Introduction to p-adic Hodge theory 4

——— Analytic functions on p-adic annuli, Lubin-Tate formal groups

<u>Recall</u> K completed valued field, $I \subseteq \mathbb{R} \cup \{\infty\}$,

$$A(I) = \{ z \in \widehat{K^{alg}} \mid v(z) \in I \}$$

$$\mathcal{H}(I) = \text{analytic functions on } A(I)$$

$$\cup\!\!\mid$$

$$\mathcal{B}(I) = \{ f(t) \in \mathcal{H}(I) \,;\ v_r(f) \text{ is uniformly bounded below for } r \in I \}$$

<u>Note</u>: If I is a closed interval $[a,b]$, then $\mathcal{H}(I) = \mathcal{B}(I)$ is a Banach space

<u>Fact</u>: $v_r(f) = \min\limits_{\substack{z \in \widehat{K^{alg}} \\ v(z) = r}} v(f(z))$ = min. valuation on the annulus $A([r,r])$

(Proof: Only finitely many n achieves $v_r(f) = v(a_n) + nr$, say $\min = n_0$, $\max = n_1$

Fix $\alpha, \beta \in \widehat{K^{alg}}^{\times}$ with $v(\alpha) = r$, $v(\beta) = v_r(f)$

then $\beta^{-1} f(\alpha t) = \cdots + \underbrace{\beta^{-1} a_{n_0} \alpha^{n_0} t^{n_0} + \cdots + \beta^{-1} a_{n_1} \alpha^{n_1} t^{n_1}}_{\text{coeffs in } \mathcal{O}_{\widehat{K^{alg}}}} + \cdots$

as long as $t_0 \bmod \mathfrak{m}_{\widehat{K^{alg}}}$ avoids finitely many zeros of $\bmod\ \mathfrak{m}_{\widehat{K^{alg}}}$.

$f(\alpha t_0)$ achieves minimal valuation $v_r(f)$.)

<u>Lemma</u>. If $f(x) \in \mathcal{H}(I)$, then f has finitely many zero on $A(I) \Rightarrow f \in \mathcal{B}(I)$

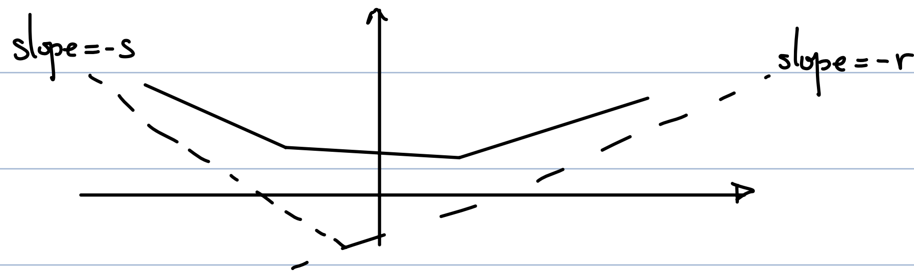
If K is discretely valued or I is closed, then $f \in \mathcal{B}(I) \Rightarrow f$ has finitely many zeros on $A(I)$.

Proof: Say $I = [r,s]$, $(r,s]$, or (r,s).

$\exists M_1,\ v(a_n) + nr \geq M_1$

Then $f(X) \in \mathcal{B}(I) \Longleftrightarrow \Big\{$ ... for all n

$\exists M_2,\ v(a_n)+ns \geq M_2$



f has finitely many zeros on $A(I) \Longleftrightarrow NP(f)$ has finitely many segments of slopes in $-I$.

$\Downarrow$

$\mathcal{B}(I)$ is clear.

Conversely, if K is discretely valued. each segment with slopes in (r,s) brings NP closer to the bound by $v(\varpi)$.

<u>Lemma</u> If $f(X) \in \mathcal{H}(I)$ has no zeros in $A(I)$, then $f(X) \in \mathcal{B}(I)^\times$.

Proof: Condition $\Rightarrow f(X) \in \mathcal{H}(I)^\times$

But previous lemma $\Rightarrow f(X) \in \mathcal{B}(I)$; so $f(X) \in \mathcal{B}(I)^\times$ $\square$

<u>Proposition</u> Assume that K is discretely valued or I is closed. Then $\mathcal{B}(I)$ is a PID

Proof: Let $J \subseteq \mathcal{B}(I)$ be an ideal.

For each $P(X) \in J$, we can write $P(X) = P_f(X) \cdot f^\times(X)$

for $P_f(X) \in K[x]$ accounts for zeros on $A(I)$, and $f^\times(X) \in \mathcal{B}(I)^\times$

All such $P_f(X)$ in $K[x]$ generate a principal ideal $(P_J(x))$.

Then $J = (P_J(x))$. $\square$

• <u>Definition</u>. A <u>divisor</u> D on $A(I)$ is a $(\mathrm{Gal}_K\text{-stable})$ multisubset D of $A(I)$ s.t.

for any closed interval $J \subseteq I$, $D \cap A(J)$ is finite ($[a,+\infty]$ is considered closed)

Facts (1) If $f\in\mathcal{H}(I)$, $\mathrm{div}(f)$ is a divisor on $A(I)$.

(b/c # of elements in $\mathrm{div}(f)$ are controlled by $NP(f)$.)

(2) Conversely, if D is a divisor on $A(I)$, then $\exists f\in\mathcal{H}(I)$ s.t. $\mathrm{div}(f)=D$

(Fix $s_0\in I$. For each $s\in I$ can define a polynomial $P_s(x)\in K[x]$,

so that $\mathrm{div}(P_s(x)) = D\cap A([s,s])$ and $\begin{cases} P_s(0)=1 & \text{if } s<s_0 \\ P_s(x) \text{ monic} & \text{if } s\geq s_0 \end{cases}$

Define $f=\prod_{s<s_0} P_s(x)\cdot\prod_{s\geq s_0}\frac{P_s(x)}{x^{\deg P_s(x)}}$.

It's like $f(x)=\prod_{n\geq 1}\underbrace{(1-p^n x)}_{s=-n \text{ terms}}\underbrace{(1-p^n x^{-1})}_{s=n \text{ terms}}$)

(3) Let D be a divisor on $A(I)$ and suppose we have $P_s(x)$ as above for each $s\in I$

Suppose that we have $Q_s(x)\in K[x]$ s.t. $\deg Q_s(x)<\deg P_s(x)$.

Then $\exists f\in\mathcal{H}(I)$ s.t. $f-Q_s(x)$ is divisible by $P_s(x)$.

(4) $\mathcal{H}(I)$ is a Bézout domain, i.e. any finitely generated ideal is principal.

(b/c (f,g) is the same as the function with $\mathrm{div}=\mathrm{div}(f)\cap\mathrm{div}(g)$.)

§1. Local Class Field Theory

Let K be a nonarchimedean local field, i.e. a finite extension of $\mathbb{Q}_p$ or $\simeq\mathbb{F}_q((t))$ for $q=p^a$.

<u>Theorem</u> (Local Class Field Theory) There exists a canonical reciprocity map

$$\mathrm{Art}: K^\times \longrightarrow \mathrm{Gal}(K^{ab}/K)$$

(normalized so that $\mathrm{Art}(\varpi_K)$ is a geometric Frobenius)

s.t. (1) If L is a finite separable extension of K,

$$L^\times \xrightarrow{\mathrm{Art}_L} \mathrm{Gal}(L^{ab}/L)$$

inclusion $\uparrow\ \downarrow$ $\mathrm{Nm}_{L/K}$ transfer $\uparrow\ \downarrow$ restriction

$$K^\times \xrightarrow{\mathrm{Art}_K} \mathrm{Gal}(K^{ab}/K)$$

<u>transfer map</u>: $\mathrm{Gal}(K^{ab}/K) = H_1(\mathrm{Gal}_K, \mathbb{Z}) \xrightarrow{\text{res}} H_1(\mathrm{Gal}_L, \mathbb{Z}) = \mathrm{Gal}(L^{ab}/L)$

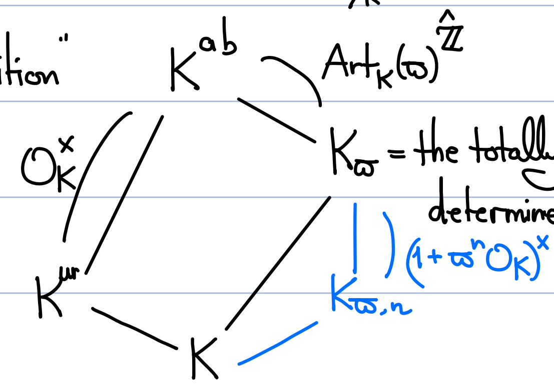
Write $\mathrm{Gal}_K = \coprod_{i=1}^{t} g_i \cdot \mathrm{Gal}_L$, then for $\forall s \in \mathrm{Gal}_K$, $g_i \cdot s = s_i \cdot g_{t(i)}$

Define $\mathrm{trans}(s) := \prod s_i$ in $\mathrm{Gal}(L^{ab}/L)$.

(2) There's a 1-1 correspondence

$$\{\text{open finite index subgps of } K^\times\} \longleftrightarrow \{\text{finite abelian extensions of } K\}$$
$$\mathrm{Nm}_{L/K}(L^\times) \longleftarrow\!\!\shortmid\ L$$

(3) "Composition"



K_ϖ = the totally ramified extension of K determined by a uniformizer $\varpi \in K$.

<u>Goal</u>: Explicitly construct $K_\varpi = \bigcup_n K_{\varpi,n}$

$$K_{\varpi,n} = (K_\varpi)^{(1+\varpi^n O_K)^\times}$$

<u>Example</u> (1) $K = \mathbb{Q}_p$, $\varpi = p$, $K_\varpi = \mathbb{Q}_p(\zeta_{p^m} ; m \in \mathbb{N})$

$K_{\varpi,n} = \mathbb{Q}_p(\zeta_{p^n})$;

note : $\langle \zeta_{p^n} \rangle = \ker\left([p^n] : \mathbb{G}_m \longrightarrow \mathbb{G}_m\right)$

ζ_{p^n} is very close to 1 : so view above as $[p^n] : \hat{\mathbb{G}}_m \longrightarrow \hat{\mathbb{G}}_m$.

(2) E = elliptic curve with CM by imag. quad field F, p inert in F

(e.g. $F = \mathbb{Q}(i)$, p inert in $F/\mathbb{Q}$, $E : y^2 = x^3 - x$.)

$F(x, y\text{-coordinates of } E[N]) \simeq F^{ab}$

$\mathbb{Q}_{p^2}(x, y\text{-coordinates of } E[p^n])$ = a totally ramified abelian extn of $\mathbb{Q}_{p^2}$.

Lubin-Tate's idea: to generate K^{ab}, just need the formal group $\hat{E}$

§2. Lubin-Tate formal group

Definition Let A be a commutative ring. A (one-dimensional commutative) formal group law is a power series $F \in A[[X,Y]]$ s.t.

(1) $F(X,Y) = X + Y + XY$ (some terms

(2) $F(X, F(Y,Z)) = F(F(X,Y), Z)$

(3) there exists a unique $i_F(X) \in -X + X^2 A[[X]]$ s.t. $F(X, i_F(X)) = 0$

(4) $F(X,Y) = F(Y,X)$.

· When A is a local ring, complete w.r.t. maximal ideal $\mathfrak{m}_A$

(or when $A = \mathcal{O}_K$, view $F \in \mathcal{O}_{K^{alg}}[[X]]$ with $A' = \mathcal{O}_{K^{alg}}$, $\rightsquigarrow \mathfrak{m}_{A'} = \mathfrak{m}_{K^{alg}}$)

Then F defines a map $\mathfrak{m}_A \times \mathfrak{m}_A \longrightarrow \mathfrak{m}_A$

$$(x_0, y_0) \longmapsto x_0 +_F y_0 := F(x_0, y_0) = x_0 + y_0 + \text{higher terms}$$

This defines a group structure on $\mathfrak{m}_A$: $(\mathfrak{m}_A, +_F)$.

(the zero for $+_F$ is $0 \in \mathfrak{m}_A$: $F(X,0) = X$; $F(0,X) = X$.)

· Fancy language: Define a functor $\mathcal{N}ilp: A\text{-alg} \longrightarrow \mathcal{S}ets$

$$\mathcal{N}ilp(S) := \{ s \in S, s \text{ nilpotent} \}$$

Then F provides $\mathcal{N}ilp$ a comm. gp structure $+_F: \mathcal{N}ilp \times \mathcal{N}ilp \longrightarrow \mathcal{N}ilp$.

Example: For $\hat{\mathbb{G}}_m$, $F(X,Y) = (1+X)(1+Y) - 1 = X + Y + XY$.

For $m \in \mathbb{N}$, define $[1](X) = X$ and $[m](X) = F(X, [m-1](X))$.

Will prove: Given a uniformizer ϖ of $\mathbb{Z}_p$ and a polynomial $f_\varpi(X) \in \varpi X + X^p + pX^2 \cdot \mathbb{Z}_p[[X]]$,

there is a unique formal group law F_{f_ϖ} (as power series) s.t.

$$[p]_{f_\varpi}(X) = f_\varpi(X)$$

Moreover, for two such f_ϖ and f'_ϖ $\Rightarrow$ $F_{f_\varpi} \simeq F_{f'_\varpi}$

E.g. for $\hat{\mathbb{G}}_m$, $[p](X) = (1+X)^p - 1 = pX + \cdots + X^p \rightsquigarrow f_p(X)$

<u>Definition</u>. If F and G are two formal group laws $F(X,Y), G(X,Y) \in A[\![X,Y]\!]$,

a homomorphism $f: F \to G$ is given by a polynomial $f(X) \in X \cdot A[\![X]\!]$

such that $f(F(X,Y)) = G(f(X), f(Y))$

<u>Definition</u>. Recall that K is a nonarch. local field. with uniformizer ϖ and residue field $\mathbb{F}_q$.

Let A be an $\mathcal{O}_K$-algebra.

A <u>(one-dim'l) formal $\mathcal{O}_K$-module</u> consists of

- a formal group law $F(X,Y) \in A[\![X,Y]\!]$, and
- $\mathcal{O}_K \subseteq \mathrm{End}(F)$; where for each $a \in \mathcal{O}_K$, the action is given by $[a](X) \in X \cdot A[\![X]\!]$

s.t. $[a](X) \in aX + X^2 A[\![X]\!]$.

<u>Preview</u>: $K_{\varpi,n} = K(\text{zero of } [\varpi^n](X))$

Put $\mathcal{F}_\varpi := \left\{ \begin{array}{l} \text{power series } f(X) \text{ in } \mathcal{O}_K[\![X]\!] \text{ s.t. } f(X) = \varpi X + \deg \geq 2 \text{ terms} \\ \qquad\qquad\qquad\qquad\qquad\qquad f(X) \equiv X^q \bmod \varpi \end{array} \right\}$

<u>Theorem</u> (1) For each $f \in \mathcal{F}_\varpi$, there exists a unique $\mathcal{O}_K$-formal module F_f for which

$$[\varpi]_{F_f}(X) = f(X).$$

(2) For each $f_1, f_2 \in \mathcal{F}_\varpi$, there exists a unique isomorphism $g(X) = X + \deg \geq 2$ terms

s.t. $F_{f_2}(g(X), g(Y)) = g(F_{f_1}(X,Y))$.