Cours 10

lunedì 19 aprile 2021 14:15

3. Zeroes of analytic functions defined over NA fields

$f(T) = \sum a_n T^n \in \underbrace{\mathbb{K}\langle T\rangle}_{\text{Tate algebra}}$ $(\mathbb{K}, |\cdot|)$ NA complete metrized field

Problem: localise $(f=0)$ in $\{|z| \leq 1\}$ closed unit ball.

Hensel's lemma (theorem):

$(\mathbb{K}, |\cdot|)$ NA complete metrized field, $f \in \mathbb{K}^\circ[T]$ (polynomial with $\mathbb{K}$-integer coefficients): $f = \sum_{n\geq 0} a_n T^n$, $|a_n| \leq 1$.

Suppose $\exists x \in \mathbb{K}^\circ$ s.t. $|f(x)| < |f'(x)|^2$. Then there exists $\xi \in \mathbb{K}^\circ$ s.t. $f(\xi) = 0$ and $|\xi - x| = \frac{|f(x)|}{|f'(x)|} < |f'(x)|$.

Moreover, ξ is the unique root of f in $B(0, |f'(x)|)$.

Proof (quick)

Apply Newton's method: set $N_f(y) = y - \frac{f(y)}{f'(y)}$.

Strategy: look at the iterate $N_f^n(x)$ and prove it converges to $\xi \in f^{-1}(0)$.

Set $x_0 := x$, $x_1 = N_f(x_0)$, ..., $x_n = N_f(x_{n-1}) = N_f^n(x_0)$. Want to estimate $|x_n|$

Set $c(x) = \left|\frac{f(x)}{(f'(x))^2}\right| < 1$, $|x - x_1| = \left|\frac{f(x)}{f'(x)}\right| = c(x)\cdot|f'(x)|$; $|x-x_1|^2 = c(x)\cdot|f(x)|$.

$$(*): \underbrace{f(x+h) = f(x) + h f'(x) + h^2 P_f(x,h)}_{\text{Taylor.}}$$

Claim: P_f is a polynomial in both variables with coefficients in $\mathbb{K}^\circ$.

It suffices to prove it for $f(T) = T^k$ (and use linearity)

$$(x+h)^k = x^k + k h x^{k-1} + h^2 \underbrace{P_k(x,h)}_{\in \mathbb{Z}[x,h]}$$

Then: $|f(x_1)| = |x - x_1|^2 |P_f(x, x - x_1)| \leq |x - x_1|^2 \leq c(x)|f(x)|$

$h = x_1 - x$.

$(**)\ f'(x+h) = f'(x) + h\,Q_f(x,h)$

$\hat{\mathbb{K}}^\circ[x,h]$ as before.

$|f'(x_1)| = |f'(x) + (x-x_1)\,Q_f(x, x-x_1)| = \max\{|f'(x)|, \underbrace{|x-x_1|}_{<|f'(x)|}\,\underbrace{|Q_f(x,x-x_1)|}_{\leq 1}\}$
$= |f'(x)|.$

$\Rightarrow$ can iterate these estimates

Observe that $c(x_1) \leq c(x)$, $|f(x_n)| \leq c(x)^n |f(x)| \to 0$.

Moreover $|x_n - x_{n+1}| \leq |f(x_n)| \to 0$. We have a Cauchy sequence and we conclude by completeness of $\mathbb{K}$.

The rest of the statement is easier (left as exercise).

□

$\cdot\ \mathbb{K}^{alg} = \mathbb{K}$, $f \in \mathbb{K}^\circ\langle T\rangle$ $f(T) = \sum_{k\geq 0} a_k T^k$ $\qquad ||f|| := \max_{k\geq 0}\{|a_k|\}$.

Assume $f \not\equiv 0$. $\qquad 1 > |a_k| \to 0$.

$\Delta(f) := \max\{k \in \mathbb{N} : |a_k| = ||f||\}$.

Theorem The number of zeroes of f inside $\{|x| \leq 1\}$ (counted with multiplicities) is equal to $\Delta(f)$. In particular, $\#\{f=0\}$ is finite.

This gives an upper bound for $\#\{f=0\}$.

Lower bound: not trivial (nor too hard) relies on Hensel's lemma, see [Robert, VI.2.2]

We focus on the upper bound (discuss the slope method by Newton).

Proof: W.L.O.G., may assume $||f|| = 1$

$f = P + h$, $h = \sum_{|a_k|<1} a_k T^k$ $\qquad P = \sum_{|a_k|=1} a_k T^k$ $\qquad \deg(P) = \Delta(f)$ (by definition)

Lemma 1: $\mathrm{Card}\left(\{f=0\} \cap \{|x|=1\}\right) \leq \mu_1 - \nu_1$,

with $\mu_1 = \max\{k : |a_k| = 1\}$, $\quad \nu_1 = \min\{k : |a_k| = 1\}$

Proof: by induction on $\mu_1 - \nu_1$. (rem: $\mu_1 - \nu_1 \geq 0$).

Proof: by induction on $\mu_1-\nu_1$. (rem: $\mu_1-\nu_1 \geq 0$).

Suppose $\mu_1-\nu_1=0$. $\Rightarrow$ $P(T)=a_{\mu_1}T^{\mu_1}$

$$f(x)=\underbrace{a_{\mu_1}x^{\mu_1}}_{|\cdot|=1}+\underbrace{\sum_{k\neq\mu_1}a_k x^k}_{|\cdot|<1} \underset{|x|=1}{\overset{NA}{\Longrightarrow}} |f(x)|=|a_{\mu_1}x^{\mu_1}|=1$$

Hence we have no zeroes x with $|x|=1$.

If $\mu_1>\nu_1$, we pick $|a|=1$ such that $f(a)=0$.

Claim: $f(T)=(T-a)g(T)$ with $g\in \mathbb{K}^\circ\langle T\rangle$

Indication of proof: look at $f(T+a)$.

It suffices to show that $f(T+a)\in\mathbb{K}^\circ\langle T\rangle$ (direct computation)

We now argue on $\tilde{\mathbb{K}}=\mathbb{K}^\circ/\mathbb{K}^{\circ\circ}=\{|z|\leq 1\}/\{|z|=1\}$.

$\mathbb{K}^\circ\ni z\longmapsto\tilde{z}$

$f\in\mathbb{K}^\circ\langle T\rangle \rightsquigarrow \tilde{f}\in\tilde{\mathbb{K}}[T]$ $\quad f(T)=\sum a_k T^k \rightsquigarrow \tilde{f}=\sum\tilde{a}_k T^k$.

$\tilde{f}(T)=(T-\tilde{a})\tilde{g}(T)$.

$\tilde{f}(T)=\tilde{a}_{\nu_1}T^{\nu_1}+\dots+\tilde{a}_{\mu_1}T^{\mu_1}$

$\Rightarrow \tilde{g}(T)=\tilde{a}_{\mu_1}T^{\mu_1-1}+\dots+\frac{\tilde{a}_{\nu_1}}{\tilde{a}}T^{\nu_1}$ $\quad$ ($\mu_1-\nu_1$ dropped by 1)

Apply the induction hypothesis to $g\in\mathbb{K}^\circ\langle T\rangle$.

$\Rightarrow$ $\mathrm{Card}\,\{g=0\}\cap\{|z|=1\}\leq\mu_1-1-\nu_1$, and we are done.

Rem: we estimated $\mathrm{Card}\,\{f=0\}\cap\partial B(0,1)$.

We want to estimate $\mathrm{Card}\,\{f=0\}\cap\overline{B(0,1)}$.

We will apply the lemma to $\partial B(0,r)$, $r\in[0,1]$.

by renormalising, we get:

Lemma 2: $f=\sum a_k T^k\in\mathbb{K}^\circ\langle T\rangle$, $\max|a_k|=1$. Pick r, $0\leq r\leq 1$.

$$\mathrm{Card}\,(\{f=0\}\cap\{|x|=r\})\leq\max\{k : |a_k|r^k=\sup_j|a_j|r^j\}+$$
$$-\min\{k : |a_k|r^k=\sup_j|a_j|r^j\}$$

$=$ if with multiplicities

Idea: if $r\in|\mathbb{K}^\times|$, $r=|\lambda|$ for some $\lambda\in\mathbb{K}^\times$, apply lemma 1 to $f(\lambda T)$.

Idea: if $r \in |\mathbb{K}^\times|$, $r = |\lambda|$ for some $\lambda \in \mathbb{K}^\times$, apply lemma 1 to $f(\lambda T)$.
if $r \notin |\mathbb{K}^\times|$, $\{|x| = r\}$ is impossible

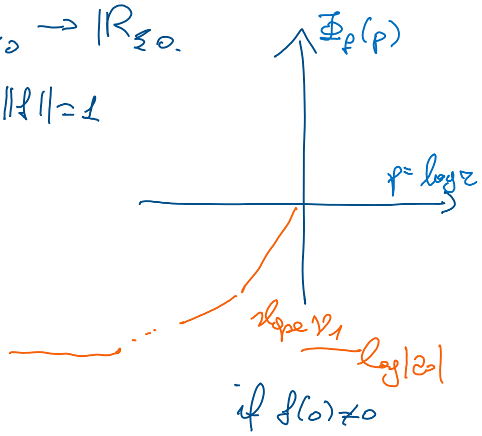
Newton's diagram.

set $\varphi_f(r) = \sup_j |a_j| r^j$ $\quad 0 < r \leq 1$. Take the logarithm:

$$\log \varphi_f(r) = \sup_j \left(\log |a_j| + j \log r \right)$$

$$\Phi_f(p) := \sup_j \left(\log |a_j| + j p \right) \quad (p \leq 0)$$
(so that $\log \varphi_f(r) = \Phi_f(\log r)$).

Rem: Φ_f is increasing and convex $\mathbb{R}_{\leq 0} \to \mathbb{R}_{\leq 0}$.
$\|f\| = 1$



Terminology: a critical radius is a $r \in (0,1]$ s.t. φ_f is not C^1 at r
($\Leftrightarrow$ Φ_f is not C^1/not linear at $\log r$).

Interpretation of lemma 2 with respect to the graph.

$$\mathrm{Card}\left(\{f = 0\} \cap \{|x| = r\} \right) = \Phi'_{f+}(\log r) - \Phi'_{f-}(\log r)$$

(well defined when $r < 1$) right and left derivative

Conclusion: $\mathrm{Card}\left(\{f=0\} \cap \{|x| \leq 1\} \right) =$
$= \mathrm{Card}\left(\{f = 0\} \cap \{x = 1\} \right) + \mathrm{Card}\left(\{f=0\} \cap \{|x| < 1\} \right) =$
$= \underbrace{\mathrm{Card}\left(\{f=0\} \cap \{x=1\} \right)}_{\Delta(f) - \Phi'_{f-}(0)} + \sum_{r \text{ critical}} \Phi'_{f+}(\log r) - \Phi'_{f-}(\log r)$
(finitely many, since slopes are $\in \mathbb{N}$).

If $r_1, r_2, \dots, r_e$ are the critical radii, we get $\Phi'_{f-}(\log r_j) = \Phi'_{f+}(\log r_{j+1})$

Hence we get lots of cancellations:

We conclude that $\mathrm{Card}\left(\{f = 0\} \cap \{x \leq 1\} \right) = \Delta(f)$.

Hence we get ~~lots of contradictions~~:

We conclude that $\mathrm{Card}(\{f=0\}\cap\{x\leq 1\}) = \Delta(f)$.

with multiplicities $\square$

4) Proof of DML (for automorphisms)

$\mathbb{K}^{alg}=\mathbb{K}$, $\mathrm{char}\,\mathbb{K}=0$. $f\in \mathrm{Aut}[\mathbb{A}^d_{\mathbb{K}}]$ $x\in\mathbb{K}^d$, $Z=\{Q=0\}$.

$Q\in\mathbb{K}[x_1,\dots x_d]$; $H=\{n\in\mathbb{N},\ f^n(x)\in Z\}$

DML: H is a finite union of arithmetic progressions $:= \bigcup_{i=1}^{s} a_i+b_i\mathbb{N}$.

$S\subseteq\mathbb{K}$ is a finite set containing all coefficients of f, f^{-1}, Q, x.

Embedding theorem: (LACH '33, CASSELS ~'60)

Let $\mathbb{L}$ be any finitely generated field extension of $\mathbb{Q}$, and $S\subset\mathbb{L}$ finite.

Then for infinitely many primes p there exists a field embedding $i:\mathbb{L}\hookrightarrow\mathbb{Q}_p$ s.t. $i(S)\subseteq\mathbb{Z}_p$.

Idea: if $\mathbb{L}=\mathbb{Q}$, it is easy: pick p not appearing in the denominators of elements of f, and we are done.

It is much less clear for generic $\mathbb{L}$, but $[\mathbb{Q}_p:\mathbb{Q}]=+\infty$.

Apply this embedding theorem to $\mathbb{L}=\mathbb{K}$ and S as above.

$$\mathbb{Z}_p^d \xrightarrow{\text{reduction}} \mathbb{F}_p^d$$
$$x \mapsto \tilde{x}$$

f polynomial map acting on $\mathbb{Z}_p \rightsquigarrow \tilde{f}$ poly. map on $\mathbb{F}_p^d$.

f^{-1} " " " " $\tilde{f}^{-1}$ " "

$\tilde{f}\circ\tilde{f}^{-1}=\mathrm{id} \Rightarrow \tilde{f}$ is a bijection on $\mathbb{F}_p^d \Rightarrow \exists N,\ \tilde{f}^N=\mathrm{id}_{\mathbb{F}_p^d}$.

$$H=\{n\in\mathbb{N}\ f^n(x)\in Z\}=\bigcup^{N-1}\{n\in\mathbb{N}\ \ f^n(f^k(x))\in Z\}.$$

$$H = \{n \in \mathbb{N},\ f^n(x) \in Z\} = \bigcup_{k=0}^{N-1} \{n \in \mathbb{N},\ f^n(f^k(x)) \in Z\}.$$

$\rightsquigarrow$ We may replace f by f^N and assume that $\tilde{f} = \mathrm{id}$ on $\mathbb{F}_p^d$.

$\rightsquigarrow$ May assume also that $\tilde{x} = 0$ (by translation).

• Apply Poonen's parametrization lemma:

$\tilde{f} = \mathrm{id}$ on $\mathbb{F}_p^d \iff f(T) - T \in (p\mathbb{Z}_p[T])^d \overset{(\mathrm{def})}{\iff} f(T) - T \equiv 0 \pmod{p}$

$\hookrightarrow \exists g \in \mathbb{Z}_p\langle T, n\rangle,\ f^n(T) = g(T, n)$

$H = \{n \in \mathbb{N} : Q(f^n(x)) = 0\} = \{n \in \mathbb{N} : Q(g(T, n)) = 0\}$

Rem: $Q(g(x, n)) \in \mathbb{Z}_p\langle n\rangle$

Hence $H \subseteq \underbrace{\{n \in \mathbb{Z}_p : Q(g(x, n)) = 0\}}$

either is finite, or $Q(g(x, n)) \equiv 0$.

Conclusion: either H is finite, or $H = \mathbb{N}$. $\square$

Rem: • We didn't use $\tilde{x} = 0$

• the proof can be adapted to the case of Z not hypersurface.

Rem: Junyi Xie: uses diophantine techniques and estimates (heights) together with p-adic arguments to extend the study to endomorphisms.

Proof of embedding theorem:

Lemma: $f \in \mathbb{Q}[x]$ non constant. Then there exist infinitely many primes s.t. f has a root modulo p (i.e., $\exists b \in \mathbb{N},\ |f(b)|_p < 1$).

Ex: $f(x) = x^2 + 1 \rightsquigarrow p \equiv 1 \pmod{4}$

Assume the lemma holds.

• $\mathbb{L}$ is a finite extension of $\mathbb{F} = \mathbb{Q}(t_1, \dots, t_d)$.

• primitive element theorem: $\mathbb{L} = \mathbb{F}[\theta]$ (we may take $\theta \in S$)

• $\exists P \in \mathbb{Z}[t_1 \dots$

- primitive element theorem: $\mathbb{L} = \mathbb{F}[\theta]$ (we may take $\theta \in S$)
- $\exists\, P \in \mathbb{Z}[t_1 \dots t_d]$ s.t. for all $s \in S$, $P \cdot s \in \mathbb{Z}[t, \theta]$
- minimal polynomial of θ over $\mathbb{F}$:

$f = x^d + c_1 x^{d-1} + \dots + c_d$, $c_j \in \mathbb{F}$.

- Δ = discriminant of $f \in \mathbb{F}$.

f irred $\Rightarrow$ f has simple roots $\Rightarrow$ $\Delta \neq 0$.

Set $\Phi = \Delta \cdot P \cdot \prod_{c_j \neq 0} c_j \in \mathbb{F}$.

Fact: there exists ∞-many $a \in \mathbb{N}^d$ s.t. $\Phi(a) = \Phi(a_1 \dots a_d)$ is well defined and $\neq 0$.

Proof: by induction on d.

If $d = 1$ easy: Φ is the ratio of two polynomials

$d \geq 2$: (fishy exercise)

Take $a \in \mathbb{N}^d$ s.t. $\Phi(a) \neq 0$. and p prime such that

① $\cdot\ |P(a)|_p = 1$ (true for ∞-many p)

② $\cdot\ |\Delta(a)|_p = 1$

③ $\cdot\ |c_i(a)|_p = 1$ $\forall i$ so that $c_i \neq 0$.

④ $\cdot\ f_a = x^d + c_1(a) x^{d-1} + \dots + c_d(a)$ to have a root modulo p.

We build the embedding $i : \mathbb{L} \hookrightarrow \mathbb{Q}_p$.

First, we embed $\mathbb{F}$: (i.e., we define $i(t_j)$)

$i(t_1) = a_1 + p\,\varepsilon_1$ $\quad \varepsilon_1 \in \mathbb{Z}_p$.

$i(t_2) = a_2 + p\,\varepsilon_2$ $\quad \varepsilon_2 \in \mathbb{Z}_p$

$\vdots \qquad\qquad\qquad \vdots$

$i(t_d) = a_d + p\,\varepsilon_d$ $\quad \varepsilon_d \in \mathbb{Z}_p$

We choose $(\varepsilon_j)_j$ in $\mathbb{Z}_p$ to be algebraic independent over $\mathbb{Q}$

[illegible]

We choose $(\varepsilon_j)_j$ in $\mathbb{Z}_p$ to be algebraic independent over $\mathbb{Q}$

This is possible because $\mathbb{Z}_p$ is uncountable.

We get hence an embedding $\mathbb{F} \xhookrightarrow{i} \mathbb{Q}_p$.

To extend to $\mathbb{L}$, we need to define $i(\theta)$

To define a morphism, we need to send θ to a root of $f_a \in \mathbb{Q}[x] \cap \mathbb{Z}_p$.

To do so, we apply Hensel's lemma to find such a root.

By condition (4), $\exists\, b \in \mathbb{N}$ s.t. $|f_a(b)|_p < 1$, i.e., $\tilde{f}_a(\tilde{b}) = 0 \pmod p$.

Claim $|f_a'(b)|_p = 1$

By Hensel's lemma, since $|f_a(b)| < |f_a'(b)|^2$, $\exists\, \beta \in \mathbb{Q}_p$ s.t.
$f_a(\beta) = 0$, $|\beta - b|_p < |f_a'(b)| = 1$, i.e., $\beta = b \bmod p$ $\left(|\beta - b| \le \frac{1}{p}\right)$.

We set
$$\begin{tikzcd} \mathbb{F}[x] \arrow[r, "\text{ring homo}"] \arrow[d, bend right] & \mathbb{Q}_p \\ \mathbb{F}[x]/(f) = \mathbb{L} \arrow[ur] & \end{tikzcd}$$
$$\theta \longmapsto \beta$$

Need to check: S is sent inside $\mathbb{Z}_p$, and the claim.

- $i(S) \subseteq \mathbb{Z}_p$: if $s \in S$, $P(t)\cdot s \in \mathbb{Z}[t, \theta]$

  $t_i \mapsto a_i + p\,\varepsilon_i \in \mathbb{Z}_p$

  $\theta \mapsto \beta \quad \in \mathbb{Z}_p$. * need to fix, not the right choice

  $P(t) \mapsto P(a)$, and by assumption $|P(a)|_p = 1$.

  $\Rightarrow i(s) \in \mathbb{Z}_p$ (ratio of something in $\mathbb{Z}_p$ divided by $P(a)$)

Idea in the claim: $|f_a'(b)|_p = 1$ corresponds to the fact that $|\Delta(a)|_p = 1$.

We work modulo p: $\tilde{\Delta}(\tilde{a}) \neq 0$ since $|\Delta(a)|_p = 1$.

$\to$ The zeros are simple, i.e., the derivative is $\neq 0$ at any root

* we send θ to a solution of the perturbation $\hat{f}$ of f.

$\hat{f}(x) = x^d + c_1(a + p\varepsilon)x^{d-1} + \dots\ c_d(a + p\varepsilon)$, $\hat{f} = f_{a+p\varepsilon}$

$f_a \equiv \hat{f} \pmod{p}$, hence everything works fine.