p-adic Analysis in Arithmetic Geometry

Problem Sheet 14

WINTER SEMESTER 2015/16

MICHAEL STOLL

January 26, 2016

(1) Let f be an analytic function on $\mathcal{D}(0,1)^-$ over $\mathbb{C}_p$ with $N < \infty$ zeros in $D(0,1)^-$, counted with multiplicity. (This means that $f(t) = q(t)(1+h(t))$ where q is a polynomial of degree N all of whose roots are in $D(0,1)^-$ and h is a power series with zero constant term and coefficients of absolute value ≤ 1).

(a) Let $0 < \rho < 1$. Show that there is a bound $B = B(p, N, \rho)$ only depending on p, N and ρ such that $t \mapsto c + \int_0^t f(u)\,du$ has at most B zeros in $D(0,\rho)$ (again counted with multiplicity), for any $c \in \mathbb{C}_p$.

HINT. Consider Newton polygons.

(b) Find an example of f as above such that $t \mapsto \int_0^t f(u)\,du$ has infinitely many zeros in $D(0,1)^-$. (This shows that in part (a) it is necessary to restrict to $D(0,\rho)$.)

HINT. Think of the logarithm.

(2) Let f be an analytic function on the open annulus $\mathcal{A}(r,R)^-$ over $\mathbb{C}_p$ such that $f(t)\,dt$ is exact. Assume that $f(t) = t^\mu q(t)(1+h(t))$ with $\mu \in \mathbb{Z}$, q a polynomial of degree N all of whose roots have absolute value strictly between r and R, and h a Laurent series whose value $h(\alpha)$ on any element $\alpha \in \mathbb{C}_p$ with $r < |\alpha|_p < R$ satisfies $|h(\alpha)|_p < 1$.

(a) Let $0 < \rho < 1$. Show that there is a bound $B' = B'(p, \max\{-2-\mu, \mu+N\}, \rho)$ depending only on the given quantities such that $t \mapsto c + \int_a^t f(t)\,dt$ has at most B' zeros (with multiplicity) on $A(r/\rho, R\rho)$, for any $c \in \mathbb{C}_p$ and any $a \in A(r/\rho, R\rho)$.

HINT. One can treat the 'positive' and 'negative' parts of the series separately.

(b) Show that the statement of part (a) can be wrong when we do not assume that $f(t)\,dt$ is exact.

HINT. Think of the logarithm.

(3) Consider the elliptic curve $E\colon y^2 = x^3 + ax + b$ over $\mathbb{C}_p$ with $|a|_p, |b|_p \le 1$.

(a) Show that $t = x/y$ is a uniformizer at the point at infinity and that the invariant differential $\omega = \frac{dx}{2y}$ has an expansion $\omega = f(t)\,dt$ such that the power series f has coefficients of absolute value ≤ 1 and converges on $D(0,1)^-$.

(b) Let $U \subset E(\mathbb{C}_p)$ be the subset corresponding to $|t|_p < 1$. Show that U is a subgroup of $E(\mathbb{C}_p)$ and that $\log_E\colon U \to \mathbb{C}_p$, $u \mapsto \int_0^u \omega$, defines a group homomorphism.

Solutions

(1) (a) We set

$$B(N,\rho) = \min\{n \ge 0 : \forall n' > n\colon n'\rho^{n'} < \rho^{N+1}\}\,.$$

Since $\rho < 1$, the set under the min is non-empty, so $B(N,\rho)$ is defined. Clearly, $B(N,\rho) \ge N+1$.

Let $g(t) = b_0 + b_1 t + \ldots$ be any power series converging on $D(0,1)^-$. Then the theory of Newton polygons implies that the number of zeros (counted with multiplicity) of $g(t)$ in $D(0,\rho)$ is the largest index $n = \nu_+(g(t),\rho)$ such that

$$\rho^n |b_n|_p = |g(t)|_\rho = \min\{\rho^m |b_m|_p : m \ge 0\}\,.$$

Similarly, the number of zeros of $g(t)$ in $D(0,1)^-$ is the smallest index $n = \nu_-(g(t),1)$ such that $|b_n|_p = \min\{|b_m|_p : m \ge 0\}$ if the minimum exists; otherwise there are infinitely many zeros.

Write $f(t) = a_0 + a_1 t + a_2 t^2 + \ldots$. Our assumption on f implies that $|a_N|_p = \min\{|a_n|_p : n \ge 0\}$ and N is the smallest such index. Without loss of generality we can scale $f(t)$ so that $a_N = 1$. Then $|a_N|_p = 1$ and $|a_n|_p \le 1$ for $n \ge N$. Recall that

$$c + \int_0^t f(u)\,du = c + a_0 t + \frac{a_1}{2}t^2 + \frac{a_2}{3}t^3 + \ldots + \frac{a_{n-1}}{n}t^n + \ldots =: g(t)\,.$$

I claim that whenever $\rho^n |a_{n-1}/n|_p = |g(t)|_\rho$, then $n \le B := B(N,\rho)$, which by the above implies that $g(t)$ has at most B zeros in $D(0,\rho)$.

To prove the claim, consider $n > B$. We have

$$\rho^n \Big|\frac{a_{n-1}}{n}\Big|_p = \frac{\rho^n}{|n|_p}|a_{n-1}|_p \le n\rho^n < \rho^{N+1} \le \rho^{N+1}\Big|\frac{a_N}{N+1}\Big|_p\,,$$

so the minimum of $\rho^m |a_{m-1}/m|_p$ cannot be attained for $m = n$. (We have used $|a_N|_p = 1$, $|a_{n-1}|_p \le 1$ for $n \ge N+1$, $|n|_p \ge 1/n$, and of course the definition of $B = B(N,\rho)$.)

Remarks.

(i) The result can be stated in the form

$$\nu_+\big(g(t),\rho\big) \le B\big(\nu_-(f(t),1),\rho\big)\,.$$

(ii) Our bound does not depend on p. One can obtain better bounds depending on p by defining

$$B(p,N,\rho) = \min\Big\{n \ge 0 : \forall n' > n\colon \frac{\rho^{n'}}{|n'|_p} < \frac{\rho^{N+1}}{|N+1|_p}\Big\}\,.$$

(b) We take $f(t) = 1/(1-t) = 1 + t + t^2 + t^3 + \ldots$; this is an analytic function on $\mathcal{D}(0,1)^-$ with no roots in $D(0,1)^-$ (we can take $q(t) = 1$ and $h(t) = t/(1-t)$). By definition, we have $\int_0^t f(u)\,du = \log(1-t)$. We know that $\log\zeta = 0$ for all roots of unity ζ. By Problem (2) on Problem Sheet 4, we know that $|1-\zeta|_p < 1$ when ζ is a root of unity of order a power of p. Since there are infinitely many such ζ, we get infinitely many zeros $t = 1-\zeta$ of $\log(1-t)$ with $|t|_p < 1$.

(2) (a) Let $0 \neq g(t) = \sum_{n=-\infty}^{\infty} b_n t^n$ be a Laurent series converging on $A(r,R)^-$. In a similar way as for power series we define

$$|g(t)|_\rho = \sup\{\rho^n |b_n|_p : n \in \mathbb{Z}\}$$

(this will be finite for $r < \rho < R$) and then

$$\nu_-(g(t),\rho) = \begin{cases} -\infty & \text{if } \max_n \rho^n |b_n|_p \text{ does not exist,} \\ \inf\{n \in \mathbb{Z} : \rho^n |b_n|_p = |g(t)|_\rho\} & \text{otherwise} \end{cases}$$

and

$$\nu_+(g(t),\rho) = \begin{cases} +\infty & \text{if } \max_n \rho^n |b_n|_p \text{ does not exist,} \\ \sup\{n \in \mathbb{Z} : \rho^n |b_n|_p = |g(t)|_\rho\} & \text{otherwise.} \end{cases}$$

Then (again in a similar way as before), $g(t)$ has exactly $\nu_+(g(t),R') - \nu_-(g(t),r')$ zeros in the closed annulus $A(r',R')$ and exactly $\nu_-(g(t),R') - \nu_+(g(t),r')$ zeros in the open annulus $A(r',R')^-$.

By assumption, $\nu_-(g(t),R) - \nu_+(g(t),r) = N$; more precisely, $\nu_-(g(t),R) = N + \mu$ and $\nu_+(g(t),r) = \mu$. Since $f(t)\,dt$ is exact, so without dt/t-term, we can write

$$f(t)\,dt = f_-(t^{-1})\,\frac{dt}{t^2} + f_+(t)\,dt = -f_-(t^{-1})\,dt^{-1} + f_+(t)\,dt$$

with power series f_-, f_+ converging on $D(0,r^{-1})^-$ and $D(0,R)^-$, respectively. Let

$$g_-(t) = \int_0^t f_-(u)\,du \qquad \text{and} \qquad g_+(t) = \int_0^t f_+(u)\,du\,;$$

then

$$g(t) := c + \int_a^t f(t)\,dt = -g_-(t^{-1}) + c' + g_+(t)\,.$$

From Problem (1a) we get (after scaling by R or r^{-1})

$$\nu_+(g(t),R\rho) \le \nu_+(g_+(t),R\rho) \le B\big(\nu_-(f_+(t),R),\rho\big) = B(\max\{0,\mu+N\},\rho)$$

and

$$\nu_-(g(t),r/\rho) \ge -\nu_+(g_-(t),r^{-1}\rho) \ge -B\big(\nu_-(f_-(t),r^{-1}),\rho\big) = -B(\max\{0,-2-\mu\},\rho)$$

(note the shift by 2 in the exponent), which finally gives the bound

$$\begin{aligned} \nu_+(g(t),R\rho) - \nu_-(g(t),r/\rho) &\le B(\max\{0,\mu+N\},\rho) + B(\max\{0,-2-\mu\},\rho) \\ &\le 2B(\max\{-2-\mu,\mu+N\},\rho) \end{aligned}$$

for the number of zeros of $g(t)$ in $A(r/\rho,R\rho)$.

(b) Let $R > 1$ and $r = 1/R$ and consider $f(t) = 1/t$. Then $g(t) = \int_0^t du/u = \log^\lambda t$. This has infinitely many zeros ζ with $|\zeta|_p = 1$ (namely, all roots of unity), so the statement in part (a) is false for $\rho = 1/R$.

(3) (a) Since x has a pole of order 2 and y has a pole of order 3 at the point O at infinity on E, $t = x/y$ has a simple zero there and is therefore a uniformizer.

We now express x and y as Laurent series in t with finite principal part. Using the relation $x = yt$ in the equation of E gives

$$y^2 = t^3y^3 + aty + b\,.$$

Since y has a triple pole, we write $y = t^{-3}\tilde{y}$, where $\tilde{y}$ is regular and nonzero at O. This gives

$$\tilde{y}^2 = \tilde{y}^3 + at^4\tilde{y} + bt^6\,;$$

hence $\tilde{y}(0) = 1$. Writing $\tilde{y} = 1 + z$ then results in the fixed point equation

$$z = -at^4 - bt^6 - at^4z - 2z^2 - z^3\,,$$

whose right hand side is contracting on the set of formal power series with zero constant term (the absolute value is given by $e^{-\text{order of vanishing at } 0}$). So the equation has a unique solution in formal power series, which can be obtained by iteration; it is then clear that the resulting power series has coefficients of p-adic absolute value ≤ 1 (since this is true for the coefficients of the right hand side). We then have $y(t) = t^{-3}(1 + z(t))$ and $x(x) = yt = t^{-2}(1 + z(t))$. This results in

$$\omega = \frac{dx(t)}{2y(t)} = \frac{-2t^{-3}(1 + z(t)) + t^{-2}z'(t)}{2t^{-3}(1 + z(t))}\,dt = \Bigl(-1 + t\frac{z'(t)}{2(1 + z(t))}\Bigr)\,dt\,.$$

Since $(1+z(t))^{-1} = 1-z(t)+z(t)^2-z(t)^3\pm$ also has p-adically integral coefficients (note that this expansion makes even sense as a formal power series, since $z(t) = -at^4 - bt^6 \pm \ldots$ has no constant term) and $z(t)$ is even, so $z'(t)$ has coefficients divisible by 2, the series

$$f(t) = -1 + t\frac{z'(t)}{2}\bigl(1 + z(t)\bigr)^{-1} = -1 + 2at^4 - 3bt^6 - 6a^2t^8 \pm \ldots$$

that satisfies $\omega = f(t)\,dt$ has coefficients of absolute value ≤ 1 and therefore converges on $D(0,1)^-$.

(b) Considering E as a curve in $\mathbb{P}^2$, the group law on E is characterized by the fact that O is the zero element and three points sum to zero if they are the three intersection points (with multiplicity) of E with a line. So we have to show that a line cannot have exactly two intersection points with E in U. We work with the affine patch given by $y = 1$, so the coordinates are $x/y = t$ and $1/y$. Let $ut + v/y = w$ be the equation of a line in these coordinates. If $v = 0$, then t is constant along the line, and the statement is clear. Otherwise, we can assume that $v = 1$. u and w are determined by the system

$$u\tau_1 - w = 1/y(\tau_1)\,, \qquad u\tau_2 - w = 1/y(\tau_2)$$

with $|\tau_j|_p < 1$. Since $|1/y(\tau)|_p = |\tau|_p^3$ for such τ, we find that

$$u = \frac{\tau_2^3 + \ldots - \tau_1^3 - \ldots}{\tau_2 - \tau_1} = \tau_1^2 + \tau_1\tau_2 + \tau_2^2 + \text{higher order terms}$$

and

$$w = \frac{\tau_1\tau_2^3 + \ldots - \tau_1^3\tau_2 - \ldots}{\tau_2 - \tau_1} = \tau_1\tau_2(\tau_1 + \tau_2) + \text{higher order terms}\,,$$

so $|u|_p, |w|_p < 1$. Substituting for $1/y$ in the equation of E then results in a cubic equation $At^3 + Bt^2 + Ct + D = 0$ with $|A|_p = 1$ and $|B|_p, |C|_p, |D|_p < 1$, so all roots have $|t|_p < 1$. This shows that U is a subgroup of $E(\mathbb{C}_p)$.

Finally, using that ω is invariant under translations by elements of $E(\mathbb{C}_p)$, we find for $u_1, u_2 \in U$ that

$$\log_E(u_1 + u_2) = \int_0^{u_1+u_2} \omega = \int_0^{u_1} \omega + \int_{u_1}^{u_1+u_2} \omega = \int_0^{u_1} \omega + \int_0^{u_2} \omega = \log_E u_1 + \log_E u_2 \,.$$