Formal Groups

08/10/07 L1.

A: ring. $A \neq 0$.

$$f \equiv 0 \pmod{\deg 1} \Leftrightarrow$$

$$A[\![X]\!] \supset (X) = \{ f = \sum_{i=0}^{\infty} a_i X^i \ ; \ a_0 = 0 \}.$$

$\psi \quad \psi$

Lem. 1 $f, g \longmapsto f \circ g$ is associative. w/ $id := X$ as identity.

Lem. 2 $f \in (X)$. $\exists f^{-1} \in (X)$ s.t. $f^{-1} \circ f = f \circ f^{-1} = id$

$\quad = \sum a_i X^i \quad \Leftrightarrow \quad a_1 \in A^\times$.

Moregenerally. $f \in A[\![X]\!]$. $F \in A[\![X_1, \cdots X_n]\!]$.

if $F \equiv 0 \pmod{\deg 1}$ $f \circ F := f(F(X_1, \cdots X_n))$

if $f \equiv 0 \pmod{\deg 1}$. $F \circ f := F(f(X_1), \cdots f(X_n))$

$\} \in A[\![X_1, \cdots X_n]\!]$.

Def. 1 Formal group / A $:= F(X, Y) \in A[\![X, Y]\!]$. w/ $F \overset{i)}{\equiv} X + Y \pmod{\deg 2}$

s.t. $\ _{ii)}\ F(X, F(Y, Z)) = F(F(X, Y), Z)$, $\ _{iii)}\ F(X, Y) = F(Y, X)$.

Ex. $\hat{G}_a(X, Y) := X + Y$. $\hat{G}_m(X, Y) := X + Y + XY$.

Define $a \in \mathbb{N}$.
$[a]_F(X) := F(X, [a-1]_F(X))$
$[0]_F(X) := 0$

Lem. 3. F: formal gp / A.

$[1]_F(X) = F(X, 0) = X$. $\exists ! [-1]_F(X) \in A[\![X]\!]$ s.t.

$F(X, [-1]_F(X)) = 0$.

Pf. $f(X) := F(X, 0) = [1]_F(X)$. $f(X) \equiv X \pmod{\deg 2}$ by i). $\Rightarrow \exists f^{-1}$ by Lem 2.

$f \circ f = f$ by ii). $\Rightarrow$ $f = id$ by composing f^{-1}.

$F(0, Y) = F(Y, 0) = Y$. $\Rightarrow$ No term in F w/ $\deg \geq 2$ contains only X or Y.

$\Rightarrow$ can solve $F(X, Y) = 0$ w.r.t. Y. get $[-1]_F(X)$. $\square$

Def. i). $f, g \in (X) \subset A[\![X]\!]$. $f +_F g := F(f(X), g(X))$.

$\Rightarrow$ (X): abel. gp w/ 0; $[-1]_F \circ f$ = inverse of f.

ii). F, G: formal gp / A. $f \in (X)$: homomorphism $F \to G$

$\Leftrightarrow$ $f \circ F = G \circ f$ i.e. $f(F(X, Y)) = G(f(X), f(Y))$

· ~~$\mathrm{Hom}_A(F,G) := \{$all hom. $f: F \to G\}$~~ :

$f: F \to G,\ g: G \to H \Rightarrow g\circ f: F \to H$

$id := X : F \to F$. f: <u>isom</u> $\Leftrightarrow \exists f^{-1}: G \to F$. $f\circ f^{-1} = f^{-1}\circ f = id$.

$0 : F \to F$. $\Leftrightarrow f = \sum a_i X^i$. $a_1 \in A^\times$ (f: hom,)

· $\mathrm{Hom}_A(F,G) := \{$all hom. $f: F \to G\}$: abel. gp by $+_G$.

$\mathrm{End}_A(F) := \mathrm{Hom}_A(F,F)$: ring w/ $+_F$, $\circ$, id, 0

<u>Lubin-Tate Groups.</u>

· K : local field (CDVF. $\underset{\text{max. ideal}}{\mathfrak{p}} \subset \underset{\text{ring of integers}}{\mathcal{O}} \subset K$. $k = \mathcal{O}/\mathfrak{p} \cong \mathbb{F}_q$). q = power of p.

· L/K : <u>complete unram. ext</u> i.e. $\begin{cases} \text{fin unram. } L/K \text{ or} \\ L = \hat{E}. \ E/K: \text{infin. unram.} \end{cases}$ ($\forall E \subset K^{ur} \subset K_{sep}$)

$\circlearrowright$

~~arithmetic Frobenius~~ ... CDVF. $\mathfrak{p}_L \subset \mathcal{O}_L \subset L$. s.t. $\mathfrak{p}_L = \mathfrak{p}\mathcal{O}_L$.

φ : <u>arithmetic Frobenius</u>

... $\varphi: L \xrightarrow{\sim} L$ s.t. $\varphi|_{\mathcal{O}_L} \bmod \mathfrak{p}$: $k_L \xrightarrow{\sim} k_L$, $x \mapsto x^q$. $k_L \subset \bar{k} = \bar{\mathbb{F}}_q$

· $\alpha^\varphi := \varphi(\alpha)$ $(\alpha \in L)$.

$F = \sum a_i X^i \in L[[X]] \Rightarrow F^\varphi := \sum a_i^\varphi X^i \in L[[X]]$.

F: formal gp$/\mathcal{O}_L \Rightarrow$ so is F^φ.

$\boxed{\text{Fix } n \geq 1}$

<u>Prop.</u> $\varpi \in \mathfrak{p}_L$: uniformizer of L. Let $f \in \mathcal{O}_L[[X]]$ s.t.

i) $f(X) \equiv \varpi X$. (mod deg 2). ii) $f(X) \equiv X^{q^n}$. (mod $\mathfrak{p}$) ... $(*)_n$.

$\Rightarrow \exists! F_f$: formal gp$/\mathcal{O}_L$ s.t. $f \in \mathrm{Hom}_{\mathcal{O}_L}(F_f, F_f^{\varphi^n})$.

<u>Lem.</u> ϖ, ϖ' : unif. of L. $f, f' \in \mathcal{O}_L[[X]]$ satisfying $(*)_n$ for ϖ, ϖ'.

~~Assume~~ $\alpha_1, \dots, \alpha_t \in \mathcal{O}_L$ satisfy $\varpi' \alpha_i = \varpi \alpha_i^{\varphi^n}$ $(1 \leq i \leq t)$.

$\Rightarrow \exists! F \in \mathcal{O}_L[[X_1, \dots, X_t]]$ s.t. i) $F \equiv \alpha_1 X_1 + \dots + \alpha_t X_t$ (mod deg 2)

ii) $f' \circ F = F^{\varphi^n} \circ f$.

$pf.$ $\cdot$ $\mathcal{O}_L[\![X_1, \dots, X_t]\!] = \varprojlim_{m} \mathcal{O}_L[X_1, \dots, X_t] / (\deg m)$

$\cdot$ $\mathcal{O}_L = \varprojlim_{s} \mathcal{O}_L / \mathfrak{p}_L^s$.

Claim. For $\forall m \geq 1$. ~~[illegible]~~ $\exists ! F_m \in \mathcal{O}_L[X_1, \dots, X_t]$. $\deg F_m \leq m$.
s.t. i), ii) hold mod deg $m+1$.

$m = 1$: assumed. induction.

$$G_{m+1} := f' \circ F_m - F_m^{\varphi^n} \circ f \; . \in \mathcal{O}_L[\![X_1, \dots, X_t]\!].$$

mod $\mathfrak{p}$ $\equiv F_m^{q^n} - F_m^{q^n}(X_1^{q^n}, \dots, X_n^{q^n}) \equiv 0$ mod $\mathfrak{p}$.

$\Rightarrow \varpi' \mid G_{m+1}$.

What should $H_{m+1} := F_{m+1} - F_m$ (homog of deg $m+1$) satisfy?

WANT $f' \circ F_{m+1} - F_m^{\varphi^n} \circ f = 0$ (mod deg $m+2$)

$$\| $$

$$G_{m+1} + (f' \circ H_{m+1} - H_{m+1}^{\varphi^n} \circ f).$$

$\boxed{\text{mod deg } m+2}$ $\equiv$

$$G_{m+1} + (\varpi' H_{m+1} - \varpi^{m+1} H_{m+1}^{\varphi^n})$$

make coeff. of each monomial of deg $m+1$ $= 0$.

$\varpi' \beta$: coeff. in G_{m+1}.
α : —— H_{m+1}

$\Rightarrow$ solve $\varpi' \beta + \varpi' \alpha - \varpi^{m+1} \alpha^{\varphi^n} = 0$.

$$\alpha^{\varphi^n} = \left(\frac{\varpi'}{\varpi^{m+1}}\right)(\alpha + \beta).$$

$$\Rightarrow \alpha = -\beta - \sum_{i=1}^{\infty} \left(\frac{\varpi^{m+1}}{\varpi'}\right)^{1 + \varphi^n + \dots + \varphi^{n(i-1)}} \beta^{\varphi^{ni}}.$$

pf of Prop. 1 Lemma for $\varpi = \varpi'$. $f = f'$. $t = 2$.
$F \equiv X + Y$ (mod deg 2)

$\Rightarrow \exists ! F_f \in \mathcal{O}_L[\![X, Y]\!]$ $\begin{cases} \cdot F_f \equiv X + Y \text{ (mod deg 2)} \\ \cdot f \circ F_f = F_f^{\varphi^n} \circ f. \end{cases}$

$\Rightarrow F_f(X, Y) = F_f(Y, X)$ by uniqueness.

$F_f(X, F_f(Y, Z)) = F_f(F_f(X, Y), Z)$ by Lemma for $\varpi = \varpi'$. $f = f'$. $t = 3$. $F \equiv X + Y + Z$.

Def. $\varpi, \varpi' \in L$: unif.

$$A^L_{\varpi,\varpi'} := \{\theta \in \mathcal{O}_L \mid \varpi'\theta = \varpi\theta^{\varphi^n}\}.$$

- additive gp
- $\times$: $A^L_{\varpi,\varpi'} \times A^L_{\varpi',\varpi''} \longrightarrow A^L_{\varpi,\varpi''}$.
- $A^L_{\varpi,\varpi} = \mathcal{O}_L \cap \mathcal{O}_n \supset \mathcal{O}$ ($\mathcal{O}_n$: ring of int. for K_n/K : unram. ext of deg n)
- f, f' w/ $(\ast)_n$ for ϖ, ϖ',

$\theta \in A^L_{\varpi,\varpi'} \Rightarrow \exists! [\theta]_{f,f'} \in \mathcal{O}_L[[X]]$ s.t.

i) $[\theta]_{f,f'}(X) \equiv \theta X$ (mod deg 2). ii) $f' \circ [\theta]_{f,f'} = [\theta]^{\varphi^n}_{f,f'} \circ f$

Prop. · $[\theta]_{f,f'} \in \mathrm{Hom}_{\mathcal{O}_L}(F_f, F_{f'})$ $(\forall \theta \in A^L_{\varpi,\varpi'})$.

· $[\cdot]_{f,f'} : A^L_{\varpi,\varpi'} \longrightarrow \mathrm{Hom}_{\mathcal{O}_L}(F_f, F_{f'})$: inj.

$$[\theta] \underset{F_{f'}}{+} [\theta'] = [\theta + \theta'], \quad [\theta']_{f', f''} \circ [\theta]_{f,f'} = [\theta\theta']_{f,f''}.$$

$\left([\cdot]_f := [\cdot]_{f,f} : \mathcal{O} \hookrightarrow \mathrm{End}_{\mathcal{O}_L}(F_f) : \text{ring hom} \right)$

$\longrightarrow \boxed{(F_f, [\cdot]_f) : \text{Formal } \mathcal{O}\text{-module} / \mathcal{O}_L}$

pf: Show $[\theta] \circ F_f = F_{f'} \circ [\theta]$ by uniqueness.

$$f' \circ ([\theta] \circ F_f) = [\theta]^{\varphi^n} \circ f \circ F_f = [\theta]^{\varphi^n} \circ F_f^{\varphi^n} \circ f = ([\theta] \circ F_f)^{\varphi^n} \circ f$$
$$f' \circ (F_{f'} \circ [\theta]) = F_{f'}^{\varphi^n} \circ f' \circ [\theta] = F_{f'}^{\varphi^n} \circ [\theta]^{\varphi^n} \circ f = (F_{f'} \circ [\theta])^{\varphi^n} \circ f.$$

$\varpi = \varpi'$. $t = 2$. $\equiv \theta X + \theta Y$ mod deg 2.

similar. $\square$

$\varpi \in A^L_{\varpi,\varpi^{\varphi^n}} \Rightarrow [\varpi]_{f,f^{\varphi^n}} = ?$ $\quad f^{\varphi^n} \circ [\varpi]_{f,f^{\varphi^n}} = [\varpi]^{\varphi^n}_{f,f^{\varphi^n}} \circ f$.

$\Rightarrow f = [\varpi]_{f,f^{\varphi^n}}$ by uniqueness.

$$\begin{cases} f = [\varpi]_{f,f^{\varphi^n}} : F_f \longrightarrow F_{f^{\varphi^n}} = F_f^{\varphi^n} \\ f(X) \equiv X^{q^n} \mod \mathfrak{p}. \end{cases}$$

Take any $\varpi_0 \in \mathcal{O}$. $\begin{cases} \varpi = u \cdot \varpi_0 \\ u \in \mathcal{O}_L^\times \end{cases} \Rightarrow [\varpi]_{f,f^{\varphi^n}} = [u]_{f,f^{\varphi^n}} \circ [\varpi_0]_{f,f}$

$\Rightarrow [\varpi_0] \equiv (\text{unit}) \cdot X^{q^n} \mod \mathfrak{p}$. $\boxed{\text{height } n}$