The ring of p-adic integers with exponential function

Nathanaël Mariaule

p-adics and exponential

As in the real case, the exponential function is defined by the serie

$$e^x = \sum_{i=0}^{+\infty} \frac{x^n}{n!}.$$

The serie is convergent iff $nv(x) - v(n!) \to \infty$ iff $v(x) > \frac{1}{p-1}$.
It defines a bijection between $p\mathbb{Z}_p$ and $1 + p\mathbb{Z}_p$.
However, there is no exponential function defined on the whole field $\mathbb{Q}_p$.
Here, we use E_p the continuous prolongation of $\mathbb{N} \to \mathbb{N} : n \longmapsto (1+p)^n$. That function is defined on the valuation ring and satisfies the following:

$$E_p : (\mathbb{Z}_p, +, 0) \cong (1 + p\mathbb{Z}_p, ., 1),$$

$$(1+p)^x = e^{\log_p(1+p)x}, \quad ((1+p)^x)' = \log_p(1+p)(1+p)^x,$$

$$v\left((1+p)^x\right) = 0, \quad v\left((1+p)^x - 1\right) = v(x) + v(\log_p(1+p)) = v(x) + 1.$$

Some questions of decidability.

Consider $\mathcal{L}_{exp} = (+, ., 0, 1, E_p)$ the language of exponential rings. The $\mathcal{L}_E$-term are called E-polynoms.

The equalities of E-polynoms holding in $\mathbb{Z}_p$ are decidable[2].

This is a straightforward consequence of:

- an identity of E-polynoms holds in $\mathbb{Z}_p$ iff it holds in $\mathbb{N}$;
- the set of identities of E-polynoms holding in $\mathbb{N}$ is primitive recursive.

Problem: Let f be a E-polynom (with $m+1$ variables). Define

$$Z(f, a_1, \cdots, a_m) := \{x \in \mathbb{Z}_p \mid \ f(a_1, \cdots, a_m, x) = 0\}.$$

Is there a primitive recursive function N from the set of E-polynoms (with $m+1$ variables) to $\mathbb{N}$ such that for all $a_1, \cdots, a_m \in \mathbb{Z}_p$, for all f E-polynom, either $Z(f, a_1, \cdots, a_m) = \mathbb{Z}_p$ either $Z(f, a_1, \cdots, a_m)$ has cardinal less than $N(f)$?
In the case of a E-polynom with one variable the existence of such bound (however not decidable) is given by Straussman's theorem. Denef-van den Dries [1] proved the existence of the bound in the multi-variable case. However, so far, nothing is known about a recursive bound.

Quantifier elimination.

The theory of $\mathbb{Z}_p$ does not eliminate the quantifiers in the language $(+, ., 0, 1, E_p, P_k; k \in \mathbb{N})$.
We define:

$$D(x,y) = z \text{ iff } \begin{cases} v(x) \geq v(y) \wedge y \neq 0 \wedge x = yz, or, \\ (v(x) < v(y) \vee y = 0) \wedge z = 0. \end{cases}$$

$$f(x,y) = \begin{cases} y(1+p)^{x/y} \\ \\ y. \end{cases}$$

We claim now we cannot eliminate the quantifier in the formula given by:

$$\Psi(x,y,z) \equiv \exists t (D(x,y) = t \wedge z = y(1+p)^t).$$

- Assume that it is not the case. Then, for all U open subset of $\mathbb{Z}_p^3$ such that the intersection between the graph of f (denoted by $\Gamma(f)$) and U is a boolean combinaison of $\{\overline{x} \mid F_i(\overline{x}) = 0\}$, $\{\overline{x} \mid P_k(F_i(\overline{x}))\}$ (F_i definable analytic functions).
- for some i (1 witouth lost of generality) F_1 vanishes on $\Gamma(f) \cap U$ for some U. Otherwise, there is U such that for all $x \in U$, $F_i(x) \neq 0$ for all i. So, $\Gamma(f) \cap U$ contains an intersection of $\{\overline{x} \mid F_i(\overline{x}) \neq 0\}$, $\{\overline{x} \mid P_k(F_i(\overline{x}))\}$ and $\{\overline{x} \mid \neg P_k(F_i(\overline{x}))\}$. But each of these sets contains an open subset of $\mathbb{Z}_p^3$.
- Now, $F_1 = H_0 + H_1 + \cdots$ with H_i homogenous polynoms of degree i. Also, as for all $t \in \mathbb{Z}_p$ $f(tx, ty) = tf(x, y)$,

$$0 = F_1(tx, ty, tz) = H_0(x,y,z) + tH_1(x,y,z) + \cdots .$$

So, for all $x, y \in \mathbb{Z}_p$, $H_r(x, y, f(x, y)) = 0$. This contradicts the fact that E_p is not an "algebraic" function.

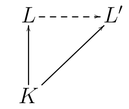
An approach to model-completeness?

- In the difference of the real case, our structure is a ring but not a field. We have therefore to consider equation and inequation. In fact, we have that any existential formula is equivalent to

$$\exists x_1 \cdots \exists x_n \bigwedge_i p_i(\overline{x}, \overline{a}_i) = 0 \wedge x_{i_1} \neq b_1 \wedge \cdots \wedge x_{i_k} \neq b_k.$$

where p_i are E-polynoms and $\overline{a}, \overline{b}$ parameters.

- Let K, L, L' be three models of $\mathrm{Th}(\mathbb{Z}_{p,exp})$ such that $K \subset L$, $K \preceq L'$, L' $|L|$-saturated. Can we find a K-embedding (of $\mathcal{L}_{exp}$-structure) of L in L'?



Assume $v(L) \neq v(K)$.
In that case, there is $x \in L$ such that $v(x) + v(K)$ is torsion-free in $v(L)/v(K)$ and $v(K(x)) = v(K) \oplus v(x)\mathbb{Z}$.
K, L, L' are models of $Th(\mathbb{Z}_p)$. So, there exists $y \in L'$ such that for all $P(X) \in K[X]$, $v(P(x)) = v(P(y))$.
Let $f : L \longrightarrow L$ be a E-polynom with coefficients in K. By the Weierstrass preparation theorem, we know that for all $t \in K$,

$$v(f(t)) = v(b_0 + b_1 t + \cdots + b_N t^N) \quad b_i \in K.$$

Furthermore,

$$f(x) = \sum_{0 \leq n \leq N} a_n x^n + R \quad \text{with } v(R) > v(a_{N+1}) + (N+1)v(x).$$

As, $v(a_n x^n) \neq v(a_m x^m)$ for all $n \neq m$ ($v(x) + v(K)$ torsion-free in $v(L)/v(K)$),

$$v(f(x)) = v(b_0 + b_1 x + \cdots + b_N x^N) = v(b_0 + b_1 y + \cdots + b_N y^N) = v(f(y)).$$

Then, the map $x \longmapsto y$ induce an K-embedding of $K(x)$ in L' compatible with the structure of exponential ring.

Can we extend this map to the henselization of $K(x)$ in L?
Certainly, by the universal property of the henselization, there exists σ an K-embedding (of valued fields) of $K(x)^h$ in L'. But is this map compatible with the exponential map? i.e. consider any E-polynom f with coefficients in K, is that true that, for all $t \in K(x)^h$, $v(f(t)) = v(f(\sigma(t)))$?

References

[1] J. Denef and L. van den Dries, *p-adic and real subanalytic sets,* vol. 128 (1988), 2nd Edition, pp. 79138.

[2] A. Macintyre, *Decision problems for exponential rings: the p-adic case*, Foundations of computation theory (Borgholm, 1983), 285289, Lecture Notes in Comput. Sci., 158, Springer, Berlin.