j|$, $|\gamma|$ and $|\eta|$ are all constant on U, and that $\varepsilon_j(y)/\varepsilon_j(b)$ is an n_j-th power in Q_p for all $y \in U$, $j = 1, \ldots, q$. Indeed every $z \in Q_p$, which is sufficiently close to 1, is an n_j-th power. We may also assume that U is compact. Since h is proper, $h^{-1}(C)$ is compact and can be covered by a finite number of compact open sets such as U. Let's call these $U_1, U_2, \ldots$. By replacing $U_1, U_2, U_3, \ldots$ by $U_1, U_2 \smallsetminus U_1, U_3 \smallsetminus (U_1 \cup U_2), \ldots$, we may suppose that they are disjoint. Then we obtain

$$Z(s) = \sum_U \int_{U \cap h^{-1}(S)} |\gamma|^s \left(\prod_{i=1}^{m} |y_i|^{M_i s} \right) |\eta| \left(\prod_{i=1}^{m} |y_i|^{\nu_i - 1} \right) |dy|.$$

Moreover, $U \cap h^{-1}(S)$ is the set of all $y \in U$ satisfying

(2) $\quad \varepsilon_j(b) \prod_{i=1}^{m} y_i^{N_{ji}}$ is (is not) an n_j-th power in Q_p, $\quad$ for $j = 1, \ldots, q$.

We identify each U with its image in the y-space, which is a compact open subset of Q_p^m. Thus each U is a finite disjoint union of sets of the form $a + p^e \mathbb{Z}_p^m$, with $a = (a_1, a_2, \ldots, a_m) \in Q_p^m$ and $e \in \mathbb{N}$. Thus to prove Theorem 3.2 it is sufficient to show that

$$J(s) = \int_V \left(\prod_{i=1}^{m} |y_i|^{M_i s + \nu_i - 1} \right) |dy|$$

is a rational function of p^{-s}, if V is the set of all $y \in a + p^e \mathbb{Z}_p^m$ which satisfy (2).

Let n be a common multiple of $n_1, \ldots, n_q$. Notice that condition (2) only depends on the n-th power residues of the y_i. Hence, summing over all the n-th power residues which satisfy (2), we may suppose that V is the set of all $y \in Q_p^m$ satisfying

$$y_i \in a_i + p^e \mathbb{Z}_p, \tag{3}$$

and

$$y_i = \lambda_i \cdot (\text{nonzero } n\text{-th power}), \tag{4}$$

for some $\lambda_i \in Q_p$, $i = 1, \ldots, m$. But then $J(s) = \prod_{i=1}^{m} I_i(s)$, with

$$I_i(s) = \int_{(3),(4)} |y_i|^{M_i s + \nu_i - 1} |dy_i|.$$

If $a_i \notin p^e \mathbb{Z}_p$, then (3) implies that $I_i(s)$ is equal to a constant times $|a_i|^{M_i s + \nu_i - 1}$. If $a_i \in p^e \mathbb{Z}_p$, then (3) is equivalent to $y_i \in p^e \mathbb{Z}_p$ and

$$I_i(s) = \sum_{k \geqq e} p^{-k(M_i s + \nu_i - 1)} \int_{\substack{\operatorname{ord} y_i = k \\ (4)}} |dy_i|.$$

Put $y_i = p^k u$, then

$$\int_{\substack{\operatorname{ord} y_i = k \\ (4)}} |dy_i| = p^{-k} \int_{\substack{\operatorname{ord} u = 0 \\ u = \lambda_i p^{-k} \cdot (n\text{-th power})}} |du|.$$

The last integral is zero unless $k \equiv \operatorname{ord} \lambda_i \bmod n$, and in that case its value γ is independent of k. Hence

$$I_i(s) = \gamma \sum_{\substack{k \geqq e \\ k \equiv \operatorname{ord} \lambda_i \bmod n}} p^{-k(M_i s + \nu_i)} = \frac{\gamma p^{-e'(M_i s + \nu_i)}}{1 - p^{-n(M_i s + \nu_i)}},$$

where e' is the smallest natural number satisfying $e' \geqq e$ and $e' \equiv \operatorname{ord} \lambda_i \bmod n$. Q.E.D.

3.3. Remark. From the above proof it also follows that $P(T)$ can be written as a polynomial in T divided by a product of factors of the form $(1 - p^a T^b)$, with $a, b \in \mathbb{N}$. (After cancellation, $a < 0$ cannot appear because $P(T)$ is a power series with integer coefficients). Moreover the poles of $P(T)$ have multiplicity at most m. (This will be proved in 6.8). The same facts hold for $\tilde{P}(T)$.

3.4. Remark. Let

$$J(s) = \int_{\mathbb{Z}_p^m} |f(x)|^s |dx|,$$

where $|f(x)| = \operatorname{Max}_i |f_i(x)|$. To prove the rationality of $\tilde{P}(T)$, Igusa [16, p. 415] (for $r = 1$) and Meuser [22, p. 310] (for $r > 1$) used the formula

$$\tilde{P}(p^{-m-s}) = \frac{1 - p^{-s} J(s)}{1 - p^{-s}} \tag{1}$$

(Later Oesterlé [25] showed that the rationality of $\tilde{P}(T)$ for $r>1$ can be reduced to the case $r=1$ by an elementary argument.)

§ 4. Some generalizations

We consider the first order language (in the sense of logic) built up from the symbols $+, \cdot, 0, 1, =, \wedge$ (and), $\vee$ (or), $\neg$ (not), and the quantifiers $\exists, \forall$. Let $\varphi(x)$ be a formula in this language with free variables $x=(x_1, \ldots, x_m)$. For $n \in \mathbb{N}$, let $\tilde{N}_{n,\varphi}$ be the number of elements in the set

$$\{x \in (\mathbb{Z}/p^n\mathbb{Z})^m \mid \varphi(x) \text{ is true in } \mathbb{Z}/p^n\mathbb{Z}\},$$

and let $N_{n,\varphi}$ be the number of elements in the set

$$\{x \bmod p^n \mid x \in \mathbb{Z}_p^m \text{ and } \varphi(x) \text{ is true in } \mathbb{Z}_p\}.$$

To these data we can associate the following Poincaré series

$$\tilde{P}_\varphi(T)=\sum_{n=0}^{\infty} \tilde{N}_{n,\varphi}\, T^n, \qquad P_\varphi(T)=\sum_{n=0}^{\infty} N_{n,\varphi}\, T^n.$$

4.1. Theorem. *$\tilde{P}_\varphi(T)$ and $P_\varphi(T)$ are rational functions of T.*
An analogous theorem for finite fields has been proved by Kiefe [19].

Proof. Let $\tilde{\varphi}(x, w)$ be obtained from $\varphi(x)$ by replacing every occurence of $=$ by $\equiv \bmod w$. Let

$$\tilde{D}_\varphi=\{(x,w) \in \mathbb{Z}_p^m \times \mathbb{Z}_p \mid \tilde{\varphi}(x,w) \text{ is true in } \mathbb{Z}_p\}$$

$$D_\varphi=\{(x,w) \in \mathbb{Z}_p^m \times \mathbb{Z}_p \mid \exists\, y \in \mathbb{Z}_p^m\colon\ x \equiv y \bmod w \text{ and } \varphi(y) \text{ is true in } \mathbb{Z}_p\}.$$

$$\tilde{I}_\varphi(s)=\int_{\tilde{D}_\varphi} |w|^s |dx|\,|dw|, \qquad I_\varphi(s)=\int_{D_\varphi} |w|^s |dx|\,|dw|.$$

Lemma 3.1 remains valid if we replace $I(s)$ by $\tilde{I}_\varphi(s)$ and P by $\tilde{P}_\varphi$, or if we replace $I(s)$ by $I_\varphi(s)$ and P by P_φ. By repeated application of Theorem 2.2 we see that $\tilde{D}_\varphi$ and D_φ are boolean combinations of subsets of Q_p^{m+1} of type III. We now apply Theorem 3.2. Q.E.D.

§ 5. Rationality of a two-variable Poincaré series

Let $f_1(x), \ldots, f_r(x)$ be polynomials in m variables $x=(x_1, \ldots, x_m)$ over $\mathbb{Z}_p$. Let $f=(f_1, \ldots, f_r)$. For $n, j \in \mathbb{N}$, let $N_{n,j}$ be the number of solutions in $\mathbb{Z}_p/p^n$ of $f \equiv 0 \bmod p^n$ which can be lifted to solutions of $f \equiv 0 \bmod p^{n+j}$. To these data we associate the Poincaré series

$$P(T,U)=\sum_{n,\, j \in \mathbb{N}} N_{n,j}\, T^n\, U^j.$$

5.1. Theorem. *$P(T, U)$ is a rational function of T and U, which can be written as*

$$P(T, U)=q(T, U)(1-U)^{-1} \prod_{i=1}^{e}(1-p^{a_i} T^{b_i} U^{c_i})^{-1}, \tag{1}$$

with $q(T, U)\in\mathbb{Z}[T, U]$, $a_i, b_i, c_i\in\mathbb{N}$, and $b_i\geqq 1$.

Moreover

$$P(t)=\lim_{u\to 1}(1-u)P(t, u),$$

if $t\in\mathbb{R}$ is close enough to zero.

Proof. Let

$$D=\{(x, w_1, w_2)\in\mathbb{Z}_p^m\times\mathbb{Z}_p\times\mathbb{Z}_p \mid \exists\, y\in\mathbb{Z}_p^m:\ x\equiv y \bmod w_1 \text{ and } f(y)\equiv 0 \bmod w_1\cdot w_2\},$$

and

$$I(s_1, s_2)=\int_D |w_1|^{s_1}|w_2|^{s_2}|dx|\,|dw_1|\,|dw_2|, \quad \text{for } s_1, s_2\in\mathbb{R},\ s_1, s_2>0.$$

Using the same argument as in Lemma 3.1, one easily gets

$$I(s_1, s_2)=\left(\frac{p-1}{p}\right)^2 P(p^{-m-1-s_1}, p^{-1-s_2}).$$

From Lemma 2.1 and Theorem 2.2 it follows that D is a boolean combination of subsets of type III. By adapting the proof of Theorem 3.2 in a straightforward way we obtain that $I(s_1, s_2)$ is a rational function of p^{-s_1} and p^{-s_2}, and that $P(T, U)$ is a rational function which can be written as a polynomial in T and U, divided by a product of factors of the form T, U or $(1-p^a T^b U^c)$, with $b, c\in\mathbb{N}$, $a\in\mathbb{Z}$. Because $P(T, U)$ is a power series with integer coefficients, we can write $P(T, U)$ as a polynomial in T and U, divided by a product of factors of the form $(1-p^a T^b U^c)$, with $a, b, c\in\mathbb{N}$. To write $P(T, U)$ in the more precise form (1) we need an additional argument. For fixed n, the sequence $N_{n,0}\geqq N_{n,1}\geqq\ldots$ stabilizes. Hence there exists $\beta(n)\in\mathbb{N}$ such that $N_{n,j}=N_n$ for $j\geqq\beta(n)$.

Let

$$R(T, U)=\sum_{n,j}(N_{n,j}-N_n)T^n U^j.$$

We have that $R(T, U)\in\mathbb{Z}[U][[T]]$, and

$$P(T, U)=R(T, U)+P(T)(1-U)^{-1}. \tag{2}$$

From Remark 3.3 and (2) it follows that $R(T, U)$ can be written as a polynomial divided by a product of factors of the form $1-p^a T^b U^c$, with $a, b, c\in\mathbb{N}$. Moreover we can take $b\geqq 1$, because $R(T, U)\in\mathbb{Z}[U][[T]]$. Indeed if an element of $\mathbb{Z}[T, U]$ is divisible by $1-p^a U^c$ in $\mathbb{Z}[U][[T]]$, then it is also divisible by $1-p^a U^c$ in $\mathbb{Z}[T, U]$. The Theorem now follows from (2). Q.E.D.

Next we discuss the relationship between Theorem 5.1 and a theorem of Greenberg [12]. For $n\in\mathbb{N}$, let $\gamma(n)$ be the smallest natural number $\geqq n$ which

satisfies the following: If $y \in \mathbb{Z}_p^m$ and $f(y) \equiv 0 \bmod p^{\gamma(n)}$, then there exists $x \in \mathbb{Z}_p^m$ such that $f(x)=0$ and $x \equiv y \bmod p^n$. (The existence of $\gamma(n)$ is clear because $\mathbb{Z}_p/p^n$ is finite.) Greenberg's theorem [12] states that $\gamma(n)$ can be bounded by a linear function of n. Thus there exist $c, d \in \mathbb{R}$ such that $\gamma(n) \leqq cn+d$ for all $n \in \mathbb{N}$. Schappacher [27] has investigated the infimum of the possible values for c, which is an invariant of the variety $f=0$. We will now prove

5.2. Proposition. *With the notation of* 5.1.(1), *suppose that none of the factors* $1-p^{a_i} T^{b_i} U^{c_i}$ *divides* $q(T, U)$ *in* $\mathbb{Z}[T, U]$. *Let* $c = 1 + \operatorname{Max}_i c_i/b_i$. *Then* c *is the smallest real number for which there exists* $d \in \mathbb{R}$ *such that* $\gamma(n) \leqq cn+d$ *for all* $n \in \mathbb{N}$.

Proof. For $n \in \mathbb{N}$, let $\beta(n)$ be the smallest natural number such that $N_{n,j} = N_n$ for $j \geqq \beta(n)$. It is clear that $\gamma(n) = n + \beta(n)$. Write

$$q(T, U) \prod_{i=1}^{e} (1-p^{a_i} T^{b_i} U^{c_i})^{-1} = \sum_{n=0}^{\infty} w_n(U) T^n, \tag{1}$$

with $w_n(U) \in \mathbb{Z}[U]$. We have

$$P(T, U) = \sum_{n=0}^{\infty} w_n(U) \left(\sum_{j=0}^{\infty} U^j \right) T^n.$$

Thus $N_{n,j}$ is equal to the sum of the coefficients of degree $\leqq j$ of $w_n(U)$. Hence $\beta(n) = \deg w_n(U)$. We may suppose that $c_1/b_1 = \operatorname{Max}_i c_i/b_i$. We have to prove that c_1/b_1 is the smallest real number such that $\deg w_n(U) \leqq n\, c_1/b_1 + O(1)$. From (1) it easily follows that $\deg w_n(U) \leqq n\, c_1/b_1 + O(1)$. Let $\lambda \in \mathbb{R}$, $\lambda < c_1/b_1$, and suppose that

$$\deg w_n(U) \leqq \lambda n + O(1). \tag{2}$$

We have to derive a contradiction. Write

$$q(T, U)(1-p^{a_1} T^{b_1} U^{c_1})^{-1} = \sum_{n=0}^{\infty} w'_n(U) T^n, \tag{3}$$

with $w'_n(U) \in \mathbb{Z}[U]$. From (1) and (2) follows

$$\deg w'_n(U) \leqq \lambda n + O(1). \tag{4}$$

Moreover from (3) follows

$$w'_{n+lb_1}(U) = (p^{a_1} U^{c_1})^l w'_n(U), \tag{5}$$

for all $n > n_0 = \deg_T q(T, U)$, and $l \in \mathbb{N}$. Using (5) to calculate the degree of $w'_{n+lb_1}(U)$, and comparing with (4), we contradict $\lambda < c_1/b_1$, unless $w'_n(U) = 0$ for all $n > n_0$. But then (3) implies that $1-p^{a_1} T^{b_1} U^{c_1}$ divides $q(T, U)$ in $\mathbb{Z}[T, U]$. Q.E.D.

5.3. Remark. Independently of the results of this section, but by using a refinement of Macintyre's Theorem which we will discuss in 6.4, one can show

the following: There exists a finite partition of $\mathbb{N}$ in congruence classes, such that on each such congruence class the function $n \mapsto \gamma(n)$ is linear for n big enough. This follows because the function $\gamma(n)$ is definable in the extended first order language introduced in 6.4.

5.4. Remark. For $j \leqq n$, let $N'_{n,j}$ be the number of solutions in $\mathbb{Z}_p/p^n$ of $f \equiv 0 \bmod p^n$ whose residue mod p^j can be lifted to a solution of $f=0$ in $\mathbb{Z}_p$. By the same argument as in 5.1 one sees that $P'(T,U)=\sum_{j \leqq n} N'_{j,n} T^n U^j$ is a rational function of T and U. Alternatively one can express $P'(T,U)$ in terms of the integral

$$\int_{\mathbb{Z}_p^m} |f(x)|^{s_1} d(x,V)^{s_2} |dx|,$$

where $d(x,V)$ is as in 6.6.

§ 6. The absolute value of a definable function

This section contains a result on the absolute value of a definable function (Corollary 6.5) which will be used in § 7. It also contains a result on the p-adic distance from a point to a variety (Corollary 6.6) which allows us to prove the rationality of $P(T)$ with less desingularization (Application 6.8). First we need some definitions.

6.1. Definition. A definable subset of Q_p^m *is a subset of the form* $\{x \in Q_p^m \mid \varphi(x)$ *is true*$\}$, *where* $\varphi(x)$ *is a formula in the first order language (in the sense of logic) built up from the following symbols:* $+$ *(addition),* $\cdot$ *(multiplication),* $|$ *(here* $x|y$ *means* $\operatorname{ord} x \leqq \operatorname{ord} y$*), for every element of* Q_p *a symbol denoting that element,* $=$, $\wedge$ *(and),* $\vee$ *(or),* $\neg$ *(not), and quantifiers* $\exists x$ *(there exists* $x \in Q_p$:*) and* $\forall x$ *(for every* $x \in Q_p$:*).*

From Lemma 2.1 and repeated application of Macintyre's Theorem 2.2 it follows that a subset of Q_p^m is definable if and only if it is a boolean combination of subsets of Q_p^m of type III. (Indeed the quantifier $\forall x$ can be written as $\neg(\exists x) \neg$.)

A definable function from Q_p^m to Q_p is a function whose graph is a definable subset of Q_p^{m+1}.

6.2. Definition. *A function* θ: $Q_p^m \to \mathbb{Z} \cup \{+\infty\}$ *is* simple *if there exists a finite partition of* Q_p^m *into definable subsets* A *such that on each* A

$$\theta(x)=\frac{1}{e} \operatorname{ord} \frac{f(x)}{g(x)}, \quad \text{for } x \in A,$$

where $e \in \mathbb{N}$, $e \neq 0$, $f(x) \in Q_p[x]$, $g(x) \in Q_p[x]$, *and* $g(x) \neq 0$ *for all* $x \in A$.

6.3. Theorem. *Let* S *be a definable subset of* Q_p^{m+1}. *Suppose that, for every* $x \in Q_p^m$, *the set* $\{\operatorname{ord} t \mid (x,t) \in S\}$ *consists of exactly one element which we will denote by* $\theta(x)$. *Then* $\theta(x)$ *is a simple function of* x.

Proof. Let $Z=\{x\in Q_p^m \mid (x,0)\in S\}$, and $\bar{Z}=Q_p^m-Z$. We have to prove that $\theta(x)$ is simple on $\bar{Z}$.

By Macintyre's Theorem 2.2 S is a boolean combination of subsets of type III. Let $f_j(x,t)$, $j=1,2,\ldots,l$, be the polynomials which appear in the description of these subsets. Let n_0 be a common multiple of all the n which appear in the description of these subsets of type III (in the notation of § 2).

Write

$$f_j(x,t)=a_{j0}(x)+a_{j1}(x)t+a_{j2}(x)t^2+\ldots,$$

with $a_{ji}\in Q_p[x]$. We partition $\bar{Z}$ in definable subsets A, such that for each A and for each j,i we have either

$$a_{ji}(x)=0 \quad \text{for all } x\in A, \tag{1}$$

or

$$a_{ji}(x)\neq 0 \quad \text{for all } x\in A. \tag{2}$$

There exists $\lambda\in\mathbb{N}$ such that any $u\in\mathbb{Z}_p$ with $u\equiv 1 \bmod p^\lambda$ is an n_0-th power. Let $j=1,\ldots,$ or l, let $\alpha\in\mathbb{Z}$, $|\alpha|<\lambda$, and let $i_1\neq i_2$ be such that a_{ji_1} and a_{ji_2} satisfy (2). Define

$$A_{j,\alpha,i_1,i_2}=\{x\in A \mid \exists t:(x,t)\in S \text{ and } \operatorname{ord}(a_{ji_1}(x)t^{i_1})=\operatorname{ord}(a_{ji_2}(x)t^{i_2})+\alpha\}.$$

$\theta(x)$ is a simple function on A_{j,α,i_1,i_2}, indeed for $x\in A_{j,\alpha,i_1,i_2}$ we have

$$\theta(x)=\operatorname{ord} t=\frac{1}{i_1-i_2}\operatorname{ord}\left(\frac{a_{ji_2}(x)p^\alpha}{a_{ji_1}(x)}\right),$$

because $t\neq 0$, since $x\notin Z$.

Let

$$B=A\setminus\bigcup A_{j,\alpha,i_1,i_2},$$

where the union is over all j,α,i_1,i_2 as above. We have to prove that $\theta(x)$ is simple on B. For all x,t with $x\in B$ and $(x,t)\in S$ the n_0-th power residue of $f_j(x,t)$ is equal to the n_0-th power residue of the term $a_{ji}(x)t^i$ of minimal order, because the orders of the terms differ by at least λ. Making a disjunction over the different possibilities of which term $a_{ji}(x)t^i$ has minimal order, at least λ less than the other terms, we obtain that for $x\in B$, the relation $(x,t)\in S$ is equivalent to a boolean combination of conditions of the form

$$\operatorname{ord} t^v\geqq\operatorname{ord}\frac{b_1(x)}{b_2(x)}, \tag{3}$$

and

$$b(x)t^\mu \text{ is an } n\text{-th power}, \tag{4}$$

with $b_1(x)$, $b_2(x)$, $b(x)\in Q_p[x]$, $v\in\mathbb{Z}$, $\mu\in\mathbb{N}$, $n\mid n_0$, and $b_1(x)\neq 0$, $b_2(x)\neq 0$ for all $x\in B$.

Making a disjunction over the different possibilities of the n_0-th power residues of t and of the $b(x)$ in (4), we obtain that for $x\in B$ the relation $(x,t)\in S$ is equivalent to a disjunction of conditions S_i, where each S_i is a conjunction

of conditions of the form (3) and definable conditions on x and one condition of the form

$$t=\rho\cdot(\text{non-zero } n_0\text{-th power}), \tag{5}$$

where $\rho\in Q_p$, $\rho\neq 0$.

Let $B_i=\{x\in B\mid\exists t\colon (x,t)\in S_i\}$. We have to prove that $\theta(x)$ is simple on B_i. For $x\in B_i$, and $\theta\in\mathbb{Z}$, we have $\theta=\theta(x)$ if and if only if θ satisfies a conjunction of conditions of the form

$$v\,\theta\geqq \operatorname{ord}\frac{b_1(x)}{b_2(x)}\,, \tag{3'}$$

and one condition

$$\theta\equiv\eta \bmod n_0, \tag{5'}$$

where $v, b_1(x), b_2(x)$ are as in (3), and $\eta=\operatorname{ord}\rho$.

The conjunction of the conditions (3') can be written as

$$\frac{1}{\gamma}\operatorname*{Max}_i \operatorname{ord} a_i(x)\leqq\theta\leqq\frac{1}{\gamma}\operatorname*{Min}_i \operatorname{ord} c_i(x),$$

with $a_i(x), c_i(x)\in Q_p(x)$, $\gamma\in\mathbb{N}$, $\gamma\neq 0$.

Write $\theta(x)=\eta+q(x)n_0$, then for $x\in B_i$ we have

$$q(x)=\left[\frac{(\operatorname*{Min}_i \operatorname{ord} c_i(x))-\eta\gamma}{\gamma n_0}\right],$$

where [ ] denotes the greatest integer function. We have to prove that $q(x)$ is simple on B_i. But this is clear, by covering B_i with definable subsets on which a particular $c_i(x)$ has minimal order and constant (γn_0)-th power residue (this implies that $\operatorname{ord} c_i(x) \bmod \gamma n_0$ is constant on such a subset). Q.E.D.

6.4. Remark. Theorem 6.3 can also be proved from the following refinement of Macintyre's Theorem 2.2: Q_p admits elimination of quantifiers[1] in the extended first order language with the following symbols: There are variables which run over Q_p and variables which run over $\mathbb{Z}$. There are symbols for $+$ and $\cdot$ in Q_p, and for $+$, $-$, and $\leqq$ in $\mathbb{Z}$, and for the function ord from $Q_p\setminus\{0\}$ to $\mathbb{Z}$. For every element of Q_p or $\mathbb{Z}$ there is a symbol to denote that element. For every $n\in\mathbb{N}$, $n\geqq 2$ there is a relation symbol to denote the set of n-th powers in Q_p. For every $n\in\mathbb{N}$, $n\geqq 2$ there is a symbol to denote the function which maps an integer y to the greatest integer $\leqq y/n$. Finally there are the symbols $=$, $\wedge$, $\vee$, $\neg$ and quantifiers $\exists x\in Q_p$, $\exists y\in\mathbb{Z}$, $\forall x\in Q_p$, $\forall y\in\mathbb{Z}$.

This refinement of Macintyre's Theorem can be proved by adapting Macintyre's proof [21]. An elementary proof will be contained in Weispfenning [32].

---

[1] This means that every formula in that language is equivalent to a formula without quantifiers

6.5. Corollary. *Let $f: Q_p^m \to Q_p$ be a definable function, then* $\operatorname{ord} f(x)$ *is a simple function of* x.

Proof. Trivially from Theorem 6.3. Q.E.D.

Let $f_1(x), \ldots, f_r(x) \in \mathbb{Z}_p[x]$, $x=(x_1, \ldots, x_m)$. The p-adic distance $d(x, V)$ from a point $x \in Q_p^m$ to the variety V, given by the equations $f_1 = \ldots = f_r = 0$, is by definition

$$d(x, V) = \operatorname{Min}\{|x-y| \,\S\, y \in Q_p^m, f_1(y) = \ldots = f_r(y) = 0\},$$

where $|x-y| = \operatorname{Max}_i |x_i - y_i|$. (We will always suppose that there exists at least one p-adic point on V).

6.6. Corollary. *Assume the above notation. Then there exists a finite partition of* Q_p^m *in definable subsets* A, *such that on each* A

$$d(x, V) = \left|\frac{h(x)}{g(x)}\right|^{1/e}, \quad \text{for all } x \in A,$$

where $e \in \mathbb{N}$, $e \neq 0$, $h(x) \in Q_p[x]$, $g(x) \in Q_p[x]$, *and* $g(x) \neq 0$ *for all* $x \in A$.

Proof. Apply Theorem 6.3 to the set S of all $(x, t) \in Q_p^m \times Q_p$ satisfying $|t| = d(x, V)$. It is clear that S is definable. Q.E.D.

The following example shows that Corollary 6.6 is best possible.

6.7. Example. Let C be the curve $x_2^2 - x_1^3 = 0$, and let $p \neq 2, 3$. Let $x = (x_1, x_2) \in \mathbb{Z}_p^2$.

If x_1 is not a square, then $d(x, C) = |x|$.

If x_1 is a square and $|x_2^2 - x_1^3| = \operatorname{Max}(|x_2|^2, |x_1|^3)$, then $d(x, C) = |x_2^2 - x_1^3|^{1/2}$.

If x_1 is a square and $|x_2^2 - x_1^3| < \operatorname{Max}(|x_2|^2, |x_1|^3)$, then $d(x, C) = |(x_2^2 - x_1^3)/x_2|$.

This follows from an elementary argument, using Hensel's Lemma.

6.8. Application. In Sect. 3 we proved the rationality of the Poincaré series $P(T)$ of a subvariety V of Q_p^m, by desingularizing a hypersurface of dimension m. We will now show how we can prove the rationality of $P(T)$ by only desingularizing a hypersurface of dimension $m-1$.

Suppose there is at least one point on V with coordinates in $\mathbb{Z}_p$. Let

$$J(s) = \int_{\mathbb{Z}_p^m} d(x, V)^s |dx|, \quad \text{for } s \in \mathbb{R}, \quad s > 0.$$

We have that

$$P(p^{-m-s}) = \frac{1 - p^{-s} J(s)}{1 - p^{-s}}. \tag{1}$$

(Note the analogy with 3.4.(1).) Indeed

$$J(s) = \sum_{n \in \mathbb{N}} p^{-ns}(W_n - W_{n+1}),$$

where W_n is the measure of the set $\{x \in \mathbb{Z}_p^m \,\S\, d(x, V) \leqq p^{-n}\}$.

Since $W_n = N_n p^{-mn}$, we obtain

$$J(s) = P(p^{-m-s}) - (P(p^{-m-s}) - 1)p^s,$$

and hence (1).

Using Corollary 6.6 and adapting the proof of Theorem 3.2 slightly, one obtains that $J(s)$ is a rational function of p^{-s}. For this we only need to desingularize a hypersurface of dimension $m-1$ because the domain of integration is now a subset of Q_p^m (instead of a subset of Q_p^{m+1} as for $I(s)$ in Sect. 3).

From this proof also follows that the multiplicity of a pole of $P(T)$ is at most m.

7. Proofs without desingularization

In this section we prove the rationality of $\tilde{P}(T)$, $P(T)$ and $P(T, U)$ without using Hironaka's deep theorem on the resolution of singularities. The key results used in the proof are Macintyre's Theorem 2.2, Corollary 6.5 and Theorem 7.3 below. Theorem 7.3 is similar to and inspired by Theorem A_n of P.J. Cohen [7, p. 140], and can be proved by suitably adapting Cohen's method. However we will use a different method which is simpler (but less powerful). First we need two lemmas.

7.1. Lemma. *Let S be a definable subset of Q_p^{m+q}. For $x \in Q_p^m$, let $S_x = \{y \in Q_p^q \mid (x, y) \in S\}$.*

Let $\alpha \in \mathbb{N}$, $\alpha \geqq 1$. Suppose, for all $x \in Q_p^m$, that S_x is nonempty and that

$$\text{Card } S_x \leqq \alpha, \tag{1}$$

where Card *denotes the cardinality. Then there exist definable functions $f_1(x), \ldots, f_q(x)$ from Q_p^m to Q_p such that $(x, f_1(x), \ldots, f_q(x)) \in S$ for all $x \in Q_p^m$.*

Proof. This lemma is a special case of a result of van den Dries [30] which states that 7.1 is true even without supposing (1). His proof uses model theory and is not elementary. We will give here an elementary proof of Lemma 7.1.

It is sufficient to prove the lemma for $q = 1$, because then the general case follows by induction on q, considering the set

$$\{(x, y_1, \ldots, y_{q-1}) \mid \exists\, y_q \in Q_p : (x, y_1, \ldots, y_q) \in S\}.$$

Thus suppose $q = 1$. If $\alpha = 1$, there is nothing to prove. Hence suppose $\alpha > 1$. It is sufficient to find a definable subset S' of Q_p^{m+1} such that $S' \subset S$, and such that, for all $x \in Q_p^m$, S'_x is nonempty and Card $S'_x \leqq \alpha - 1$, where $S'_x = \{y \in Q_p \mid (x, y) \in S'\}$.

Let $k \in \mathbb{N}$, $k > 1$ be fixed. If, for each $x \in Q_p^m$, we have

(2) Card $S_x = 1$, or
the elements of S_x do not all have the same order, or
the elements of S_x do not all have the same k-th power residue,

then it is easy to find such an S'. Indeed take only those $y \in S_x$ which have minimal order and which, if all the elements of S_x have the same order, have

minimal k-th power residue (minimal with respect to an arbitrary but fixed ordening of the k-th power residues).

For $x \in Q_p^m$, let $\bar{y}(x)$ denote the mean value of the elements in S_x, i.e. $\bar{y}(x) = (\sum_{y \in S_x} y)/\mathrm{Card}(S_x)$. It is clear that $\bar{y}(x)$ is a definable function (because of (1)).

Replacing S by $\{(x, y-\bar{y}(x)) \mid (x, y) \in S\}$, we may suppose that

$$\bar{y}(x) = 0, \quad \text{for all } x \in Q_p^m. \tag{3}$$

Let $\kappa = \operatorname{Max}_{n=1,\ldots,\alpha} \operatorname{ord} n$, and let $k = \phi(p^{\kappa+1})$, where ϕ denotes Euler's ϕ function. For this value of k we will prove that (3) implies (2). Fix $x \in Q_p^m$. Let $n = \mathrm{Card}\, S_x \leqq \alpha$, and $S_x = \{y_1, y_2, \ldots, y_n\}$. Suppose $n > 1$ and $\operatorname{ord} y_1 = \operatorname{ord} y_2 = \ldots = \operatorname{ord} y_n$. We have to prove that not all the y_i have the same k-th power residue. Write $y_i = p^{\operatorname{ord} y_1} y_i'$, then $\operatorname{ord} y_i' = 0$. From (3) follows

$$\sum_{i=1}^{n} y_i' = 0. \tag{4}$$

We have to prove that not all the y_i' have the same k-th power residue. Suppose they all have the same k-th power residue, then, by the special choice of k, all the y_i' have the same residue mod $p^{\kappa+1}$ (relatively prime with p). But then (4) would imply $n \equiv 0 \bmod p^{\kappa+1}$, which is in contradiction with the choice of κ. Q.E.D.

7.2. Lemma. *Let $f(x,t) \in Q_p[x,t]$, $x = (x_1, \ldots, x_m)$, t one variable. Let $n \in \mathbb{N}$, $n > 0$, be fixed. Then there exists a finite partition of Q_p^{m+1} into subsets A of the form*

$$A = \{(x,t) \in Q_p^{m+1} \mid x \in C \text{ and } |t - c_j(x)| \square_{j,l} |a_{j,l}(x)|, \text{ for } j \in S,\ l \in S_j\}, \tag{1}$$

where C is a definable subset of Q_p^m, $\square_{j,l}$ denotes either $\leqq$, $\geqq$, $<$ or $>$, S and the S_j are finite index sets, and $c_j(x)$, $a_{j,l}(x)$ are definable functions from Q_p^m to Q_p, such that for all $(x,t) \in A$ we have

$$f(x,t) = u(x,t)^n h(x) \prod_{j \in S} (t - c_j(x))^{e_j}, \tag{2}$$

with $u(x,t)$ a unit in $\mathbb{Z}_p$, $h(x)$ a definable function from Q_p^m to Q_p, and $e_j \in \mathbb{N}$.

Proof. There exists a finite extension K of Q_p such that for all $x \in Q_p^m$, $f(x,t)$, as a polynomial in t, splits into linear factors over K. (Because there are only a finite number of extensions of Q_p with given degree).

Choose a basis $\xi_1 = 1, \xi_2, \ldots, \xi_k$ for K over Q_p such that for all $z_i \in Q_p$ we have

$$\operatorname{ord}\left(\sum_{i=1}^{k} z_i \xi_i\right) = \operatorname{Min}_i \operatorname{ord}(z_i \xi_i), \tag{3}$$

and

$$0 \leqq \operatorname{ord}(\xi_i) < 1, \quad \text{for } i = 1, \ldots, k. \tag{4}$$

This is possible by taking $u_i \pi^j$ as basis elements, where π is a uniformizing parameter for K, and the $u_i \bmod \pi$ form a basis for the residue field extension.

Let $f(x,t)=a_0(x)t^d+a_1(x)t^{d-1}+\ldots$, with the $a_i(x)\in Q_p[x]$.

Let $Z=\{(x,t)\in Q_p^{m+1} \mid a_0(x)=0\}$, $\bar{Z}=Q_p^{m+1}\setminus Z$. By induction on d, it is sufficient to find a partition of $\bar{Z}$. For $(x,t)\in\bar{Z}$ we have

$$f(x,t)=a_0(x)\prod_{j=1}^{d}(t-b_{1j}(x)-b_{2j}(x)\xi_2-\ldots-b_{kj}(x)\xi_k), \tag{5}$$

for some functions $b_{ij}(x)$ from Q_p^m to Q_p. From Lemma 7.1 it easily follows that we can take the $b_{ij}(x)$ to be definable functions. From (3) it follows that we can partition $\bar{Z}$ in subsets A of the form (1) such that on such an A we have

$$|t-b_{1j}(x)-b_{2j}(x)\xi_2-\ldots-b_{kj}(x)\xi_k|$$

$$=|t-b_{1j}(x)|\neq 0, \quad \text{for } j\in I_1, \tag{6}$$

$$=|b_{i(j),j}(x)|\,|\xi_{i(j)}|\neq 0, \quad \text{for } j\in I_2, \tag{7}$$

$$=0, \quad \text{for } j\in I_3,$$

where $I_1\cup I_2\cup I_3=\{1,2,\ldots,d\}$, and $I_1\cap I_2=\emptyset$.

If $I_3\neq\emptyset$, then $f(x,t)$ is zero on A and (2) is obvious. Thus we may suppose that $I_3=\emptyset$.

There exists $\lambda\in\mathbb{N}$ such that any $u\in\mathbb{Z}_p$ with $u\equiv 1 \bmod p^\lambda$ is an n-th power in $\mathbb{Z}_p$.

For $(x,t)\in A$ we have

$$f(x,t)=a_0(x)\prod_{j\in I_1}(t-b_{1j}(x))\prod_{j\in I_2}b_{i(j),j}(x)\prod_{j=1}^{d}C_j(x,t),$$

with

$$C_j(x,t)=1-\frac{b_{2j}(x)}{t-b_{1j}(x)}\xi_2-\frac{b_{3j}(x)}{t-b_{1j}(x)}\xi_3-\ldots, \quad \text{for } j\in I_1,$$

$$=\frac{t-b_{1j}(x)}{b_{i(j),j}(x)}-\frac{b_{2j}(x)}{b_{i(j),j}(x)}\xi_2-\ldots, \quad \text{for } j\in I_2.$$

From (3), (4) and (6) it follows that

$$\frac{b_{ij}(x)}{t-b_{1j}(x)}\in\mathbb{Z}_p, \tag{8}$$

and ord $C_j(x,t)=0$, for $j\in I_1$, $i\geqq 2$, and $(x,t)\in A$. From (3), (4) and (7) it follows that

$$\frac{t-b_{1j}(x)}{b_{i(j),j}(x)}\in\mathbb{Z}_p, \quad \frac{b_{ij}(x)}{b_{i(j),j}(x)}\in\mathbb{Z}_p, \tag{9}$$

and $0\leqq$ ord $C_j(x,t)<1$, for $j\in I_2$, $i\geqq 2$, and $(x,t)\in A$.

We now partition A with respect to the different possibilities for the residue classes $\bmod p^{\lambda+d}$ of (8) and (9). If these residue classes are fixed then $\prod_{j=1}^{d} C_j(x,t)\in\mathbb{Z}_p$ has constant order less than d and has constant n-th power residue. From this (2) follows.

We still have to show that we can fix the residue classes $\bmod p^{\lambda+d}$ of (8) and (9) by conditions of the form (1). For (9), this is clear. Concerning (8), we have to express the condition

$$\frac{b_{ij}(x)}{t-b_{1j}(x)}\equiv\theta \bmod p^{\lambda+d}, \tag{10}$$

where $\theta\in\mathbb{Z}_p$, in the form (1). If $\theta\equiv 0 \bmod p^{\lambda+d}$, this is clear. Thus suppose $\theta\not\equiv 0 \bmod p^{\lambda+d}$. Then (10) implies

$$\operatorname{ord}(t-b_{1j}(x))=\operatorname{ord} b_{ij}(x)-\operatorname{ord}\theta. \tag{11}$$

A straightforward calculation shows that (10) is equivalent with

$$\operatorname{ord}(t-b_{1j}(x)-b_{ij}(x)\theta^{-1})\geqq\lambda+d-\operatorname{ord}\theta+\operatorname{ord}(t-b_{1j}(x)). \tag{12}$$

Substituting (11) in (12) we see that (10) is equivalent with the conjunction of (11) and

$$\operatorname{ord}(t-b_{1j}(x)-b_{ij}(x)\theta^{-1})\geqq\lambda+d-2\operatorname{ord}\theta+\operatorname{ord}b_{ij}(x). \quad \text{Q.E.D.}$$

7.3. Theorem. *Let $f_i(x,t)\in Q_p[x,t]$, $i=1,\ldots,r$, $x=(x_1,\ldots,x_m)$, t one variable. Let $n\in\mathbb{N}$, $n>0$, be fixed. Then there exists a finite partition of Q_p^{m+1} into subsets A of the form*

$$A=\{(x,t)\in Q_p^{m+1}\mid x\in C \text{ and } |a_1(x)|\square_1|t-c(x)|\square_2|a_2(x)|\}, \tag{1}$$

where C is a definable subset of Q_p^m, and $\square_1$ resp. $\square_2$ denotes either $\leqq$, $<$, or no condition, and $a_1(x)$, $a_2(x)$, $c(x)$ are definable functions from Q_p^m to Q_p, such that for all $(x,t)\in A$ we have

$$f_i(x,t)=u_i(x,t)^n h_i(x)(t-c(x))^{v_i}, \quad \text{for } i=1,\ldots,r, \tag{2}$$

with $u_i(x,t)$ a unit in $\mathbb{Z}_p$, $h_i(x)$ a definable function from Q_p^m to Q_p, and $v_i\in\mathbb{N}$.

Proof. From Lemma 7.2 it follows that there exists a finite partition of Q_p^{m+1} in subsets A of the form 7.2.(1) such that for all $(x,t)\in A$ we have

$$f_i(x,t)=u_i(x,t)^n h_i(x)\prod_{j\in S}(t-c_j(x))^{e_{ji}}, \quad \text{for } i=1,\ldots,r, \tag{3}$$

with $u_i(x,t)$ a unit in $\mathbb{Z}_p$, $h_i(x)$ a definable function from Q_p^m to Q_p, and $e_{ji}\in\mathbb{N}$. It is easy to see that it is sufficient to prove that we can take S such that it contains only one element (The Theorem then follows after a straightforward further partitioning).

Suppose that 1, $2 \in S$, thus $t-c_1(x)$ and $t-c_2(x)$ may appear in 7.2.(1) and (3). We will eliminate from 7.2.(1) and (3) either $t-c_1(x)$ or $t-c_2(x)$, or else eliminate both and introduce a new $c(x)$. This will prove the Theorem. After a partition of A into the set $\{(x,t) \in A \mid c_1(x)=c_2(x)\}$ and its complement in A, we may suppose that $c_1(x) \neq c_2(x)$ for all $(x,t) \in A$. There exists $\lambda \in \mathbb{N}$, $\lambda > 0$, such that any $u \in \mathbb{Z}_p$ with $u \equiv 1 \bmod p^\lambda$ is an n-th power in $\mathbb{Z}_p$.

To simplify the notation we will write c_1, c_2 instead of $c_1(x)$, $c_2(x)$. We have

$$\frac{p^\lambda(t-c_1)}{c_2-c_1} = \frac{p^\lambda(t-c_2)}{c_2-c_1} + p^\lambda. \tag{4}$$

From (4) it follows that we can partition A into subsets each of which satisfies one additional condition (I), (II), (III), or (IV_a) below. (Indeed if neither (I) nor (II) is satisfied, then the right hand side of (4) has nonnegative order less than 2λ, so that we are in case (III) or (IV_a)).

Case (I): $\operatorname{ord}\left(\frac{t-c_1}{c_2-c_1}\right) \geqq \lambda$.

In this case $t-c_2 = t-c_1-(c_2-c_1) = -(c_2-c_1)u(x,t)^n$, with $u(x,t)$ a unit. Thus we can eliminate $t-c_2$.

Case (II): $\operatorname{ord}\left(\frac{t-c_1}{c_2-c_1}\right) < -\lambda$.

In this case $t-c_2 = t-c_1-(c_2-c_1) = (t-c_1)u(x,t)^n$, with $u(x,t)$ a unit. Thus we can eliminate $t-c_2$.

Case (III): $\frac{p^\lambda(t-c_2)}{c_2-c_1} \equiv 0 \bmod p^{2\lambda}$.

In this case, (4) implies

$$\frac{p^\lambda(t-c_1)}{c_2-c_1} = p^\lambda u(x,t)^n,$$

with $u(x,t)$ a unit. Thus we can eliminate $t-c_1$.

Case (IV_a): $\frac{p^\lambda(t-c_2)}{c_2-c_1} \equiv a \bmod p^{3\lambda}$,

where a is a fixed residue class of $\mathbb{Z}_p \bmod p^{3\lambda}$, with $a \not\equiv 0 \bmod p^{2\lambda}$, and $a \not\equiv -p^\lambda \bmod p^{2\lambda}$.

In this case we have

$$\begin{aligned} \frac{p^\lambda(t-c_2)}{c_2-c_1} + p^\lambda &\equiv a + p^\lambda \bmod p^{3\lambda} \\ &\not\equiv 0 \bmod p^{2\lambda} \\ &= (a+p^\lambda)u(x,t)^n, \end{aligned}$$

with $u(x,t)$ a unit. Hence from (4) it follows that

$$t-c_1 = p^{-\lambda}(c_2-c_1)(a+p^\lambda)u(x,t)^n. \tag{5}$$

Moreover

$$\frac{p^{\lambda}(t-c_2)}{c_2-c_1} \equiv a \bmod p^{3\lambda}$$
$$\not\equiv 0 \bmod p^{2\lambda}$$
$$= a\,v(x,t)^n,$$

with $v(x,t)$ a unit. Hence

$$t-c_2 = p^{-\lambda}(c_2-c_1)\,a\,v(x,t)^n. \tag{6}$$

Now use (5) and (6) to eliminate $t-c_1$ and $t-c_2$. However, to express the condition (IV_a), we need a new $t-c$. Q.E.D.

We will now prove the rationality of $\tilde{P}(T)$ and $P(T)$ without using Hironaka's theorem on the resolution of singularities. For this we have to prove Theorem 3.2 without desingularization. In the same way, the results of § 5 can be proved without desingularization, but we leave this to the reader. To prove Theorem 3.2, we will prove

7.4. Theorem. *Let S be a definable subset of Q_p^m, which is contained in a compact subset. Let $h(x)$ be a definable function from Q_p^m to Q_p such that $|h(x)|$ is bounded on S. Let $e\in\mathbb{N}$, $e\geqq 1$. Suppose that $\mathrm{ord}\,h(x)\in e\mathbb{Z}\cup\{+\infty\}$, for all $x\in S$. Let $x=(x_1,\ldots,x_m)$. Then*

$$Z_S(s)=\int_S |h(x)|^{s/e}\,|dx|, \qquad (\textit{for } s\in\mathbb{R}, s>0)$$

is a rational function of p^{-s}.

Proof. Let $\hat{x}=(x_1,\ldots,x_{m-1})$. We will first separate the variable x_m from $\hat{x}$ in the integral $Z_S(s)$.

From Corollary 6.5 it follows that we may suppose that

$$|h(x)|^{1/e}=\left|\frac{g_1(x)}{g_2(x)}\right|^{1/e'}, \qquad \text{for all } x\in S, \tag{1}$$

with $e'\in\mathbb{N}$, $e'\geqq 1$, $g_1(x)$, $g_2(x)\in Q_p[x]$, and $g_2(x)\neq 0$ for all $x\in S$.

From Macintyre's Theorem 2.2 it follows that S is a boolean combination of subsets of type III. Since $\int_{A\cup B} = \int_A + \int_B - \int_{A\cap B}$, we may suppose that S is the set of all $x\in Q_p^m$ satisfying

$$f_j(x) \text{ is (is not) an } n_j\text{-th power}, \qquad \text{for } j=1,\ldots,l, \tag{2}$$

where $f_j\in Q_p[x]$, $n_j\in\mathbb{N}$, $n_j\geqq 1$.

Apply Theorem 7.3 on the polynomials g_1, g_2, f_j, with t replaced by x_m, m replaced by $m-1$, and $n=\prod_j n_j$. We partition S in subsets of the form $S\cap A$, with A as in 7.3. Thus A is the set of all $x\in Q_p^m$ satisfying $\hat{x}\in C$ and

$$\mathrm{ord}(x_m-c(\hat{x}))\square_i \mathrm{ord}\,a_i(\hat{x}), \qquad \text{for } i=1,2, \tag{3}$$

where C is a definable subset of Q_p^{m-1}, and $c(\hat{x})$, $a_i(\hat{x})$ are definable functions from Q_p^{m-1} to Q_p, and $\square_1$, resp. $\square_2$, denotes either $\leqq$, $<$, $\geqq$, or $>$. From (1) and 7.3 it follows that for all $x \in S \cap A$

$$|h(x)|^{1/e} = |h_0(\hat{x})|^{1/e'} |x_m - c(\hat{x})|^{v/e'},$$

with $v \in \mathbb{Z}$ and $h_0(\hat{x})$ a definable function. Also, for all $x \in A$, condition (2) is equivalent with

(2') $\quad h_j(\hat{x})(x_m - c(\hat{x}))^{v_j}$ is (is not) an n_j-th power, for $j = 1, \ldots, l$,

where the $h_j(\hat{x})$ are definable functions and $v_j \in \mathbb{N}$.

We partition $S \cap A$ into subsets S' on which $h_j(\hat{x})$ and $x_m - c(\hat{x})$ have constant n-th power residue. Such an S' is the set of all $x \in Q_p^m$ satisfying (3), $\hat{x} \in D$, and

(4) $\quad x_m - c(\hat{x}) = \lambda \cdot (\text{nonzero } n\text{-th power}),$

where D is a definable subset of Q_p^{m-1}, and $\lambda \in Q_p$.

Put $v = x_m - c(\hat{x})$, then

$$\begin{aligned} Z_{S'}(s) &= \int_D |h_0(\hat{x})|^{s/e'} \int_{(3),(4)} |v|^{vs/e'} |dv|\,|d\hat{x}|, \\ &= \int_D |h_0(\hat{x})|^{s/e'} \Big(\sum_{\substack{k_m \in \mathbb{Z} \\ (5)}} p^{-k_m vs/e'} \int_{\substack{\operatorname{ord} v = k_m \\ v = \lambda \cdot (n\text{-th power})}} |dv| \Big) |d\hat{x}|, \end{aligned}$$

where (5) is the condition

(5) $\quad k_m \square_i \operatorname{ord} a_i(\hat{x}), \quad$ for $i = 1, 2.$

Put $v = p^{k_m} u$, then

$$\int_{\substack{\operatorname{ord} v = k_m \\ v = \lambda \cdot (n\text{-th power})}} |dv| = p^{-k_m} \int_{\substack{\operatorname{ord} u = 0 \\ u = \lambda p^{-k_m} \cdot (n\text{-th power})}} |du|.$$

The last integral is zero unless $k_m \equiv \operatorname{ord} \lambda \bmod n$, and in that case its value γ is independent of k_m. Hence

$$\begin{aligned} Z_{S'}(s) &= \gamma \int_D |h_0(\hat{x})|^{s/e'} \Big(\sum_{\substack{(5) \\ k_m \equiv \operatorname{ord} \lambda \bmod n}} p^{-k_m vs/e' - k_m} \Big) |d\hat{x}|, \\ &= \gamma \sum_{k_m \equiv \operatorname{ord} \lambda \bmod n} p^{-k_m vs/e' - k_m} \int_{D,(5)} |h_0(\hat{x})|^{s/e'} |d\hat{x}|. \end{aligned}$$

Repeating this process, but now also applying Corollary 6.5 and Theorem 7.3 to $a_i(\hat{x})$ in (5), we can separate the variable x_{m-1}. Continuing in this way we can express $Z_S(s)$ as a linear combination of convergent series of the form

(6) $$\sum_{\substack{(k_1, \ldots, k_m) \in L \\ k_i \equiv \mu_i \bmod \alpha_i}} p^{(-q_1 k_1 - \ldots - q_m k_m)s - k_1 - \ldots - k_m},$$

where $q_1, \ldots, q_m \in Q$, $\mu_i \in \mathbb{Z}$, $\alpha_i \in \mathbb{N}$, and L is the set of all integers $k_1, \ldots, k_m$ satisfying a system of linear inequalities in $k_1, \ldots, k_m$ with integer coefficients.

Let d be a common denominator of the rational numbers q_j which appear in the expressions (6). Write $k_i = \mu_i + \alpha_i k_i'$. Then Lemma 7.5 below implies that $Z_S(s)$ is a rational function of $p^{-s/d}$.

Put $T = p^{-s}$. Thus $Z_S(s)$ is a rational function of $\sqrt[d]{T}$. On the other hand, $Z_S(s)$ is a power series in T times an integral power of T, indeed

$$Z_S(s) = \sum_{k \in \mathbb{Z}} T^k \int_{\substack{\operatorname{ord} h(x) = ek \\ x \in S}} |dx|.$$

Since $|h(x)|$ is bounded on S, only finitely many negative k appear in the above series. Thus $Z_S(s)$ is a rational function of T. Q.E.D.

The following Lemma (in a slightly less general form) is contained in Meuser [22].

7.5. Lemma. *Let L be the set of all integers $k_1, \ldots, k_m$ satisfying a finite system of linear inequalities in $k_1, \ldots, k_m$ with integer coefficients. Let $A_1(s), \ldots, A_m(s)$ be linear polynomials in s with integer coefficients. Let $p \in \mathbb{N}$, $p > 1$. Suppose that*

$$J(s) = \sum_{(k_1, \ldots, k_m) \in L} p^{-\sum_{i=1}^{m} k_i A_i(s)} \tag{1}$$

is convergent for $s \in S$, with S an open subset of $\mathbb{R}$.

Then $J(s)$ is a rational function of p^{-s} on S.

Proof. The proof is by induction on m. Summing over a finite number of cases, we may suppose that $k_1, \ldots, k_m \geqq 0$ if $(k_1, \ldots, k_m) \in L$. If all the A_i are identically zero, then there is nothing to prove. Hence suppose that $A_m(s)$ is not identically zero.

The system of inequalities which determines L consists of inequalities not involving k_m and some inequalities

$$\gamma k_m \leqq B_j(k_1, \ldots, k_{m-1}), \quad j = 1, \ldots, q, \tag{2}$$

$$\gamma k_m \geqq C_j(k_1, \ldots, k_{m-1}), \quad j = 1, \ldots, l, \tag{3}$$

with B_j, C_j linear polynomials with integer coefficients, and $\gamma \in \mathbb{N}$, $\gamma \geqq 1$.

Summing over a finite number of cases and adding inequalities in $k_1, \ldots, k_{m-1}$, we may suppose in (2), (3) that $q = 1$ or $q = 0$ (i.e. no B_j is involved), and $l = 1$. And we may also assume that the inequalities in $k_1, \ldots, k_{m-1}$ imply $C_1 \leqq B_1$ (if $q \neq 0$).

Summing over all the possible residue classes of $k_1, \ldots, k_{m-1} \bmod \gamma$ and by substituting $\gamma k_i + r_i$ for k_i, we may suppose in (2), (3) that $\gamma = 1$. Thus

$$J(s) = \sum_{(k_1, \ldots, k_{m-1}) \in L'} p^{-\sum_{i=1}^{m-1} k_i A_i} \sum_{C_1 \leqq k_m \leqq B} p^{-k_m A_m},$$

where L' is a system of linear inequalities in $k_1, \ldots, k_{m-1}$ with integer coefficients, and where B is either $+\infty$ or a linear polynomial in $k_1, \ldots, k_{m-1}$ with integer coefficients. (We have written A_i, C_1 instead of $A_i(s)$, $C_1(k_1, \ldots, k_{m-1})$). Let $S_0 = \{s \in S \mid A_m(s) \neq 0\}$. For $s \in S_0$ we have

$$(4) \qquad J(s) = \Big(\sum_{(k_1,\ldots,k_{m-1}) \in L'} p^{-\left(\sum_{i=1}^{m-1} k_i A_i\right) - C_1 A_m} \Big) (1 - p^{-A_m})^{-1}$$

$$- \Big(\sum_{(k_1,\ldots,k_{m-1}) \in L'} p^{-\left(\sum_{i=1}^{m-1} k_i A_i\right) - B A_m} \Big) p^{-A_m} (1 - p^{-A_m})^{-1}.$$

(If $B = +\infty$, then from the convergence of (1) it follows that $A_m > 0$ on S, and the second series in (4) is zero). The two series in (4) are convergent, hence we can apply the induction hypothesis. Thus $J(s)$ is a rational function of p^{-s} on S_0, and hence on S, since $J(s)$ is continuous on S (because $J(s)$ can be written as a Laurent series in $T = p^{-s}$). Q.E.D.

7.6. Remark. The above proof of Theorem 7.4 also implies Remark 3.3, indeed it shows that

(i) $Z_S(s)$ can be written as a polynomial in p^{-s} and p^s divided by a product of factors of the form $(1 - p^{a+sb})$, with $a, b \in \mathbb{Z}$, and

(ii) the poles of $Z_S(s)$ have multiplicity at most m.

7.7. Remark. Theorem 7.4 and 7.6 (i) remain true when S and $h(x)$ are definable in the richer language built up from the symbols mentioned in 6.4 and an additional symbol to denote the function $\pi: \mathbb{Z} \to Q_p: n \mapsto p^n$. Ax and Kochen [2, III] proved that Q_p admits elimination of quantifiers in this language. However 7.6 (ii) does not remain true. We will return to this in a future paper.

References

1. Atiyah, M.F.: Resolution of singularities and division of distributions. Comm. pure Appl. Math. **23**, 145–150 (1970)
2. Ax, J., Kochen, S.: Diophantine problems over local fields I, II. Amer. J. Math. **87**, 605–648 (1965); III. Ann. Math. (2) **83**, 437–456 (1966)
3. Bernstein, I.N.: The analytic continuation of generalized functions with respect to a parameter. Functional Anal. Appl. **6**, 273–285 (1972)
4. Bernstein, I.N., Gel'fand, S.I.: Meromorphic property of the function P^{λ}. Functional Anal. Appl. **3**, 68–69 (1969)
5. Bollaerts, D.: On the Poincaré series associated to the p-adic points on a curve (Preprint)
6. Borewicz, S.E., Šafarevič, I.R.: Zahlentheorie. Basel, Stuttgart: Birkhaeuser 1966
7. Cohen, P.J.: Decision procedures for real and p-adic fields. Comm. Pure Appl. Math. **22**, 131–151 (1969)
8. Delon, F.: Hensel fields in equal characteristic $p > 0$, in Model Theory of Algebra and Arithmetic. Lecture Notes in Mathematics, vol. 834, pp. 108–116. Berlin-Heidelberg-New York: Springer 1980
9. Driggs, J.H.: Approximations to solutions over Henselian rings. Thesis, Ann Arbor (1976)
10. Eršov, Ju.L.: On elementary theories of local fields. Algebra i Logika **4**, 5–30 (1965)

11. Eršov, Ju.L.: On the elementary theory of maximal normed fields. Soviet Math. Dokl. 6, 1390–1393 (1965)
12. Greenberg, M.J.: Rational points in henselian discrete valuation rings. Publ. Math. IHES **31**, 59–64 (1966)
13. Hayes, D.R., Nutt, M.D.: Reflective functions on p-adic fields. Acta Arithmetica XL, 229–248 (1982)
14. Hironaka, H.: Resolution of singularities of an algebraic variety over a field of characteristic zero. Ann. Math. **79**, 109–326 (1964)
15. Igusa, J.-I.: Complex powers and asymptotic expansions I. J. reine angew. Math. **268/269**, 110–130 (1974); II ibid. 278/279, 307–321 (1975)
16. Igusa, J.-I.: Some observations on higher degree characters. Am. J. Math. **99**, 393–417 (1977)
17. Igusa, J.-I.: On the first terms of certain asymptotic expansions. Complex Analysis and Algebraic Geometry, Baily, W.L., Jr., Shioda, T. (ed.), pp. 357–368. Cambridge University Press, 1977
18. Igusa, J.-I.: Lectures on forms of higher degree. Tata Inst. Fund. Research, Bombay (1978)
19. Kiefe, C.: Sets definable over finite fields, their Zeta-Functions. Trans. Amer. Math. Soc. **223**, 45–59 (1976)
20. Kochen, S.: The model theory of local fields, in Logic Conference, Kiel 1974. Lecture Notes in Mathematics, vol. 499. Berlin-Heidelberg-New York: Springer 1975
21. Macintyre, A.: On definable subsets of p-adic fields. J. Symb. Logic **41**, 605–610 (1976)
22. Meuser, D.: On the rationality of certain generating functions. Math. Ann. **256**, 303–310 (1981)
23. Meuser, D.: On the poles of a local Zeta function for curves. Invent. Math. **73**, 445–465 (1983)
24. Oesterlé, J.: Réduction modulo p^n des sous-ensembles analytiques fermés de $\mathbb{Z}_p^N$. Invent. math. **66**, 325–341 (1982)
25. Oesterlé, J.: Images modulo p^n d'un sous-ensemble analytique fermé de $\mathbb{Z}_p^N$ (Résumé de l'exposé oral). Séminaire de Théorie des Nombres, Paris 1982–83
26. Prestel, A., Roquette, P.: Lectures on formally p-adic fields. Lecture Notes in Mathematics, vol. 1050. Berlin-Heidelberg-New York: Springer 1984
27. Schappacher, N.: Some remarks on a theorem of Greenberg, in Proceedings of the 1979 Kingston Number Theory Conference. Queen's Mathematical Papers, 100–114 (1980)
28. Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. Publ. Math. IHES **54** (1981)
29. Strauss, L.: Poles of a two-variable p-adic complex power. Trans. Amer. Math. Soc. **278**, 481–493 (1983)
30. Dries, L., van den: Algebraic theories with definable Skolem functions (Preprint)
31. Weispfenning, V.: On the elementary theory of Hensel Fields. Annals of Math. Logic **10**, 59–93 (1976)
32. Weispfenning, V.: Quantifier elimination and decision procedures for valued fields, in Logic Colloquium, Aachen 1983. Lecture Notes in Mathematics (to appear)

Oblatum 21-XI-1983