Course(s) of June 16

Analytic functions on $\mathbb{Q}_p$ and other complete valued fields

Let (K, v) be a complete valued field, with value group Γ contained in $\mathbb{R}$. If one fixes a real r with $0 < r < 1$, then one can define an *absolute value* $|\ |_v$ on K, by setting $|x|_v = r^{v(x)}$. Thus $|x|_v = 0 \iff x = 0$. $\mathcal{O}_v$ coincides with the elements of absolute value ≤ 1 (the *unit disk*).
Consider a sequence $(a_n)_{n\in\mathbb{N}}$ of elements of K. Assume that for every $\varepsilon > 0$ there is some n_0 such that for $n > n_0$ one has $|a_n|_v < \varepsilon$. In other words, for every $m > 0$, there is some $n_0 = n_0(m)$ such that for $n > n_0$ one has $v(a_n) \geq m$. If one defines $b_m = \sum_{i\leq n_0(m)} a_i$, one then obtains

$$v(b_{m+k} - b_m) \geq \inf\{v(a_n) \mid n > n_0\} \geq m$$

for every $k > 0$. Thus the sequence $(b_n)_{n\in\mathbb{N}}$ has a limit b in K, and one writes $b = \sum_{n\in\mathbb{N}} a_n$.

We define the ring of analytic functions on K (in m variables) to be the subring $K\{X_1, \ldots, X_m\}$ of $K[\![X_1, \ldots, X_m]\!]$ consisting of those series $\sum_{\mathbf{i}\in\mathbb{N}^m} a_{\mathbf{i}} X^{\mathbf{i}}$ such that $|a_{\mathbf{i}}|_v \to 0$ as $|\mathbf{i}| \to \infty$. Here $\mathbf{i} = (i_1, \ldots, i_m)$ is a multi-index, $|\mathbf{i}| = i_1 \cdots + i_m$ and $X^{\mathbf{i}} = X_1^{i_1} \cdots X_m^{i_m}$. By the above observation, these series define functions $\mathcal{O}_v^m \to K$.

Using the same type of strategy, one can define functions which are defined on a multidisk $B(0, r_1) \times \cdots \times B(0, r_m)$ (here I am using the "multiplicative radius"; $r_1, \ldots, r_m \in \mathbb{R}^{>0}$), by looking at series $\sum_{\mathbf{i}\in\mathbb{N}^m} a_{\mathbf{i}} X^{\mathbf{i}}$ such that $|a_{\mathbf{i}}|_v r^{\mathbf{i}} \to 0$ as $|\mathbf{i}| \to \infty$.
And even on annuli, let me give you an example when $m = 1$. Suppose we have $0 < s < r$ two reals, and we want to look at the set of "analytic" functions which converge on the annulus $\{x \in K \mid s \leq |x|_v \leq r\}$. Because we are bounded away from 0, we can in fact consider formal sums of the form $\sum_{n\in\mathbb{Z}} a_n x^n$, and try to determine when they converge. They will converge if both series $\sum_{n\geq 0} a_n x^n$ and $\sum_{n<0} a_n x^n$ converge. I.e., if $|a_n|_v r^n \to 0$ as $n \to +\infty$, and $|a_n|_v s^{-n} \to 0$ as $n \to -\infty$.

Example 28. On the p-adics, we consider the usual series for the exponential function: $\exp(x) = \sum_{n=0}^{\infty} x^n/n!$. It does not converge on $\mathbb{Z}_p$, but it does on $p\mathbb{Z}_p$. It extends extensions of $\mathbb{Q}_p$ (as long as they are complete and with valued group contained in $\mathbb{R}$), and one computes that its radius of convergence is $1/(p-1)$ (i.e., $\{x \mid |x|_p < p^{-1/(p-1)}\}$). Similarly the function $\log(1+x) = \sum_{n=0}^{\infty}(-1)^{n+1}x^n/n$ converges on the maximal ideal $\mathcal{M}$.

Definition 29. We consider the language $\mathcal{L}_{an} = \{+, -, \cdot, 0, 1, P_n, f\}_{n,f}$ where n ranges over the integers ≥ 2, and f ranges over the analytic functions in m variables over $\mathbb{Z}_p$, $m \geq 1$. The $\mathcal{L}_{an}$-structure on $\mathbb{Z}_p$ is the usual structure of the $\mathcal{L}_{\mathrm{Mac}}$-language, and the function symbols f are interpreted as functions $\mathbb{Z}_p^m \to \mathbb{Z}_p$ (for the appropriate m).
We also define the language $\mathcal{L}_{an}^D = \mathcal{L}_{an} \cup \{D\}$, where D is a binary function symbol, which is interpreted as

$$D(x, y) = \begin{cases} x/y \text{ if } y \neq 0 \text{ and } v(x) \geq v(y), \\ 0 \text{ otherwise.} \end{cases}$$

Theorem 30. *The $\mathcal{L}_{an}^D$-structure $\mathbb{Z}_p$ eliminates quantifiers.*

This result was proved by Denef and van den Dries, in [3]. The proof is long, uses resolution of singularities, and I will just give one or two main results which appear in the proof. Actually, the first trick is to replace the predicates P_n vby the predicates P_n^*, defined by $P_n^*(x) \iff P_n(x) \wedge x \neq 0$. Thus, $x \neq 0$ is equivalent to $P_2(x^2)$.
It follows that every $\mathcal{L}_{an}$-quantifier-free definable subset of $\mathbb{Z}_p^m$ can be expressed as a union of *basic sets*

$$B = \{x \in \mathbb{Z}_p^M \mid f(x) = 0,\ P_{n(1)}^*(g_1(x)), \ldots, P_{n(k)}^*(g_k(x))\}$$

where $f, g_1, \ldots, g_k \in \mathbb{Z}\{x\}$. Note that f and the g_i's are simply terms of the language $\mathcal{L}_{an}$. Here we are using the following trick: In a field which is not algebraically closed, using a *norm map*, for each $r \geq 2$ there is a polynomial P_r such that $P_r(x_1, \ldots, x_r) \iff x_1 = \cdots = x_r = 0$. For instance, if our field is $\mathbb{R}$ (or any orderable field), we have $P_r(x_1, \ldots, x_r) = x_1^2 + \cdots + x_r^2$. Over $\mathbb{Q}_p$, we could take $P_r(x_1, \ldots, x_r) = \sum_{i=1}^r p^i x_i^r$. This allows us to replace a conjunction of equations by a single equation.
One can also make all subscripts $n(i)$ equal, using $P_n^*(x) \iff P_{nm}^*(x^m)$. Similarly, we define *D-basic subsets* as

$$B = \{x \in \mathbb{Z}_p^M \mid f(x) = 0,\ P_{n(1)}^*(g_1(x)), \ldots, P_{n(k)}^*(g_k(x))\}$$

where $f, g_1, \ldots, g_k$ are terms of the language $\mathcal{L}_{an}^D$.
So another way of phrasing Theorem 30 is to say

Theorem 30'. *Let $\pi : \mathbb{Z}_p^{N+M} \to \mathbb{Z}_p^N$ be the projection on the first M coordinates, where $N, M \in \mathbb{N}$. If $B \subseteq \mathbb{Z}_p^{M+N}$ is basic, then $\pi(B)$ is a finite union of D-basic sets.*

One uses the following remark: a D-basic subset of $\mathbb{Z}_p^M$ can be written as a finite union of projections of basic subsets of $\mathbb{Z}_p^{M+N}$ for some N. Indeed, observe that

$$\begin{aligned} D(x_1, x_2) = x_3 \iff &(|x_1 \leq |x_2| \wedge x_2 \neq 0 \wedge x_1 = x_2 x_3) \vee \\ &((|x_1| > |x_2| \vee x_2 = 0) \wedge x_3 = 0). \end{aligned}$$

So, one rewrites each $\mathcal{L}_{an}^D$-term by adding extra variables and the corresponding additional equation. The end result for an $\mathcal{L}_{an}^D$ term g in the tuple of variables x will be something like $g(x) = y \iff \bigvee_i \exists z_i h_i(x, z_i) = y \wedge \theta_i(x, z_i)$, where the z_i are tuples of new variables, and the h_i are $\mathcal{L}_{an}$-terms, and the θ_i are quantifier-free formulas distinguishing between the various cases. Very tedious to write down properly.
One very important ingredient is the following

Lemma 31. *Let $X = (X_1, \ldots, X_M)$, $Y = (Y_1, \ldots, Y_n)$, $N > 0$, and $\phi(X, Y)$ a quantifier-free $\mathcal{L}_{an}^D$-formula in which D is only applied to terms not involving the variables of Y. Then there is a quantifier-free $\mathcal{L}_{an}^D$-formula $\psi(X, Z)$, $Z = (Z_1, \ldots, Z_{N-1})$, such that*

(i) $\mathbb{Z}_p \models \exists Y\, \phi(X, Y) \leftrightarrow \exists Z\, \psi(X, Z)$;

(ii) In ψ, D is only applied to terms not involving the new variables of Z.

This lemma is used N times to get a quantifier-free $\mathcal{L}_{an}^D$-formula $\theta(X)$ such that $\mathbb{Z}_p \models \exists Y \phi(X,Y) \leftrightarrow \theta(X)$. Obviously, the lemma is the hardest to prove. It uses a Weierstrass preparation theorem, here is the statement in a particular case:
Let K be a complete valued field as above. We are given some non constant $f \in K\{X,Y\}$, Y a single variable, and we write it as $f = \sum_{i=0}^{\infty} a_i(X)Y^i$, where the $a_i \in K\{X\}$. Let $d > 0$ be such that $a_d \notin (X)$, and for $i > d$, $a_i(X) \in (X)$. Then f can be written as uF, where $F(X,Y) \in K\{X\}[Y]$ is monic of degree d in Y, and $u(X,Y) \in K\{X,Y\}$ is a unit, i.e., $\notin (X,Y)$. So, $\exists Y\, f(X,Y) = 0$ if and only if $\exists Y\, F(X,Y) = 0$. And the latter is a quantifier-free condition in the $\mathcal{L}_{\text{Mac}}$-language on the coefficients of F. To take care of the subformulas involving the P_n^*, one needs something more subtle. (See e.g. 2.2.5 in [5]).

Applications

Definition 32. We work in $\mathbb{Z}_p$; we could as well have worked in $\mathbb{Q}_p$ or in a finite extension of $\mathbb{Q}_p$, but the phrasing has to be slightly changed.

(1) A subset S of $\mathbb{Q}_p^m$ is *semi-analytic* if every $x \in \mathbb{Z}_p^m$ has a neighbourhood U such that $U \cap S$ is a finite union of basic sets. In fact, it just corresponds to being quantifier-free definable in $\mathcal{L}_{an}$, i.e., of being a finite union of basic sets.

(2) A subset S of $\mathbb{Z}_p^m$ is *subanalytic at x* if there is an open neightbourhood U of x, and a semi-analytic $S' \subset U \times \mathbb{Z}_p^N$ such that $U \cap S = \pi(S')$, $\pi : \mathbb{Z}_p^{m+N} \to \mathbb{Z}_p^m$.

(3) A subset S of $\mathbb{Z}_p^m$ is *subanalytic* if it is subanalytic at every points of $\mathbb{Z}_p^m$. Again, this corresponds to being existentially definable in $\mathcal{L}_{an}$. And by the qe result, to being a finite union of D-basic sets.

Rationality of Poincaré series

Let $S \subset \mathbb{Z}_p^m$ be subamalytic. For each $n > 0$, let $N_{n,S} = \text{Card}(\pi_n(S))$, where $\pi_n : \mathbb{Z}_p^m \to (\mathbb{Z}/p^n\mathbb{Z})^m$ is the natural map. Consider the power series

$$P_S(T) = \sum_{n \in \mathbb{N}} N_{n,S} T^n.$$

Then $P_s(T) \in \mathbb{Q}(T)$. (See below for an explicit calculation).

Uniform finiteness

Let $S \subset \mathbb{Z}_p^{m+1}$ be subanalytic. Then there is some number A such that for any $x \in \mathbb{Z}_p^m$, if S_x $(= \{y \in \mathbb{Z}_p \mid (x,y) \in S\})$ is finite, then it has cardinality $\leq A$.

Skolem functions

Recall that an $\mathcal{L}$-structure M has *definable Skolem functions* if for every $\mathcal{L}$-formula $\varphi(x,y)$, y a single variable, there is a definable function $f_\varphi : M^{|x|} \to M$ such that

$$M \models \exists y \varphi(x,y) \iff \varphi(x, f_\varphi(x)).$$

I.e., among the possible elements y which satisfy $\varphi(x,y)$, the function f_φ picks one. The fact that the function f_φ is definable implies uniformity results. Denef and van den Dries show that the $\mathcal{L}^D_{an}$-theory of $\mathbb{Z}_p$ has definable Skolem functions. Expressed in temrs of subanalytic sets, this gives:

Subanalytic selection Theorem: *Let $S \subseteq \mathbb{Z}_p^{M+N}$ be suvbanalytic, and $\pi : \mathbb{Z}_p^{M+N} \to \mathbb{Z}_p^M$ the natural projection. There is a function $f : \pi(S) \to \mathbb{Z}_p^N$ whose graph is subanalytic in $\mathbb{Z}_p^{M+N}$ and contained in S.*

I should also mention that thet theory of $\mathbb{Q}_p$ in the usual ring language also has definable Skolem functions. Here is a sketch of the proof. We have a formula $\varphi(x,y)$, and a point $a \in M^m$, for some $M \equiv \mathbb{Q}_p$. By what we proved earlier, we know that the relative algebraic closure A in M of the field generated by a, is an elementary substructure of $\mathbb{Q}_p$. Hence, if there is some b such that $M\varphi(a,b)$, then one can find this b in A. Using some uniformity, one can find finitely many polynomials $f_i \in \mathbb{Z}_p[X,Y]$ such that for any a, if there is some b with $M \models \varphi(a,b)$, then there is such a b which satisfies $f_i(a,Y) = 0$, for some i with $f_i(a,Y) \not\equiv 0$. It then suffices to show that, uniformly, one can distinguish between the roots of $f_i(a,Y) = 0$, and choose one.

Integration

Let $f : \mathbb{Z}_p^M \to \mathbb{Z}_p$ be analytic, and $S \subset \mathbb{Z}_p^m$ be subanalytic. For $s \in \mathbb{C}$ with $\Re(s) > 0$, define

$$Z(f,S,s) = \int_S |f(x)|^s |dx|.$$

(Here $|\ | = |\ |_p$, and the integal is taken with respect to the usual Haar measure on $\mathbb{Z}_p^m$). So, one gets:

Theorem. *$Z(f,S,s)$ is a rational function of p^{-s}. It can be written as a polynomial in p^{-s} with coefficients in $\mathbb{Q}$, quotiented by a product of factors of the form $(1 - p^{-a-sb})$ with $a, b \in \mathbb{N}^{>0}$. Each pole of $Z(f,S,s)$ has multiplicity $\leq m$.*

The proof when S is semi-analytic is a straightforward generalisation of Denef's result in the algebraic case. The subanalytic case is more complicated, one needs to find a "nice" map $h : \mathbb{Z}_p^m \to \mathbb{Z}_p^m$ and then conmpute

$$Z(f,S,s) = \int_{h^{-1}(S)} |f \circ h(x)|^s |h^*(dx_1 \wedge \cdots \wedge dx_m)|.$$

From this one then compute the rational function $P_s(T)$ (see above).

Applications of the rationality results on Poincaré series

The first application is a result of Gruenewald, Segal and Smith (Inventiones 1988):

Let G be a finitely generated group, and let $\mathcal{X}$ be one of the following families of subgroups of G:
all subgroups of G;
all normal subgroups of G
all subgroups H of G such that $H \simeq G$;
all subgroups H of G such that H and G have the same finite quotients.

Let a_n be the number of subgroups of G of index n in G and which belong to $\mathcal{X}$, and define $\zeta_{G,\mathcal{X}}(s) = \sum_{n>0} a_n n^{-s}$.
If G is nilpotent, then $\zeta_{G,\mathcal{X}}(s) = \prod_p \zeta_{G,\mathcal{X},p}(s)$, where p runs over all primes, and $\zeta_{G,\mathcal{X},p}(s) = \sum a_{p^n} p^{-ns}$. The function $\zeta_{G,\mathcal{X}}$ converges for $s \in \mathbb{C}$ with real part sufficiently large. If one furthermore assumes that G is torsion free, then using Denef's result on the rationality of Poincaré series, one gets that the function $\zeta_{G,\mathcal{X},p}(s)$ is a rational function of p^{-s}.

References

[1] Z. Chatzidakis, notes in French of a course taught in 2008.
`http://www.math.ens.fr/∼zchatzid/papiers/cours08.pdf`

[2] J. Denef, The rationality of the Poincaré series associated to the p-adic points on a variety, Invent. Math. 77 (1984), no. 1, 1 – 23.

[3] J. Denef, L. van den Dries, *p-adic and real subanalytic sets*, Annals of Math, 128 (1988), 79 – 138.

[4] Antonio J. Engler, Alexander Prestel, *Valued fields*, Springer monographs in Mathematics, Berlin (2005).

[5] M. Jarden, *Algebraic patching*, Springer Monographs in Mathematics, 2011

[6] I. Kaplansky, Maximal fields with valuations, Duke Math. J. 9, (1942), 303 – 321.