

# Lecture 2

10/10/07

1

Ex.  $K = \mathbb{Q}_p$ .  $\mathcal{O} = \mathbb{Z}_p$ .  $f = (1+x)^p - 1 \equiv \begin{cases} pX \pmod{x^2} \\ X^p \pmod{p} \end{cases}$ .  $L = \mathbb{Q}_p \Rightarrow \varphi$ .  
 $\Rightarrow F_f \equiv \hat{G}_m(x,y) = x+y+xy = (1+x)(1+y) - 1$ .  $f = [\varphi]_f$ .  $[p^m] = (1+x)^{p^m} - 1$ .

$m \geq 1$ .  $F_f[p^m] := \{ \alpha \in \overline{\mathbb{Q}_p} \mid [\varphi^m](\alpha) = 0 \} = \{ \zeta - 1 \mid \zeta^{p^m} = 1 \}$ .

Lubin-Tate ext's.  $\Rightarrow$  tot. ram. abel. ext.  $\mathbb{Q}_p(\mu_{p^m})$

$K$ : local field.  $\mathfrak{p} \subset \mathcal{O} \subset K$ .  $L/K$ : complete unram.

$n=1$  today.  $\mathcal{O}/\mathfrak{p} \cong \overline{\mathbb{F}_q}$ .  $\varphi(x) \equiv x^q \pmod{\mathfrak{p}}$  ( $\forall x \in \mathcal{O}_L$ ).

Def.  $\vartheta \in L$ : unif.  $f \in \mathcal{O}_L[x]$ : monic s.t.  $\begin{cases} \equiv \vartheta X \pmod{x^2} \\ \equiv X^g \pmod{\mathfrak{p}} \end{cases}$   
 $\forall m \geq 1$ .  $f_m := f \circ \varphi^{m-1} \dots \circ f \circ \varphi \circ f$   
 $= f \circ \varphi^{m-1} \circ f_{m-1}$ . ( $f_1 = f$ .  $f_0(x) := X$ ).

$L(\mu_{f,m}) \subseteq \bar{L} :=$  splitting field of  $f_m$  over  $L$ .

$\mu_{f,m} := \{ \alpha \in L(\mu_{f,m}) \mid f_m(\alpha) = 0 \}$ .

Lem.  $L(\mu_{f,m})/L$ : separable. (automatic if char  $K = 0$ ).

Study: fin. sep. ext.  $L' := L(\mu_{f,m})/L$ .  $\mathfrak{p}_L \subset \mathcal{O}_L \subset L'$ .

$f_m \in \mathcal{O}_L[x] \Rightarrow \mu_{f,m} \subset \mathcal{O}_L$ .

## Prop. 1

1)  $\mu_{f,m}$ :  $\mathcal{O}$ -module by  $+_{F_f}, [\cdot]_f$ . isom. to  $\mathcal{O}/\mathfrak{p}^m$ .

More precisely.  $\mathcal{O}/\mathfrak{p}^m \ni a \mapsto [a]_f(\alpha) \in \mu_{f,m}$  for  $\forall \alpha \in \mu_{f,m}/\mu_{f,m-1}$

2)  $L'/L$ : totally ramified Galois ext,  $[L':L] = |\mathcal{O}/\mathfrak{p}^m|^x = q^{m-1}(q-1)$

$\forall \alpha$  as above: unif. of  $L'$ .

3)  $\exists$  can. isom  $\text{Gal}(L'/L) \xrightarrow{\sim} (\mathcal{O}/\mathfrak{p}^m)^x = \text{Aut}_{\mathcal{O}}(\mu_{f,m})$

$(\alpha \mapsto [u]_f(\alpha), \forall \alpha \in \mu_{f,m}) \longmapsto u \pmod{\mathfrak{p}^m}$

pf.  $\forall \alpha_i \in \mathcal{O}_E$ .  $E/L$ : sep.  $F \in \mathcal{O}_L[x_1, \dots, x_t] \Rightarrow F(\alpha_1, \dots, \alpha_t) \in \mathcal{O}_E$ .

1) Recall  $f = [\vartheta]_{f,f^\varphi}$ .  $\Rightarrow f_m = [\vartheta^{p^{m-1}}]_{f^{p^{m-1}}, f^{p^m}} \dots \circ [\vartheta^\varphi]_{f^\varphi, f^{p^2}} \circ [\vartheta]_{f,f^\varphi}$   
 $= [\vartheta^{p^{m-1}} \dots \vartheta^\varphi \vartheta]_{f, f^{p^m}}$

Claim

$\mu_{f,m} \subset \mathfrak{p}_L \Rightarrow \alpha \in \mathcal{O}_L^x \Rightarrow f_m(\alpha) \in \mathcal{O}_L^x$



Claim.  $\mathcal{M}_{f,m} = F_f[\mathfrak{p}^m] := \{ \alpha \in \mathfrak{P}_{L_{sep}} \mid [a](\alpha) = 0 \ \forall a \in \mathfrak{p}^m \}$ .  
 $= \{ \alpha \in \mathfrak{P}_{L_{sep}} \mid [\mathfrak{a}_0^m](\alpha) = 0 \}$   $\mathfrak{a}_0 \in K : \text{unif.}$

$\therefore$  Recall...

$$\mathfrak{D}_m := \mathfrak{D}^{\varphi^{m-1}} \dots \mathfrak{D}^{\varphi} \mathfrak{D} \Rightarrow \mathfrak{D}_m = u \cdot \mathfrak{D}_0^m \quad u \in \mathcal{O}_L^\times.$$

$$\Rightarrow f_m = [\mathfrak{D}_m]_{f, f^{\varphi^m}} = [u]_{f, f^{\varphi^m}} \circ [\mathfrak{D}_0^m]_f$$

$[u]_{f, f^{\varphi^m}} : \text{isom.}$   $\Rightarrow f_m(\alpha) = 0 \Leftrightarrow [\mathfrak{D}_0^m]_f(\alpha) = 0 \quad (\forall \alpha \in L_{sep}).$

$\Rightarrow \mathcal{M}_{f,m} = F_f[\mathfrak{p}^m] \cong \mathcal{O}$ . by  $\tau_{F_f}[\cdot]_f$ .  $(f^{\varphi^{m-1}}(x)/x) \circ f_{m-1}$

$\exists \alpha \in \mathcal{M}_{f,m} \setminus \mathcal{M}_{f,m-1}$   $\left[ \begin{array}{l} \therefore \text{take a root } \alpha \text{ of } f_m/f_{m-1} \text{ in } L' \\ \Rightarrow f_{m-1}(\alpha) : \text{non-zero root of } f^{\varphi^{m-1}}(x). \end{array} \right]$

$$[\mathfrak{p}^{m-1}](\alpha) \neq 0 \Rightarrow |[0](\alpha)| \geq |\mathcal{O}/\mathfrak{p}^m| = g^m = \deg f_m \geq |\mathcal{M}_{f,m}| \geq |[0](\alpha)|.$$

$$\Rightarrow [0](\alpha) = \mathcal{M}_{f,m}, \quad (|\mathcal{M}_{f,m}| = g^m, \text{ } f_m \text{ has no multiple roots})$$

2). By 1).  $\mathcal{M}_{f,m} \subset L(\alpha)$ . i.e.  $L' = L(\alpha)$ .  $\Rightarrow L'/L : \text{Galois.}$

Const. term of  $f_m/f_{m-1}$ .  $\mathfrak{D}^{\varphi^{m-1}} = \prod_{\alpha \in \mathcal{M}_{f,m} \setminus \mathcal{M}_{f,m-1}} (-\alpha)$ .  $\left[ \begin{array}{l} \mathcal{M}_{f,m} : \text{roots of } f_m \\ \mathcal{M}_{f,m-1} : \text{roots of } f_{m-1} \end{array} \right]$

Take  $v_L$ .  $e(L'/L) = \sum v_L(-\alpha) \geq |\mathcal{M}_{f,m} \setminus \mathcal{M}_{f,m-1}| = g^{m-1}(g-1)$ .

$[v_L(\alpha) \geq 1 \text{ by } \alpha \in \mathfrak{P}_{L'}]$   $\ll [L':L] \leq \deg(f_m/f_{m-1}) = g^{m-1}(g-1)$ .

$\Rightarrow f_m/f_{m-1} : \text{min. pol. of } \alpha \text{ i.e. irred.}$

3).  $\text{Gal}(L'/L) \curvearrowright \mathcal{M}_{f,m}$  respects the  $\mathcal{O}$ -mod str.

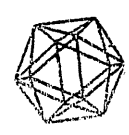
$\Rightarrow \text{Gal}(L'/L) \rightarrow \text{Aut}_{\mathcal{O}}(\mathcal{M}_{f,m})$  inj. by  $L' = L(\mathcal{M}_{f,m})$ .

$\text{Aut}_{\mathcal{O}}(\mathcal{O}/\mathfrak{p}^m) \cong (\mathcal{O}/\mathfrak{p}^m)^\times$  surj. by 2). can.?

Lubin-Tate extensions ~~are isom~~ /  $\hat{K}^{ur}$

$$L := \hat{K}^{ur} \ni \varphi.$$

Lemma.  $\mathcal{O}_L^\times \ni u \mapsto u^\varphi/u \in \mathcal{O}_L^\times$  is surj.



Cor.  $\varpi, \varpi' \in L, f, f' \in L$  satisfy  $\textcircled{*} = \textcircled{*}_1$ .

$\parallel \Rightarrow \exists \text{ isom. } [\theta]_{f, f'} : F_f \xrightarrow{\sim} F_{f'}$ .

$\therefore$  Take  $\theta \in \mathcal{O}_L^\times$  s.t.  $\theta^\varphi / \theta = \varpi' / \varpi \in \mathcal{O}_L^\times$ .  $\perp$

Cor.  $L(\mathcal{M}_{f, m}) = L(\mathcal{M}_{f', m}) \stackrel{(\forall f, f')}{=} K_m \Rightarrow K_m / K : \text{tot. ram. w/ Gal} \simeq (\mathcal{O}/\mathfrak{p}^m)^\times$ .

$\therefore [\theta]_{f, f'} : \mathcal{M}_{f, m} \xrightarrow{\sim} \mathcal{M}_{f', m} : \mathcal{O}\text{-isom.}$   
 $[\theta] \in \mathcal{O}_L[x].$   $\perp$

Lubin-Tate ext's /  $L/K$ : fin.

$L/K$  fin. unram.  $[L:K] = n$ .

$[\theta]_{ii} \in \mathcal{O}_{K^{ur}}[x]$

Prop.  $\Rightarrow \varpi, \varpi' \in L, f, f' \in L$  satisfy  $\textcircled{*}$ . Take  $[\theta]_{f, f'}$  as above.

$\parallel \Rightarrow [\theta]^{\varphi^n} = [\theta] \circ [N_{L/K}(\varpi'/\varpi)]_f$

In particular:  $N_{L/K}(\varpi) = N_{L/K}(\varpi') \Leftrightarrow [\theta] \in \mathcal{O}_L[x]$ .

$(\Rightarrow F_f \xrightarrow{[\theta]} F_{f'} / \mathcal{O}_L)$

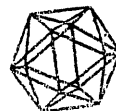
$\therefore [\theta]^{\varphi^n} = [\theta^{\varphi^n}] = [\theta]_{f, f'} \cdot [\theta^\varphi / \theta]_f$   
 $= [\theta]_{f, f'} \cdot [N_{L/K}(\varpi'/\varpi)]_f$

$\theta^{\varphi^n} / \theta = N_{L/K}(\theta^\varphi / \theta)$   
 $= N_{L/K}(\varpi' / \varpi)$

$\left[ \begin{array}{l} \varpi\theta = \theta^\varphi\varpi \\ \theta^\varphi / \theta = \varpi' / \varpi \in \mathcal{O}_L \end{array} \right] \perp$

~~LEM.  $N_{L/K} : L^\times \rightarrow \mathcal{V}_K^{-1}(n\mathbb{Z})$  is surj.~~  
 ~~$(\mathcal{O}_L^\times \rightarrow \mathcal{O}_K^\times)$~~

~~DEF.  $x \in \mathfrak{p} \setminus \{0\}, \mathcal{V}_K(x) = n$ . Take  $\varpi \in L, N_{L/K}(\varpi) = x$ .~~



$K$ : local field.  $\mathfrak{p} \subset \mathcal{O} \subset K$ .  $\mathcal{O}/\mathfrak{p} \cong \mathbb{F}_q$ .  $\varpi \in K$ : unif.

$$f(x) \in \mathcal{O}[x]. \text{ s.t. } f(x) \equiv \begin{cases} \varpi x \pmod{x^2} \\ x^2 \pmod{\mathfrak{p}} \end{cases}$$

Separability of  $f_m$

Lemma 1)  $\mathcal{O}'$ :  $\mathcal{O}$ -alg, domain.  $\alpha \in \mathcal{O}'$ .  $\alpha \notin \mathcal{O}'^\times \Rightarrow f'(\alpha) \neq 0$

$$\begin{aligned} & \parallel 2) \mathcal{O}'/\mathcal{O}: \text{fin. domain. } \alpha, \beta \in \mathcal{O}'. f(\alpha) = \beta. \\ & \alpha \in \mathcal{O}'^\times \Rightarrow \begin{cases} \text{i) } \beta \neq 0 \\ \text{ii) } \beta | \varpi \text{ in } \mathcal{O}' \Rightarrow \beta \in \mathcal{O}'^\times. \end{cases} \end{aligned}$$

pf. 1).  $f'(\alpha) = \varpi(1 + \alpha \cdot g(\alpha))$ .  $g \in \mathcal{O}[x]$ .  $[\dots] \varpi(g)$ .  
 $\alpha \notin \mathcal{O}'^\times \Rightarrow 1 + \alpha g(\alpha) \neq 0 \Rightarrow f'(\alpha) \neq 0$ .  $\square$

2).  $\beta = f(\alpha) = \alpha^n + \varpi \cdot g(\alpha)$ .  $g \in \mathcal{O}[x]$ .  
 $\alpha \in \mathcal{O}'^\times \Rightarrow \beta - \varpi \cdot g(\alpha) \in \mathcal{O}'^\times \Rightarrow \begin{cases} \text{i) } \beta \neq 0 \quad (\because \mathcal{O}'/\mathcal{O}: \text{fin. } \varpi \notin \mathcal{O}'^\times [K \neq \mathcal{O}']) \\ \text{ii) } \beta(1 - \beta^{-1} \cdot g(\alpha)) \in \mathcal{O}'^\times \end{cases}$   
 $\underbrace{\beta | \varpi}_{\varpi = \beta \beta'} \in \mathcal{O}' \Rightarrow \beta \in \mathcal{O}'^\times \quad \square$

Prop.  $f_0(x) := x$ .  $f_m := f^{\varpi^{m-1}} \circ f_{m-1}$  ( $m \geq 1$ ).  $\alpha \in \bar{K}$ .  $\mathcal{O}[\alpha] \subset \bar{K}$ .

$$\begin{aligned} & \parallel 1) \alpha, f(\alpha), \dots, f_{m-1}(\alpha) \notin \mathcal{O}[\alpha]^\times \Rightarrow f'_m(\alpha) \neq 0 \\ & 2) f_m(\alpha) = 0 \Rightarrow \alpha, f(\alpha), \dots, f_{m-1}(\alpha) \notin \mathcal{O}[\alpha]^\times. \end{aligned}$$

pf. 1).  $m=0$ : empty.  $f'_0 = 1 \neq 0$ . induction on  $m$ .  
 $f_{m-1}(\alpha) \notin \mathcal{O}[\alpha]^\times \Rightarrow \underbrace{(f^{\varpi^{m-1}})'(f_{m-1}(\alpha))}_{\text{lem 1)}} \neq 0 \Rightarrow f'_m(\alpha) \neq 0$ .  
 ind. hyp.  $\Rightarrow f'_{m-1}(\alpha) \neq 0$ .  $\square$

2)  $f_i(\alpha) = 0 \Rightarrow \forall j \geq i, f_j(\alpha) = 0$ .  
 $\Rightarrow$  can assume  $\alpha, f(\alpha), \dots, f_{m-1}(\alpha) \neq 0$ .  $[f_m: \text{monic} \Rightarrow \alpha: \text{integral}]$   
 $\Rightarrow \alpha | f(\alpha) | f_2(\alpha) | \dots | f_{m-1}(\alpha) | \varpi^{p^{m-1}}$  in  $\mathcal{O}[\alpha]/\mathcal{O}: \text{fin}$

Assume  $0 \leq i \leq m-1$ .  $f_i(\alpha) \in \mathcal{O}[\alpha]^\times$ . choose maximal such  $i$ .  
 $i \neq m-1 \Rightarrow f_{i+1}(\alpha) | \varpi \Rightarrow f_{i+1}(\alpha) \in \mathcal{O}[\alpha]^\times \quad \times$   
 $\underbrace{\text{lem 2 ii)}}_{\text{hence } i = m-1} \Rightarrow f_m(\alpha) \neq 0 \quad \times$ .  $\square$

Cor.  $f_m$ : separable for  $\forall m \geq 0$ .