(Local) Class Field Theory

$K/\mathbb{Q}_p$ finite extn

Goal: $K^\times \hookrightarrow \mathrm{Gal}(\overline{K}/K)_{ab} = \mathrm{Gal}(K^{ab}/K)$ with dense image

where $K \subseteq K^{ab} \subseteq \overline{K}$ is the maximal abelian subextension

What is K^{ab}?

Thm. (Global Kronecker – Weber) $\mathbb{Q}^{ab} = \bigcup_n \mathbb{Q}(\zeta_n)$

Thm. (Local Kronecker – Weber) $\mathbb{Q}_p^{ab} = \bigcup_n \mathbb{Q}_p(\zeta_n)$

These results fail for nontrivial finite extensions.

$$\begin{tikzcd}
& \bigcup_n \mathbb{Q}_p(\zeta_n) \arrow[dl, dash] \arrow[dr, dash] & \\
\bigcup_n \mathbb{Q}_p(\zeta_{p^n}) \arrow[dr, dash, "\text{totally ramified}"'] & & \bigcup_{p\nmid n} \mathbb{Q}_p(\zeta_n) \arrow[dl, dash, "\text{maximal unramified}"] \\
& \mathbb{Q}_p &
\end{tikzcd}$$

Try to imitate this for K.

$k_K = \mathbb{F}_q$

$k_{K^{ab}} = \overline{k_K} = \overline{\mathbb{F}_q} = \bigcup_{p\nmid m} \mathbb{F}_q(\zeta_m)$

M comes from Eisenstein polynomials

Difficulty: their Galois groups

$$\begin{tikzcd}
& K^{ab} \overset{?}{=} K^{ur}\cdot M \arrow[dl, dash, "\text{dream}"'] \arrow[dr, dash] & \\
M \arrow[dr, dash, "\text{totally ramified abelian}"'] & & \bigcup_{p\nmid m} \mathbb{Q}_p(\zeta_m) = K^{ur} \arrow[dl, dash, "\text{maximal unramified}"] \\
& K &
\end{tikzcd}$$

Approaches to LCFT:

- Galois cohomology, possibly with Brauer groups / central singularities
- Lubin – Tate thy.
- Neukirch approach
- Dwork / Hazewinkel approach

} connected to each other

A local field looks like an orientable surface $\Rightarrow$ we expect some form of Poincaré duality $H^1(K,-) \simeq H_1(K,-)^*$, Hurewicz thm. $\pi_1(K)_{ab} \simeq H_1(K,\mathbb{Z})$

Problem: we don't quite know what the iso actually is.

PD: $H^1(\ ) \times H^1(\ ) \xrightarrow{\sim} \underbrace{H^2(\ )}_{\text{Brauer grp.}} \simeq \mathbb{Q}/\mathbb{Z}$ (perfect pairing)

Formal groups / formal group laws

Rmk. A ring. Then for $f, g \in A[[X]]$: $f \circ g$ is well-def'd. when $g \in (X)$

E.g. $f = \sum X^i$, $g = 1$ $\longrightarrow$ $f \circ g = 1 + 1 + 1 + \dots$ is not well-def'd.

Recall that $f \in A[[X]]^\times$ iff the constant coeff is in $A^\times$.

Note that $f \in (X)$ is invertible under composition iff the linear coeff is in $A^\times$

Def. A formal group over A is a formal power series $F(X,Y) \in A[[X,Y]] = A[[X]][[Y]]$ such that

(1) $F(X,Y) = X + Y + (\deg \geq 2)$ First order looks like addition

(2) $F(F(X,Y), Z) = F(X, F(Y,Z))$ Associativity under composition

(3) $F(X,Y) = F(Y,X)$. Commutativity

Different terminology: one-dimensional formal group law.

(2) should be regarded as an identity in $A[[X,Y,Z]]$, one cannot substitute anything for Z

A formal group is not a group.

Ex. Formal additive group $\widehat{\mathbb{G}}_a$ over $\mathbb{Z}$: $F(X,Y) := X + Y$.

Ex. Formal multiplicative group $\widehat{\mathbb{G}}_m$ over $\mathbb{Z}$: $F(X,Y) := X + Y + XY$

Aside. $\mathbb{G}_m$: Rings $\longrightarrow$ Groups functor, $\mathbb{G}_m = \operatorname{Spec} \mathbb{Z}[T, T^{-1}]$. This is used when studying algebraic groups.
$R \longmapsto R^\times$

Rmk. For a formal group $F(X,Y) \in A[[X,Y]]$ $\exists! \, i_F \in A[[X]]$ s.t. $F(X, i_F(X)) = 0$, called the formal inverse of F.

Notation. $\alpha +_F \beta := F(\alpha, \beta)$ whenever this has a meaning

Def. F, G formal groups over A. Then a homomorphism of formal groups $f: F \longrightarrow G$ is an element $f \in TA[[T]]$ s.t. $f \circ F = G \circ f$, i.e. $f(F(X,Y)) = G(f(X), f(Y))$.

Def. $\operatorname{Hom}(F,G) :=$ set of homomorphisms $F \longrightarrow G$.

This is an abelian group under $f \mp g := G(f,g)$ (which is basically the same as $+_G$)

$\operatorname{End}(F) := \operatorname{Hom}(F,F)$ becomes a ring under composition.

p. 33 instead

Now let $K/\mathbb{Q}_p$ be a finite extension, $k_K = \mathbb{F}_q$

Let L/K be a possibly infinite complete unramified extension.

E.g. L/K finite unramified or $L := \widehat{K^{ur}}$

Def. an unramified extension of K is ~~an algebraic~~ extension such that every finite subextension is unramified in the previous sense. (i.e. has ramification index 1).

Every ur extn of K has the same value group as K; in particular, any such L is a discretely valued field.

Checking the following statements from p. 32: let F, G be formal groups over A. Then

1) $\mathrm{Hom}_A(F,G)$ is an abelian gp under $f +_G g = G(f,g)$.
2) $\mathrm{End}_A(F)$ is a ring under $+_F$ and composition.

Pf: 1) $G(f,g)\big(F(X,Y)\big) \overset{?}{=} G\big(G(f,g)(X),\ G(f,g)(Y)\big)$

$$\begin{aligned}
\text{LHS} &= G\big(f(F(X,Y)),\ g(F(X,Y))\big) && \text{unravel } G(f,g)\\
&= G\big(G(f(X),f(Y)),\ G(g(X),g(Y))\big) && \text{since } f,g\in \mathrm{Hom}_A(F,G)\\
\text{RHS} &= G\big(G(f(X),g(X)),\ G(f(Y),g(Y))\big) && \text{unravel } G(f,g)\\
\text{LHS} &= G\Big(f(X),\ G\big(f(Y),\ G(g(X),g(Y))\big)\Big) && \text{associativity of } G\\
&= G\Big(f(X),\ G\big(g(X),\ G(g(Y),f(Y))\big)\Big) && \text{associativity + commutativity of } G\\
&= G\big(G(f(X),g(X)),\ G(f(Y),g(Y))\big) && \text{associativity of } G
\end{aligned}$$

Rmk. With the more general defn of (not necessarily 1-dim) formal group laws, they form an additive category. B. does not know whether it is abelian.

Let $K/\mathbb{Q}_p$ be a fin extension, $k_K = \mathbb{F}_q$, L/K the completion of an unramified extension of K.

Def. L/K is called unramified if it is algebraic and all finite subextensions $K \subseteq K' \subseteq L$ are unramified in the sense we used so far, i.e. $e_{K'/K} = 1$.

Rmk. There is a unique continuous extension of the absolute value to L,

$L = \text{top. compl.}\left(\bigcup_{K'/K \text{ fin}} K'\right)$ L is a discretely valued field because the value group doesn't change for any K'/K fin.

Rmk. $\mathfrak{m}_L = \mathfrak{m}_K \cdot \mathcal{O}_L$ because this is true for fin extensions, hence for the union and completion as well. From now on we may thus use the notation $\mathfrak{m}$ quite liberally without worrying about which maximal ideal it denotes.

Def. $x \mapsto x^q$ in k_L is called the arithmetic Frobenius.

$$\begin{tikzcd}
L \arrow[from=r, hook'] \arrow[d, dash, "\text{compl of ur}"'] & \mathcal{O}_L \arrow[r, two heads] \arrow[d, dash] & k_L \arrow[d, dash] \\
K \arrow[from=r, hook'] \arrow[d, dash, "\text{fin}"'] & \mathcal{O}_K \arrow[r, two heads] \arrow[d, dash] & k_K = \mathbb{F}_q,\quad q = p^a \arrow[d, dash, "\text{fin}"] \\
\mathbb{Q}_p \arrow[from=r, hook'] & \mathbb{Z}_p \arrow[r, two heads] & \mathbb{F}_p
\end{tikzcd}
\qquad
\begin{tikzcd}
L \arrow[d, dash] & & \\
\tilde{L} := \bigcup K' \arrow[from=r, hook'] \arrow[d, dash] & \mathcal{O}_{\tilde{L}} \arrow[r, two heads] \arrow[d, dash] & k_{\tilde{L}} \arrow[d, dash] \\
K \arrow[from=r, hook'] & \mathcal{O}_K \arrow[r, two heads] & \mathbb{F}_q
\end{tikzcd}$$

$\mathrm{Gal}(\tilde{L}/K) \simeq \mathrm{Gal}(k_{\tilde{L}}/k_K)$ We have shown this for unramified, take the union $\Rightarrow$ true for $\tilde{L}$.

$\tilde{\varphi} \in \mathrm{Gal}(k_{\tilde{L}}/k_K)$ canonical for $\varphi \in \mathrm{Gal}(\tilde{L}/K)$

Def. The canonical element $\bar{\varphi} : x \mapsto x^q$ pins down a unique elt $\varphi \in \mathrm{Gal}(\tilde{L}/K)$ and then by cont. continuation to the topological completion L defines a unique automorphism $\varphi : L \to L$. We also call this φ the arithmetic Frobenius.

Notation: $\forall \alpha \in L$: $\alpha^{\varphi} := \varphi(\alpha)$. Note that this notation, while it seems to abrasively mix left and right actions, is not "wrong".

Def. $F = \sum f_i T^i \in \mathcal{O}_L[[T]]$ then $F^{\varphi} := \sum f_i^{\varphi} T^i$

Rmk. If $F \in \mathcal{O}_L[[X,Y]]$ is a formal group $/\mathcal{O}_L$ then F^{φ} is also a formal group (because φ respects addition & multiplication).

Def. $\pi, \pi' \in L$ uniformisers. Let $\Theta^L_{\pi,\pi'} := \left\{ \vartheta \in \mathcal{O}_L \;\middle|\; \frac{\vartheta^{\varphi}}{\vartheta} = \frac{\pi'}{\pi} \right\}$

Rmk. Suppose π'' is another uniformiser. Then if $\vartheta \in \Theta^L_{\pi,\pi'}$ and $\vartheta' \in \Theta^L_{\pi',\pi''}$ then $\vartheta \cdot \vartheta' \in \Theta^L_{\pi,\pi''}$.

Pf: $\frac{\vartheta^{\varphi}}{\vartheta} = \frac{\pi'}{\pi}$ & $\frac{(\vartheta')^{\varphi}}{\vartheta'} = \frac{\pi''}{\pi}$ $\Rightarrow$ $\frac{(\vartheta\vartheta')^{\varphi}}{\vartheta\vartheta'} = \frac{\vartheta^{\varphi}}{\vartheta} \cdot \frac{(\vartheta')^{\varphi}}{\vartheta'} = \frac{\pi'}{\pi} \cdot \frac{\pi''}{\pi'} = \frac{\pi''}{\pi}$ □

Ex. $L = K$. Then the residue field extension is trivial, $\varphi = \mathrm{id}$.

$$\Rightarrow \Theta^L_{\pi,\pi'} = \left\{ \vartheta \in \mathcal{O}_L \;\middle|\; \frac{\vartheta}{\vartheta} = 1 = \frac{\pi'}{\pi} \right\} = \begin{cases} \mathcal{O}_L & \text{if } \pi' = \pi \\ \emptyset & \text{if } \pi' \neq \pi \end{cases}$$

Ex. L arbitrary, $\pi' = \pi$ $\Rightarrow$ $\Theta^L_{\pi,\pi'} = \{\vartheta \in \mathcal{O}_L \mid \vartheta^{\varphi} = \vartheta\} \supseteq \mathcal{O}_K$ Actually, one can show $\Theta^L_{\pi,\pi'} = \mathcal{O}_K$.

Lemma. Let π be a uniformiser of L, $f \in \mathcal{O}_L[[X]]$ s.t. (1) $f(X) = \pi X + (\deg \geq 2)$,
(2) $f(X) \equiv X^q \pmod{m_L}$

Let π', f' be another such pair.

Assume $\vartheta_1, \dots, \vartheta_t \in \Theta^L_{\pi,\pi'}$. Then $\exists!\, F \in \mathcal{O}_L[[X_1, \dots, X_t]]$ s.t. (a) $F = \vartheta_1 X_1 + \dots + \vartheta_t X_t + (\deg \geq 2)$
(b) $f' \circ F = F^{\varphi} \circ f$

Pf: "This will be absolute magic. You'll love it!"

Sts $\forall m \geq 1$ $\exists!\, F_m$, $\deg F_m \leq m$ s.t. (a) and (b) hold true mod deg $m+1$. (This is like the proof of Hensel's Lemma.)

We construct F_m by induction, $m=1$ just corresponding to our assumptions (1) and (2): take $F_1 := \vartheta_1 X_1 + \dots + \vartheta_t X_t$, $\deg F_1 \leq 1$, (a) holds by def. and

$$\left.\begin{aligned} f' \circ F &= f'(\vartheta_1 X_1 + \dots + \vartheta_t X_t) \overset{(1)}{=} \pi'(\vartheta_1 X_1 + \dots + \vartheta_t X_t) + (\deg \geq 2) \\ F^{\varphi} \circ f &\underset{\substack{(1)\\ \text{for } f}}{=} F^{\varphi}(\pi X_1 + \dots + \pi X_t) + (\deg \geq 2) \end{aligned}\right\} \text{equal by def of } \Theta^L_{\pi,\pi'}$$

$G_m := f' \circ F_m - F_m^{\varphi} \circ f$. Then it follows that $G_m \equiv F_m^q - F_m^{\varphi}(x_1^q, \dots, x_m^q) \equiv 0 \mod m_L$

$\Rightarrow$ all coeffs of G_m are in $\pi' \mathcal{O}_L$

Define H_{m+1} homogeneous in degree $m+1$ s.t. $H_{m+1} = F_{m+1} - F_m$. (Where F_{m+1} is still yet to be defined.)

We need: $f' \circ F_{m+1} - F_{m+1}^{\varphi} \circ f \equiv G_m + (f' \circ H_{m+1} - H_{m+1}^{\varphi} \circ f) + (\deg \geq m+2)$

$$\equiv G_m + (\pi' H_{m+1} - \pi^{m+1} H_{m+1}^{\varphi})$$ by homogeneity

For any monomial of deg $m+1$ appearing in H_{m+1}, let $\pi'\beta$ be its coefficient in our equation, $\beta \in \mathcal{O}_L$. $\quad \pi'\beta + \pi'\alpha - \pi^{m+1}\alpha^q = 0 \quad (\dagger)$

<u>Claim.</u> $\alpha := -\beta - \sum_{i=1}^{\infty} \left(\frac{\pi^{m+1}}{\pi'}\right)^{1+\varphi+\varphi^{i-1}} \beta^{\varphi^i}$

$$= -\beta - \beta^{\varphi} - \left(\frac{\pi^{m+1}}{\pi'}\right)^{1+\varphi} \beta^2 + \dots \quad \text{satisfies } (\dagger)$$

Pf. The power series converges. Plugging in shows the claim.
(Cf. proof of Hilbert 90)

Thus existence is settled. Now we turn to uniqueness.

↯ Suppose $\alpha_1 \neq \alpha_2$. Let $\gamma := \frac{\pi^{m+1}}{\pi'}$; then $(\dagger) \Leftrightarrow \alpha - \gamma\alpha^{\varphi} = \beta$.

$\Rightarrow \alpha_1 - \alpha_2 = \gamma(\alpha_1^{\varphi} - \alpha_2^{\varphi}) \Rightarrow v_L(\alpha_1 - \alpha_2) = v_L(\gamma) + v_L(\alpha_1^{\varphi} - \alpha_2^{\varphi})$

$\alpha_1 - \alpha_2 \neq 0 \Rightarrow \alpha_1 - \alpha_2 \in L^\times \Rightarrow v_L(\gamma) = 0$ ↯ ≥ 1.

<u>Prop.</u> $f, f' \in \mathcal{O}_L[[X]]$ as above with lin coeffs π, π' resp. Then

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

2) $\exists!\, [\cdot]_{ff'} : \Theta^L_{\pi,\pi'} \longrightarrow m_L \mathcal{O}_L[[X]]$ s.t. $[\vartheta]_{f,f'} = \vartheta X + (\deg \geq 2)$,
$$f' \circ [\vartheta]_{f,f'} = [\vartheta]^{\varphi}_{f,f'} \circ f$$
It satisfies $[\vartheta]_{f,f'} + [\vartheta']_{f,f'} = [\vartheta + \vartheta']_{f,f'}$ and if $\tilde{\vartheta} \in \Theta^L_{\pi,\pi'}$ then
$[\tilde{\vartheta}\vartheta]_{ff''} = [\tilde{\vartheta}]_{f'f''} \circ [\vartheta]_{ff'}$ where f'', π'' are a pair as above.

3) $[\vartheta]_{f,f'} \in \mathrm{Hom}_{\mathcal{O}_L}(F_f, F_{f'}) \quad \forall \vartheta \in \Theta^L_{\pi,\pi'}$

<u>Def.</u> For an $f \in \mathcal{O}_L[[X]]$, <u>F_f</u> is the <u>Lubin–Tate formal group</u> of f.

Cf. Lubin–Tate: "Formal complex multiplication for local fields"

In char 0: alg groups $\rightsquigarrow$ Lie groups.

However, there are problems in char p, hence the introduction of formal gps.
These are "between" alg gps and Lie gps.

Literature: Silverman: E.C.

Fröhlich: Formal Gps.

Lazard: Comm. F. G.

Iwasawa: LCFT

04.12.2018

Prop. (recap) f, f' as before. Then

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

2) $\exists! \ [\cdot]_{f,f'} : \Theta^L_{\pi,\pi'} \longrightarrow X\mathbb{Q}[[X]]$ s.t. $[\vartheta]_{f,f'}(X) = \vartheta X + (\deg \geq 2)$,

$$f' \circ [\vartheta]_{f,f'} = [\vartheta]^{\varphi}_{f,f'} \circ f$$

with a) $[\vartheta]_{f,f'} +_{F_f} [\vartheta']_{f,f'} = [\vartheta + \vartheta]_{f,f'} \quad \forall \vartheta, \vartheta \in \Theta^L_{\pi,\pi'}$

b) $[\vartheta_2]_{f',f''} \circ [\vartheta_1]_{f,f'} = [\vartheta_1 \vartheta_2]_{f,f''} \quad \forall \vartheta_1 \in \Theta^L_{\pi,\pi'}, \ \forall \vartheta_2 \in \Theta^L_{\pi',\pi''} \quad (\Rightarrow \vartheta_1\vartheta_2 \in \Theta^L_{\pi,\pi''})$

c) $[\vartheta]_{f,f'} \in \mathrm{Hom}_{\mathbb{Q}}(F_f, F_{f'}) \quad \forall \vartheta \in \Theta^L_{\pi,\pi'}$

Pf: First note that $\vartheta, \vartheta' \in \Theta^L_{\pi,\pi'} \Rightarrow \vartheta + \vartheta' \in \Theta^L_{\pi,\pi'}$:

$$\frac{\vartheta^{\varphi}}{\vartheta} = \frac{\vartheta'^{\varphi}}{\vartheta'} = \frac{\pi'}{\pi} \Rightarrow \frac{(\vartheta' + \vartheta)^{\varphi}}{\vartheta + \vartheta} = \frac{\pi'}{\pi}$$

Hence a) makes sense indeed.

1) Use Lemma with $\pi' = \pi$, $f' = f$, $t = 2$, $\vartheta_1 = \vartheta_2 = 1$, $F \equiv X + Y + (\deg \geq 2)$ and define F_f as the output of the Lemma.

A priori F_f need not be a formal gp, but if it is, $f \in \mathrm{Hom}_{\mathcal{O}_L}(F_f, F_f^{\varphi})$ automatically holds.

Checking axioms:

- first order ✓
- associativity: $F_f(F_f(X,Y), Z) \stackrel{?}{=} F_f(X, F_f(Y,Z))$

  Use Lemma with $t = 3$, $\vartheta_1 = \vartheta_2 = \vartheta_3 = 1$, same uniformisers.

  LHS $= (X+Y) + Z + (\deg \geq 2)$, RHS $= X + (Y + Z) + (\deg \geq 2)$ agree in first order

  Uniqueness in Lemma $\Rightarrow$ LHS = RHS ✓
- commutativity: same idea, use uniqueness in Lemma for $F_f(Y,X)$

  $\Rightarrow$ first order $X + Y + \ldots = Y + X + \ldots \Rightarrow$ ✓

2) Use Lemma for ϑ as given. Use uniqueness a lot to prove the rest.

Ex. $K := \mathbb{Q}_p$, $\pi := p$, $f := (1+X)^p - 1 = \sum_{j=1}^{p} \binom{p}{j} X^j = pX + p \cdot (\ldots) + X^p$

$\Rightarrow f(X) = pX + (\deg \geq 2)$ ✓, $f(X) \equiv X^p \pmod{m_L}$ ✓ All conditions are satisfied.

$\Rightarrow$ get F_f associated LT formal gp, $F_f \simeq \widehat{\mathbb{G}}_m$. To see this, check in first order terms.

LCFT, lecture 16–17

<u>Rmk.</u> 1) $[\cdot]_{f,f}: \mathcal{O}_K \longrightarrow \mathrm{End}_{\mathcal{O}_L}(F_f)$ is injective: if an elt is sent to zero, it must be zero in 1st order, use uniqueness.

2) $\vartheta \in \Theta^L_{\pi,\pi'} \cap \mathcal{O}_L^\times \Rightarrow [\vartheta]_{f,f'}$ is an iso $/\mathcal{O}_L$ of formal gps with inverse $[\vartheta^{-1}]_{f',f}$:

$$[\vartheta]\circ[\vartheta^{-1}]_{..} = [\vartheta\cdot\vartheta^{-1}]_{..} = [1]_{..,} \quad \text{use uniqueness.}$$

<u>Ex.</u> Note that $\pi \in \Theta^L_{\pi,\pi^\varphi}$ as $\frac{\pi^\varphi}{\pi} = \frac{\pi^\varphi}{\pi}$. $\Rightarrow$ get $[\pi]_{f,f^\varphi} = f: F_f \longrightarrow F_f^\varphi$ by uniqueness.

<u>Def.</u> Define $\underline{f_m} := (f^{\varphi^{m-1}})\circ(f^{\varphi^{m-2}})\circ\ldots\circ f^\varphi\circ f \in \mathcal{O}_L[X]$ for $m \geq 1$, $f_0 := X$.

Notice that $f_1 = f$.

We have $f_m = [\pi^{\varphi^{m-1}}]_{f^{\varphi^{m-1}},f^{\varphi^m}} \circ [\pi^{\varphi^{m-2}}]_{f^{\varphi^{m-2}},f^{\varphi^{m-1}}} \circ \ldots \circ [\pi]_{f,f^\varphi}$

<u>Def:</u> Define $\underline{\pi_m} := \prod_{t=0}^{m-1} \pi^{\varphi^t}$.

Then $f_m = [\pi_m]_{f,f^{\varphi^m}}$

So we have constructed:

$$F_f \xrightarrow{f_1} F_f^{\varphi}$$
$$F_f \xrightarrow{f_2} F_f^{\varphi^2}$$
$$F_f \xrightarrow{f_3} F_f^{\varphi^3}$$
$$\vdots$$

cf. pp 38–39

<u>Def.</u> Let $f \in \mathcal{O}_L[X]$ be as above, with linear coefficient π. For every $m \geq 1$ let $\underline{L_f^m}$ be the splitting field of f_m.

$\underline{\mu_{f,m}} := \{\alpha \in L_f^m \mid f_m(\alpha) = 0\}$ generalised roots of unity

<u>Ex.</u> (cont.) $L = K = \mathbb{Q}_p$, $f = (X+1)^p - 1$, $F_f = \widehat{\mathbb{G}}_m \Rightarrow f_m = (1+X)^{p^m} - 1$

$\Rightarrow L_f^m = \mathbb{Q}_p(\zeta_{p^m})$, $\mu_{f,m} = \{\zeta - 1 \mid \zeta \text{ a } p^m\text{th root of unity}\}$

<u>Lemma X.</u> Let $m \geq 1$, $L' := L_f^m$ for brevity.

1) $\mu_{f,m} \subseteq \mathfrak{m}_{L'}$

2) $\forall x \in K^\times\ \forall \alpha \in \mathfrak{m}_L$: $v_L(x) = m \ \&\ \alpha \in \mu_{f,m} \iff [x]_{f,f}(\alpha) = 0$

$\iff [a](\alpha) = 0 \quad \forall a \in \mathfrak{m}_{L'}^m$

Pf: 1) After Weierstrass preparation, $f_m = $ (monic polynomial)$\cdot$(unit). ✓ But if $y \in \mu_{f,m}$, it is a root of a monic polynomial $/\mathcal{O}_L$. L'/L is a finite extn, $\mathcal{O}_{L'} = $ int closure of $\mathcal{O}_L$ in L'.

$\Rightarrow y \in \mathcal{O}_{L'}$

$\mathcal{O}_{L'} = \mathcal{O}_{L'}^\times \amalg m_L$

Sts y is not a unit. $\nexists\, y \in \mathcal{O}_{L'}^\times$. Consider $\mathcal{O}_{L'}^\times \longrightarrow k_{L'}^\times$ $\Rightarrow$ get that y is a unit mod $m_{L'}$. But if $0 = f(y) \equiv y^q \pmod{m_{L'}}$ for $q = \# k_K$.

$\Rightarrow y \equiv 0 \ (m_{L'})$ but 0 is not a unit mod $m_{L'}$ $\lightning$

2) $[x]_{f,f} = [x/\pi_m]_{f\varphi^m, f} \circ \underbrace{f_m}_{[\pi_m]_{f, f\varphi^m}}$

$v_L(\pi_m) = m \Rightarrow x/\pi_m$ is a unit

The last equivalence is done similarly. $\square$

Prop: $m \geq 1$, f, π as before.

1) $\mu_{f,m}$ is an (honest) $\mathcal{O}_K$-module with $+_F$ and $[\cdot]_f$.

$\forall \alpha \in \mu_{f,m}^\times := \mu_{f,m} \setminus \mu_{f,m-1}$ we have an iso of $\mathcal{O}_K$-modules

$$\psi: \mathcal{O}_K/m_K^m \longrightarrow \mu_{f,m}$$

$$a \bmod m_K^m \longmapsto [a]_f(\alpha)$$

2) $\cdot\ L_f^m = L(\alpha)$, i.e. α is a primitive elt for L_f^m/L.

$\cdot\ N_{L_f^m/L}(-\alpha) = \pi^{\varphi^{m-1}}$

$\cdot\ \alpha$ is a uniformiser of L_f^m

Moreover, L_f^m/L is a tot ram Gal. extn of degree $\# \mu_{f,m}^\times = q^{m-1}\cdot(q-1)$

Pf: 1): $\mu_{f,m} \subseteq m_{L'}$ by prev. Prop. Since $F_f \in \mathcal{O}_L[[X,Y]]$ and $\underbrace{[\cdot]_{f,f}}_{=:[\cdot]_f \text{ in some books}} \in \mathcal{O}_L[[X]]$, it follows $F_f(-,-)$ and $[\cdot]_{f,f'}$ converge in $m_{L'}$.

$F_f(m_L) := \{y \in m_L\}$ with $y + y' := F_f(y,y')$ and $\alpha \cdot y := [\alpha]_{f,f}(y)$ $\forall \alpha \in \mathcal{O}_K$

$\longrightarrow F_f(m_L)$ has an honest $\mathcal{O}_K$-module structure.

06.12.2018.

Better defs: by Weierstrass preparation: $f_m = \pi^i \cdot g \cdot u$, $u \in \mathcal{O}[[X]]^\times$, g

mod m: LHS $\not\equiv 0$, but RHS $\not\equiv 0$ iff $i = 0$ $\Rightarrow f_m = g \cdot u$

$g = X^{\deg(g)} + \pi \cdot (\dots)$ $\Rightarrow X^{q^m} \equiv X^{\deg(g)}\, u_0 \left(1 + \frac{u_1}{u_0} X + \frac{u_2}{u_0} X^2 + \dots\right) \Rightarrow \deg g = q^m$,

$u_0 \equiv 1$, $\frac{u_i}{u_0} \equiv 0 \bmod m$ $\Rightarrow$ g satisfies the same conditions that f did

(namely $f = \pi X + (\deg \geq 2)$, $f \equiv X^q \pmod{m_L}$)

So the better defs are: $L_f^m :=$ splitting field of g

$\mu_{f,m} := \{\alpha \in L_f^m \mid g(\alpha) = 0\}$

Cf. Iwasawa: "LCFT". His definitions are as follows:

$$\mu_{f,m} := \{\alpha \in L^{sep} \mid f(\alpha) = 0 \ \& \ \alpha \in \mathfrak{m}_{L(\alpha)}\}$$

$$L_f^m := L(\mu_{f,m})$$

We append the Prop.

Prop. 3) $\rho_{f,m}: \mathrm{Gal}(L_{f,}^m/L) \xrightarrow{\sim} \mathrm{Aut}_{\mathcal{O}_K}(\mu_{f,m}) \xrightarrow{\sim} (\mathcal{O}_K/\mathfrak{m}_K^m)^\times$

as α is a primitive element, this aut extends to an L-algebra map $\longleftrightarrow (\alpha \mapsto [u]_f(\alpha)) \longleftrightarrow u$

Pf: 1) Haven't checked yet: $x + y,\ a \cdot x \overset{?}{\in} \mu_{f,m}$.

$\alpha \in \mu_{f,m} \overset{*}{\Leftrightarrow} [b]_{f,f}(\alpha) = 0 \quad \forall b \in \mathfrak{m}_K^m$

Hence $x \in \mu_{f,m} \Rightarrow \underbrace{[b]_{f,f}[a]_{f,f}(x)}_{a\cdot x} = [a]_{f,f}\underbrace{[b]_{f,f}(x)}_{\overset{*}{=}0} = 0 \quad \forall b$, i.e. $a \cdot x \in \mu_{f,m}$

Similarly: $x, y \in \mu_{f,m} \Rightarrow \forall b \in \mathfrak{m}_L^m: [b]_f x = [b]_f y = 0$

$\Rightarrow [b]_f(x \underset{F_f}{+} y) = [b]x \underset{F_f}{+} [b]y = F_f(0,0) = 0.$ ✓

So $F_f(\mathfrak{m}_L)$ indeed has an $\mathcal{O}_K$-module structure.

We know that $\mathcal{O}_K \xrightarrow{\hat{\psi}} \mu_{f,m}$ is an $\mathcal{O}_K$-module homomorphism,

$[a_1 + a_2]_f = [a_1]_f \underset{F_f}{+} [a_2]_f, \quad [a_1 \cdot a_2]_f = [a_1]_f \cdot [a_2]_f$

If $a \in \mathfrak{m}_K^m \Rightarrow [a]_f x = 0 \quad \forall x \in \mu_{f,m} \Rightarrow \mathfrak{m}_K^m \subseteq \mathrm{Ker}\,\hat{\psi}$, $\hat{\psi}$ descends to the map $\psi: \mathcal{O}_K/\mathfrak{m}_K^m \longrightarrow \mu_{f,m}$.

Claim. ψ is injective.

Pf: $\alpha \in \mu_{f,m} \setminus \mu_{f,m-1} \Rightarrow \exists a \in \mathfrak{m}_K^{m-1}: [a]\alpha \neq 0$.

Claim. ψ is surjective.

Pf: $\#|\mathcal{O}_K/\mathfrak{m}_K^m| = q^m$ because $\mathfrak{m}_K^{m-1}/\mathfrak{m}_K^m \hookrightarrow \mathcal{O}_K/\mathfrak{m}_K^m \twoheadrightarrow \mathcal{O}_K/\mathfrak{m}_K^{m-1} \Rightarrow \mathfrak{m}_K^{m-1}/\mathfrak{m}_K \simeq \mathcal{O}_K/\mathfrak{m}_K \simeq \mathbb{F}_q$

and induction.

distinguished part

$\mu_{f,m} = \{\alpha \in L^{sep} \mid f_m(\alpha) = 0\}$ Seen: deg(distinguished part of f_m) $= q^m$

Since $f_m = f^{\varphi^{m-1}} \circ \dots \circ f^{\varphi} \circ f$, $\#\mu_{f,m} \leqq q^m$. So we are done by injectivity.

$\Rightarrow \psi$ is an iso of $\mathcal{O}_K$-modules.

Rmk. It also follows that $\mu_{f,m}^{\times} = \{\text{roots of distinguished part of } f_m\}$

2) We have $\mu_{f,m} \subseteq L(\alpha)$ and L_f^m/L is Galois.

The constant term of f_m / f_{m-1} is:

$$f = \pi X + (\deg \geq 2) \Rightarrow f_m = \pi^{\varphi^{m-1}} \cdots \pi^{\varphi} \pi X + (\deg \geq 2) \Rightarrow \text{const coeff of } \frac{f_m}{f_{m-1}} = \pi^{\varphi^{m-1}}$$

$$\Rightarrow \pi^{\varphi^{m-1}} = \prod_{\alpha \in \mu_{f,m}^{\times}} (-\alpha) \underset{\substack{\uparrow \\ L_f^m/L \text{ is Galois}}}{=} N(-\alpha) \qquad (\#)$$

Take $v_{L_f^m}(-)$ of $(\#)$: $\quad e(L_f^m/L) = \sum_{\alpha \in \mu_{f,m}^{\times}} \underbrace{v_{L_f^m}(-\alpha)}_{\geq 1} \geq \# \mu_{f,m}^{\times} = \# \mu_{f,m} - \# \mu_{f,m-1} = q^{m-1}(q-1)$

$$\deg \left(\frac{f_m^{dp}}{f_{m-1}^{dp}} \right) \overset{*}{=} \underbrace{q^{m-1}(q-1)}_{\geq (L_f^m : L) = e(L_f^m/L) \cdot f(L_f^m/L) \geq q^{m-1}(q-1) \cdot 1} \quad \text{where } \_^{dp} \text{ denotes the distinguished piece.}$$

$\Rightarrow$ have equality, $f(L_f^m/L) = 1$, L_f^m/L is totally ramified of degree $\# \mu_{f,m}^{\times} = q^{m-1}(q-1)$

Also α is a primitive elt.

* Roots of $\frac{f_m^{dp}}{f_{m-1}^{dp}}$ correspond to elts of $\mu_{f,m} \setminus \mu_{f,m-1}$.

11.12.2018

To give a better insight, consider the following example:

$K := \mathbb{Q}_p$, $k_K = \mathbb{F}_p$, $L := K = \mathbb{Q}_p$, $\varphi := id$, $f = (1+X)^p - 1 = pX + (\deg \geq 2)$,

$\pi = p$ uniformiser, $f \equiv X^p \pmod{p}$

Claim. $F_f = \hat{\mathbb{G}}_m$

Pf: Uniqueness $\Rightarrow$ sts $f \in \mathrm{Hom}_{\mathbb{Z}_p}(F_{\hat{\mathbb{G}}_m}, F_{\hat{\mathbb{G}}_m})$.

Recall: $F_{\hat{\mathbb{G}}_m} = X + Y + XY = (X+1)(Y+1) - 1$ (this looks more like a multiplication, just with a little twist of adding / substracting 1)

$f = (1+X)^p - 1$

Multiplication is compatible w/ taking $(-)^p$. This proves the Claim. ©

Already known: $f_m = [\pi_m]_{f, f^{\varphi^m}}$ for $\pi_m = \prod_{t=0}^{m-1} \pi^{\varphi^t}$

$f_m = (1+X)^{p^m} - 1$, $\pi_m = p^m$, $f_m = [p^m]_{f,f}$

$L_f^m = (\mathbb{Q}_p)_f^m = \mathbb{Q}_p(\zeta - 1 \mid \zeta \text{ a } p^m\text{th root of } 1)$, $\mu_{f,m} = \{\zeta - 1 \mid \zeta \text{ a } p^m\text{th root of } 1\}$

Recall Lemma X; p. 37.

$$[a](X) = [\underbrace{1 + \cdots + 1}_{a \text{ times}}]_{f,f}(X) = \underbrace{X \underset{F_f}{+} \cdots \underset{F_f}{+} X}_{a \text{ times}} = (1+X)^a - 1$$

Also recall $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$

$$\mu_{f,m} = \{\zeta - 1 \mid \zeta \text{ root of } 1\} \underset{\text{Set}}{\simeq} \underbrace{\{\zeta \mid p^m\text{th root of } 1\}}_{\mathbb{Z}/p^m\mathbb{Z}\text{ - module}}$$

$\mu^\times_{f,m} = \{ \zeta \text{ primitive } p^m\text{th root of } 1\}$

Pf of surjectivity of ψ again: (cf. p. 39)

$$\mathcal{O}_K/m_K \xrightarrow[\cdot \pi_K]{\sim} m_K/m_K^2 \xrightarrow[\cdot \pi_K]{\sim} m_K^2/m_K^3 \xrightarrow{\sim} \dots \Rightarrow \# \left| m_K^i / m_K^{i+1} \right| = \# \mathbb{F}_q = q$$

$$m_K^i/m_K^{i+1} \hookrightarrow \mathcal{O}_K/m_K^{i+1} \twoheadrightarrow \mathcal{O}_K/m_K^i \quad \text{exact} \Rightarrow \# \left|\mathcal{O}_K/m_K^{i+1}\right| = \# \left| m_K^i/m_K^{i+1}\right| \cdot \# \left|\mathcal{O}_K/m_K^i\right|$$

Induction $\longrightarrow \# \left|\mathcal{O}_K/m_K^m\right| = q^m$.

$\mathcal{O}_K/m_K^m \simeq \mathbb{Z}_p/p^m\mathbb{Z}_p \simeq \mathbb{Z}/p^m\mathbb{Z}$ has $\# = p^m$

$\# \left|\mathcal{O}_K/m_K^m\right| = q^m = \deg(\text{dist part of } f_m) \geq \# \mu_{f,m} \geq q^m$ by injectivity of ψ

We must have equality $\Rightarrow$ surjectivity. ✓

Rmk. $f(X) = \pi X + (\deg \geq 2) \Rightarrow f(0) = 0$

$f_m = f^{\varphi^{m-1}} \circ f_{m-1} \Rightarrow f_m(0) = 0$

$\Rightarrow$ all roots of dist part of f_{m-1} are also roots of dist part of f_m

$\Rightarrow \mu_{f,1} \subseteq \mu_{f,2} \subseteq \mu_{f,3} \subseteq \dots$ (a p^{m-1}th root of 1 is also a p^mth root of 1)

$\Rightarrow f_m/f_{m-1} \in \mathcal{O}_L[\![X]\!]$ (Weierstrass prep.) (We need not worry about multiple roots by $\hookrightarrow$)

Moreover, $\dfrac{dp(f_m)}{dp(f_{m-1})} \in \mathcal{O}_L[X]$

$\Rightarrow \mu^\times_{f,m} = \mu_{f,m} \setminus \mu_{f,m-1} = \left\{ \text{roots of } \dfrac{dp(f_m)}{dp(f_{m-1})} \right\}$

$dp(f_m) = (X+1)^{p^m} - 1$

Claim $\mu_{f,m} \subseteq L(\alpha)$

$$\begin{tikzcd}[column sep=small] L_f^m \arrow[dr, dash] \arrow[ddr, dash] & \\ & L(\alpha) \arrow[d, dash] \\ & L \arrow[d, dash] \\ & K \end{tikzcd}$$

Pf: ψ iso, $[a]_{f,f} \in \mathcal{O}_L[\![X]\!] \Rightarrow [a]_{f,f}(\alpha) \in L(\alpha)$

$L(\alpha)/L$ already has the properties of a splitting field.

$\Rightarrow L(\alpha) = L_f^m \Rightarrow L' := L_f^m$ is Galois over L

ζ primitive root of 1 $\Rightarrow$ generates all p^mth roots of 1

$$\begin{tikzcd}[column sep=small] \mathbb{Q}_p(p^m\text{th roots of } 1) \arrow[dr, dash] \arrow[ddr, dash] & \\ & \mathbb{Q}_p(\zeta) \arrow[d, dash] \\ & \mathbb{Q}_p \end{tikzcd}$$

$f = \pi X + (\deg \geq 2) \Rightarrow \underbrace{\dfrac{f_m}{f_{m-1}}} = \pi^{\varphi^{m-1}} + (\deg \geq 1)$

$$= \frac{\pi^{\varphi^{m-1}} \pi^{\varphi^{m-2}} \cdots \pi X + (\deg \geq 2)}{\pi^{\varphi^{m-2}} \cdots \pi X + (\deg \geq 2)} \quad \text{by def of } f_m, f_{m-1}$$

$\dfrac{f_m(X)}{f_{m-1}(X)} = \left(\prod_{\beta \in \mu^\times_{f,m}} (X - \beta) \right) (\ldots)$ Subst. $X := 0$. $\longrightarrow \pi^{\varphi^{m-1}} = \left(\prod_{\beta \in \mu^\times_{f,m}} (-\beta) \right) \underbrace{(\ldots)}_{\text{unit in } \mathcal{O}_L}$

requires a bit more computation $\longrightarrow = N_{L'|L}(-\alpha)$

because L'/L is Galois and α is a primitive element of this extension.

(actually, we don't even need that $= N_{L'/L}(-\alpha)$ part for the rest of the pf.)

(*) $v_{L'}\left(\pi^{\varphi^{m-1}}\right) = \sum_{\beta \in \mu^\times_{f,m}} v_L(+\beta)$ by disregarding units

$\dfrac{f_m}{f_{m-1}} = \underbrace{\dfrac{(X+1)^{p^m} - 1}{(X+1)^{p^{m-1}} - 1}}_{\Phi_{p^m}(X)}$, plug in $X := 1 \longrightarrow p = \prod (1 - \zeta)$

ζ prim. p^mth root of 1

$v_{L'}\left(\pi^{\varphi^{m-1}}\right) = e(L'/L)$

$\beta \in \mu_{f,m} \Rightarrow \beta \in m_L$ by Lemma X (p. 37),

$\sum v_L(\beta) \geq \# \mu^\times_{f,m}$ $\quad v_L(\beta) \geq 1$ (**)

$\# \mu^\times_{f,m} = \deg\left(\dfrac{d_p f_m}{d_p f_{m-1}}\right) \Rightarrow (L' : L) \geq \deg\left(\dfrac{d_p f_m}{d_p f_{m-1}}\right)$

But $(L' : L) = \deg(\text{minpoly of } \alpha / L)$ and $(L' : L) = e(L'/L) \cdot f(L'/L)$

$\Rightarrow f(L'/L) = 1$, L'/L is tot ramified

$(L' : L) \geq \# \mu^\times_{f,m} \geq (L' : L) \Rightarrow (L' : L) = \# \mu^\times_{f,m} = \deg(\text{minpoly of } \alpha / L)$

$\alpha \in \mu^\times_{f,m}$ is a root of $\dfrac{d_p(f_m)}{d_p(f_{m-1})} \Rightarrow \underbrace{\text{minpoly}(\alpha)}_{\deg = \# \mu^\times_{f,m}} \Bigm| \underbrace{\dfrac{d_p(f_m)}{d_p(f_{m-1})}}_{\deg = \# \mu^\times_{f,m}}$

$\Rightarrow \dfrac{d_p(f_m)}{d_p(f_{m-1})}$ is irreducible because it is a scalar multiple of the minpoly.

(*) $\rightarrow \forall v_L(\beta) = 1$ since we must have equality in (**)

$\Rightarrow$ all elements of $\mu^\times_{f,m}$ are uniformisers of L^f_m.

3): $\sigma \in Gal(L'/L) \Rightarrow \forall x, y \in m_{L'}: \sigma(F(x,y)) = F(\sigma x, \sigma y)$ & $\sigma([a]_{f,f}(x)) = [a]_{f,f}(\sigma x)$

since $F \in O_L[\![X,Y]\!]$ and $[a]_{f,f} \in O_L[\![X]\!]$

$\Rightarrow Gal(L'/L) \curvearrowright \mu_{f,m}$ via O_K-module automorphisms

$\Rightarrow$ get $\rho_{f,m}: Gal(L'/L) \xrightarrow[\text{Grp}]{} Aut_{O_K}(\mu_{f,m}) \xrightarrow{\psi} Aut_{O_K}\left(O_K/m_K^m\right) \simeq \left(O_K/m_K^m\right)^\times$

$\rho_{f,m}$ is injective by def

$\rho_{f,m}$ is surjective: $\left.\begin{array}{l} \# Gal(L'/L) = (L':L) = \# \mu_{f,m} = q^m - q^{m-1} \\ \# O_K/m_K^m = q^m - q^{m-1} \end{array}\right\}$

$\rightarrow \rho_{f,m}$ is an iso.

$K/\mathbb{Q}_p$ fin ext, $K^\times \longrightarrow Gal(K^{ab}/K)$ 13.12.2018

Dream: make this "almost" an iso of gps

$\rightarrow$ would be nice to understand ramification filtration of RHS in terms of $K^\times$

<u>Motivating example.</u> $K = \mathbb{Q}_p$

$\mathbb{Q}_p^{ab} = \bigcup \mathbb{Q}_p(\zeta_n)$ LKW

$(\mathbb{Z}/m)^\times \xrightarrow{\sim} Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$

$\prod \mathbb{Z}_p \simeq \hat{\mathbb{Z}} = \varprojlim (\mathbb{Z}/m)^\times = Gal(\mathbb{Q}_p^{ab}/\mathbb{Q})$

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}_p^{ab} \arrow[dl, dash] \arrow[dr, dash] & \\ \bigcup_{p\nmid m} \mathbb{Q}_p(\zeta_m) \arrow[dr, dash] & & \bigcup_{p\mid m} \mathbb{Q}_p(\zeta_m) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

<u>General story.</u>

$$\begin{tikzcd}[column sep=small] & \text{compositum} \arrow[dl, dash] \arrow[dr, dash] & \\ \bigcup_{m\geq 1} K_f^m \arrow[dr, dash, "\text{ab tamely ram.}"'] & & \bigcup_{p\nmid m} K(\zeta_m) = K^{ur} \arrow[dl, dash, "\text{Gal, max ur}"] \\ & K & \end{tikzcd}$$

$Gal(K^{ur}/K) \simeq Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q) \simeq \hat{\mathbb{Z}}$

$\varprojlim \left(O_K/m_K^m\right)^\times \simeq O_K$

$O_K^\times \longrightarrow K^\times \xrightarrow{v_K} \mathbb{Z}$ here we define the maps using a uniformiser, which is not canonical

To get a uniform theory, let L/K be a fin ur ext.

$$\begin{tikzcd}[column sep=small] K^{ur} \arrow[d, dash] & \bigcup_{m\geq 1} L_f^m \arrow[dl, dash, "\text{ab tot ram}"] \\ L \arrow[d, dash, "\text{fin ur}"] & \\ K & \end{tikzcd}$$

After we set up the theory we will see that everything is choice-independent. Then take $L := K$ and get the theory we want. (The interesting thing is that we cannot do this without introducing L.)

Def. $(-)^{(i)} := (-)^{\varphi^i}$ for brevity

$\mu^{(i)}_{f,m} := \mu_{f^{(i)},m} = \mu_{f^{\varphi^i},m}$

Recall: $f_m = f^{\varphi^{m-1}} \circ \dots f^{\varphi} \circ f$

$$\pi_m = \prod_{t=0}^{m-1} \pi^{\varphi^t} \quad (m \geq 0) \longrightarrow \pi_1 = \pi, \quad \pi_0 = 1, \quad [\pi_m]_{f, f^{(m)}} = f_m$$

Lemma. We can extend the def of π_m for $m \in \mathbb{Z}$: $\pi_m \in L^\times$ s.t.

1) for $m \geq 0$, the new def agrees with the old one

2) $\pi_{j+j'} = \pi_{j'}^{(j)} \cdot \pi_j \quad \forall j, j' \in \mathbb{Z}$ "Numerical Lemma"

3) $\vartheta \in \Theta^L_{\pi,\pi'} \Rightarrow \dfrac{\vartheta^{(j)}}{\vartheta} = \dfrac{\pi'_j}{\pi_j} \quad \forall j \in \mathbb{Z}$

4) $\pi_j \in \Theta^L_{\pi, \pi^{(j)}}$

PO, nothing happens in the pf. □

Lemma. $f, f' \in \mathcal{O}_L[\![X]\!]$, $f = \pi X + (\deg \geq 2)$, $f \equiv X^q \pmod{m_L}$, same for f'.

If $\vartheta \in \Theta^{L,\times}_{\pi,\pi'}$ then $\forall m \geq 1$: $[\vartheta] := [\vartheta]_{f,f'}$ defines an $\mathcal{O}_K$-module iso

$$\begin{aligned} \mu_{f,m} &\longrightarrow \mu_{f',m} \\ x &\longmapsto [\vartheta](x) \end{aligned}$$

and moreover $L^m_f = L^m_{f'}$.

Pf: Given such a ϑ, $\exists! \, [\vartheta]_{f,f'} \in X\mathcal{O}_L[\![X]\!]$ s.t. $[\vartheta]_{f,f'} = \vartheta X + (\deg \geq 2)$,

$f' \circ [\vartheta]_{f,f'} = [\vartheta]^{\varphi}_{f,f'} \circ f$.

$f'_m = [\pi'_m]_{f', f'^{\varphi^m}}$, $\quad f_m = [\pi_m]_{f, f^{\varphi^m}}$

$$[\vartheta]^{(m)}_{f,f'} \circ f_m = [\vartheta^{(m)}]_{f^{\varphi^m}, f'^{\varphi^m}} \circ [\pi]_{f, f^{\varphi^m}}$$

$$= [\vartheta^{(m)} \cdot \pi]_{f', f'^{\varphi^m}}$$

Analogously for $f'_m \circ [\vartheta]_{f,f'} \Rightarrow f'_m \circ [\vartheta] = [\vartheta]^{(m)} \circ f_m$

Precompose this scalar multiplication operation with any $[a]_{f,f}$ and use compatibility to see that $[\vartheta]$ is an $\mathcal{O}_K$-module hom. on $\mu_{f,m}$.

Since ϑ is a unit, ϑ^{-1} gives an inverse $\longrightarrow$ $[\vartheta]$ is an iso.

$\mu_{f,m} = [\vartheta](\mu_{f,m})$ since $[\vartheta]$ is an iso

$$\underbrace{[\vartheta](\overbrace{\mu_{f,m}}^{\subseteq L^m_f})}_{\subseteq L^m_f}$$

$\subseteq L^m_f$ since L is complete ($\Leftarrow$ limit of power series)

But we know that $L^m_{f'} = L(\mu_{f',m})$. Hence $L^m_f = L^m_{f'}$. □

Def. K'/K Galois, its <u>Weil group</u> is $W(K'/K) := \{\sigma \in \mathrm{Gal}(K'/K) \mid \sigma|_{K' \cap K^{ur}} \in \mathrm{Gal}(K' \cap K^{ur}/K)$ is an integer power of the arithmetic Frobenius$\}$

Note: $\mathrm{Gal}(K' \cap K^{ur}/K) \simeq \mathrm{Gal}(k_{K'}/k_K) \simeq \hat{\mathbb{Z}}$.

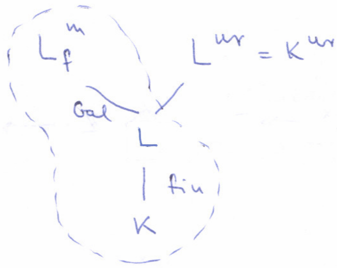
Rmk. If $K' \supseteq K^{ur}$ then $W(K'/K) = \{\sigma \in \mathrm{Gal}(K'/K) \mid \sigma|_{K^{ur}} \in \mathbb{Z} \subseteq \hat{\mathbb{Z}}\}$

Prop. $m \geq 1$, $f \in \mathcal{O}_L[\![X]\!]$, $f = \pi X + (\deg \geq 2)$, $f \equiv X^q \pmod{m_L}$

1) L_f^m/K is Galois and $\forall \alpha \in \mu_{f,m}^\times$:

$$K^\times/(1+m_K^m) \xrightarrow[\text{set}]{\sim} \coprod_{j \in \mathbb{Z}} \mu_{f,m}^{(j),\times}$$

$$x \longmapsto [x\pi_j]_{f,f^{(j)}}(\alpha) \quad \text{for } v_K(x) = -j$$



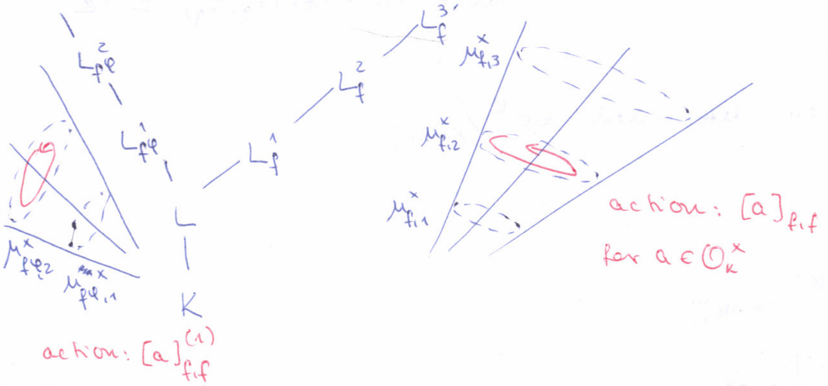
2) $\breve{K} :=$ max ur ext of K (see Problem Sheet 8). Then $\rho_{f,m}$ extends to an iso

$$\rho_{f,m} : W(\breve{K}_f^m/K) \xrightarrow{\sim} K^\times/(1+m_K^m)$$

$$\left(\alpha \mapsto [x\pi]_{f,f^{(j)}}(\alpha)\right) \longleftarrow x \text{ with } v_K(x) = -j$$

Idea. $\left(\mathcal{O}_K/m_K^m\right)^\times \simeq \mathrm{Gal}(L_f^m/L)$. $L_f^m = L(\alpha)$, $\alpha \in \mu_{f,m}^\times$, $\mu_{f,m}^\times$ is a full Galois orbit of α,

$\mu_{f,m}^\times$ is a $\mathrm{Gal}(L_f^m/L)$-torsor.



$L_f^m = L_{f'}^m$

The two pictures look the same.

Pf OF PROP: $v_K(x) = -j \Rightarrow x \cdot \pi_j \in \mathcal{O}^L_{\pi, \pi^{(j)}}$: $\dfrac{(x\pi_j)^\varphi}{x\pi_j} \overset{(*)}{=} \dfrac{\pi^{(j)}}{\pi}$

$\pi_j^{(j')}\pi_{j'} = \pi_{j+j'} = \pi_{j'}^{(j)} \cdot \pi_j \Rightarrow$ for $j' = 1$: $\pi_j^{(1)} \cdot \pi = \pi^{(j)} \cdot \pi \Rightarrow \dfrac{\pi_j^{(1)}}{\pi_j} = \dfrac{\pi^{(j)}}{\pi}$, $x = x^\varphi$ $\Big\} \Rightarrow (*)$

$x\pi_j \in \mathcal{O}^L_{\pi, \pi^{(j)}} \Rightarrow [x\pi_j]_{f,f^{(j)}} : \mu_{f,m} \xrightarrow{\sim} \mu_{f,m}^{(j)}$ $\mathcal{O}_K$-mod iso by Lemma.

$$\Rightarrow \underbrace{\{v_K^{-1}(j) \subseteq K^\times\}/(1+m_K^m)}_{U_K^{(m)}} \xrightarrow{\sim} \mu_{f,m}^{(j)}$$

Prev. lecture: $\mathcal{O}_K/m_K^m \xrightarrow{\sim} \mu_{f,m}$ iso of $\mathcal{O}_K$-modules

$$x \longmapsto [x\pi_j]_{f,f^{(j)}}$$

Starting again:

1) $$\mathcal{O}_K^\times/_{1+\mathfrak{m}_K^m} \xrightarrow[\text{Grp}]{\sim} \left(\mathcal{O}_K/_{\mathfrak{m}_K^m}\right)^\times \xrightarrow[\substack{\text{Grp}\\ \text{(by Prop.)}}]{\sim} \mathrm{Aut}(\mu_{f,m})$$

$$\begin{tikzcd} & \mathrm{Aut}(\mu_{f,m}) \arrow[d, "\sim\ \text{Grp (by Prop.)}"] \\ \underbrace{\mu_{f,m}^\times}_{} & \mathrm{Gal}(L_f^m/L) \arrow[l, "\sim"', "\text{Set}"] \end{tikzcd}$$

once we choose $\alpha \in \mu_{f,m}^\times$

$$\begin{tikzcd} \breve{K}_f^m \arrow[dr, dash, "\text{tot ram ab}"] \arrow[d, dash] & \\ L_f^m \arrow[dr, dash, "\text{tot ram ab}"'] & \breve{K} \arrow[d, dash] \\ & L \arrow[dl, dash] \\ K \arrow[d, dash, "\text{fin}"] & \\ \mathbb{Q}_p & \end{tikzcd}$$

$$0 \to \mathcal{O}_K^\times \to K^\times \xrightarrow{v_K} \mathbb{Z} \to 0 \quad \Rightarrow \quad K^\times \underset{\text{Set}}{\simeq} \coprod_{j\in\mathbb{Z}} \mathcal{O}_K^\times$$

$$x \mapsto x\pi_j, \quad v(x) = -j$$

This factors to $K^\times/_{\mathfrak{m}_K^m} \simeq \coprod \mathcal{O}_K^\times/_{1+\mathfrak{m}_K^m}$ by def of π_j.

2) Suppose $\sigma \in W(\breve{K}_f^m/K)$.

$\Rightarrow \sigma|_{\breve{K}} = \varphi^j$ for some $j\in\mathbb{Z}$ where φ is the ar. Frob.

α is a primitive elt of $\breve{K}_f^m/\breve{K}$ if $\alpha \in \mu_{f,m}^\times$.

Then $\sigma(\alpha) \in \mu^\times_{f^{\varphi^j},m} =: \mu^{(j),\times}_{f,m}$

$$\begin{tikzcd} \breve{K}_f^m \arrow[loop left, "\sigma"] \arrow[d, dash, "\leftarrow \alpha \text{ prim elt}"] & \\ \breve{K} \arrow[dr, dash] \arrow[dd, dash] & \\ & K^{ur} \arrow[dl, dash] \\ K & \end{tikzcd}$$

$\mu_{f,m} \simeq \mathcal{O}_K/_{\mathfrak{m}_K^m}$ as $\mathcal{O}_K$-modules

$\mu_{f^{\varphi^j},m} \simeq \mathcal{O}_K/_{\mathfrak{m}_K^m}$ as $\mathcal{O}_K$-modules

$\mathrm{Gal}(K^{ur}/K) \simeq \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \hat{\mathbb{Z}} \supseteq \mathbb{Z}$

\# By 1): $\sigma(\alpha) = [x\pi_j]_{f,f^{(j)}}(\alpha)$ for a uniquely determined $x \in K^\times/_{1+\mathfrak{m}_K^m}$

We have a natural diagram

$$\begin{tikzcd} W(\breve{K}_f^m/K) \arrow[r, "\rho_{f,m}"] \arrow[d, "\text{quot.}"'] & K^\times/_{1+\mathfrak{m}_K^m} \arrow[d, "\text{quot.}"] \\ W(\breve{K}_f^{m-1}/K) \arrow[r, "\rho_{f,m-1}"'] & K^\times/_{1+\mathfrak{m}_K^{m-1}} \end{tikzcd} \qquad \sigma \mapsto x$$

Claim.

i) x is independent of α

ii) The diagram commutes.

Pf: Any other primitive $\alpha' \in \mu_{f,m}^\times$ can be written as $\alpha' = [a]_{f,f}(\alpha)$ for some $a\in\mathcal{O}_K$.

because $\mu_{f,m} \xrightarrow[\mathcal{O}_K]{\sim} \mathcal{O}_K/_{\mathfrak{m}_K^m}$ and $\mathcal{O}_K/_{\mathfrak{m}_K^m}$ is gen by a single element, say $a \in \mathcal{O}_K \setminus \mathfrak{m}_K$

Even better, any $\alpha' \in \mu_{f,m}$ (w/o cross!) can be written as $\alpha' = [a]_{f,f}(\alpha)$ for some $a\in\mathcal{O}_K$.

Now let $\alpha' \in \mu_{f,m}$ be arbitrary. $\Rightarrow \alpha' \overset{*}{=} [a]_{f,f}(\alpha) \Rightarrow \sigma(\alpha') = \sigma\left([a]_{f,f}(\alpha)\right) =$

$$= [a]_{f,f}^{\varphi^j}(\sigma\alpha) \underset{\#}{\overset{\Uparrow}{=}} [a]_{f,f}^{\varphi^j}[x\pi_j]_{f,f^{(j)}}(\alpha) = \left([x\pi_j]_{f,f^{(j)}} \circ [a]_{f,f}\right)(\alpha) \underset{*}{\overset{\Uparrow}{=}} [x\pi_j]_{f,f^{(j)}}(\alpha')$$

So if we had done our construction w/ α' instead of α, the result would be just the same. The same also goes for $\mu^{\times}_{f,m}$, and proves i) and ii)

Claim. $\rho_{f,m}$ is a group hom.

Pf: Suppose $\sigma, \tau \in W(\breve{K}^m_f/K)$.

$\sigma(\alpha) = [x\pi_j]_{f,f^{(j)}}$ for some $x \in K^\times$, $v_K(x) = -j$

$\tau(\alpha) = [y\pi_{j'}]_{f,f^{(j')}}$ for some $y \in K^\times$, $v_K(y) = -j'$

$$\Rightarrow (\sigma\circ\tau)(\alpha) = \sigma\left([y\pi_{j'}]_{f,f^{(j')}}(\alpha)\right) = [y\pi_{j'}]_{f,f^{(j')}}(\sigma\alpha) = [y\pi_{j'}]^{(j)}_{f,f^{(j')}} \circ [x\pi_j]_{f,f^{(j)}}(\alpha)$$

$$= [y\pi_{j'}^{(j)}]_{f^{(j)},f^{(j+j')}} \circ [x\pi_j]_{f,f^{(j)}}(\alpha) = [xy\underbrace{\pi_j\pi_{j'}^{(j)}}_{\pi_{j+j'}}]_{f,f^{(j+j')}}(\alpha)$$

This also shows abelianity.

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_K^\times/1+\mathfrak{m}_K^m \arrow[r] \arrow[d, "\rho_{f,m}\ (\text{long ago})"] \arrow[dr, phantom, "\circlearrowleft"] & K^\times/1+\mathfrak{m}_K^m \arrow[r, "v_K"] \arrow[d, "\rho_{f,m}\ (\text{today})"] \arrow[dr, phantom, "\circlearrowleft"] & \mathbb{Z} \arrow[r] \arrow[d, "\sim"] & 0 \\
0 \arrow[r] & \mathrm{Gal}(\breve{K}^f_m/\breve{K}) \arrow[r] & W(\breve{K}^f_m/K) \arrow[r] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

Def. $\breve{K}^{LT}_f := \bigcup_{m\geq 1} \breve{K}^m_f$

We get a canonical iso $\rho_f : W(\breve{K}^{LT}_f/K) \xrightarrow{\sim} K^\times$.

Pf. Define ρ_f for any fin subext $\subseteq \breve{K}^m_f$ by $\rho_{f,m}$ and since we have shown compatibility, this is indep of the choice of m.

Form an inverse system along surjections of $K^\times/1+\mathfrak{m}_K^m$

$\Rightarrow \rho : W(\breve{K}^{LT}_f/K) \xrightarrow{\sim} \varprojlim$

Exercises: $\mathcal{O}_K \longrightarrow \mathcal{O}_{\breve{K}} \xrightarrow{u \mapsto \frac{u^\varphi}{u}} \mathcal{O}_{\breve{K}}$ is exact. //

The fixed field of $\breve{K}$ under φ^n is the unique deg n ur extn of K.

Prop. $\breve{K}^m_f$ and $\rho_{f,m}$ (hence $\breve{K}^{LT}_f$) are indep of the choice of f.

Pf: For f, f' with π, π' take $\theta \in \Theta^{\breve{K}}_{\pi,\pi'}$ ($\neq \emptyset$ because $\frac{\theta^\varphi}{\theta} = \frac{\pi'}{\pi}$ is solvable by #)

$\Rightarrow [\theta]_{\pi,\pi'} \in \mathcal{O}_K[[X]]$ induces an iso $\mu_{f,m} \xrightarrow[\mathcal{O}_K]{\sim} \mu_{f',m}$

Def. L/K ur fin. extn. Let $K^m := K^{ur} \cdot L_f^m$.

Prop. • The metric completion of K^m is $\breve{K} \cdot L_f^m$.

• $K^m =$ (metric completion of K^m) $\cap \bar{K}$ where $\bar{K}$ is the alg cl.

Pf: If V is a fin dim vct field over a top field F then the metric completion of V is $V \otimes_F F_{comp}$ where F_{comp} is the completion of F.

This yields the first assertion.

$\bar{K} \cap$ (metr compl of K^m) $\supseteq K^m$ is obvious. $\subseteq$ Suppose $y \in \bar{K} \cap (\text{mc of } K^m) \setminus K^m$.

Since $y \in \bar{K}$, it is algebraic, hence has a minpoly w/ fin many coeffs $\Rightarrow \exists L'/K$ fin ur extn s.t. y alg $/L'$. (L' containing all the necessary coeffs). $\Rightarrow L'(y)/L'$ fin alg extn.

$\Rightarrow L'(y)/K$ fin $\Rightarrow$ "$ef = n$" holds.

If $L'(y)/L'$ ur $\Rightarrow L'(y) \subseteq (L')^{ur} = K^{ur} \Rightarrow y \in K^{ur} \Rightarrow y \in K^m$ ↯

Hence $L'(y)/L'$ has $e \geq 2$. $\Rightarrow v_L((L')^\times) \twoheadrightarrow \frac{1}{e}\mathbb{Z}$. But this contradicts the fact that the value group does not change under metric completion. ↯ □

$\Rightarrow K^m$ is also indep of f because all K^{ur}, $\bar{K}$ and L_f^m are (the latter by Prop. on p.47.)

Def. $K^{LT} := \bigcup_{m \geq 1} K^m$

20.12.2018

We now call $\rho_{f,m}$ the local Artin map $\mathrm{Art}_K : K^\times \xrightarrow{\sim} W(K^{LT}/K)$.

LCFT: if L/K is Galois then we have

$$\begin{tikzcd}
\widehat{L^\times} \arrow[r, "\mathrm{Art}_L", "\sim"'] \arrow[d, "N_{L/K}"] \arrow[dr, phantom, "\circlearrowright"] & \mathrm{Gal}(L^{LT}/L) \arrow[d] \\
\widehat{K^\times} \arrow[r, "\sim", "\mathrm{Art}_K"'] & \mathrm{Gal}(K^{LT}/K)
\end{tikzcd}$$

The rows come from completing $K^\times \xrightarrow{\sim} W(K^{LT}/K)$.

We don't have this yet: the compatibility needs to be checked. Also, what is the right vertical map?

Next goal: if L/K is some abelian Galois extn, we wts that its subgp (coming from Galois theory) under the Artin map is its norm group.

Def. K'/K finite extn. $N(K'/K) := N_{K'/K}((K')^\times) \subseteq K^\times$ is the norm group of K'.

For K'/K algebraic but not necessarily finite, let $N(K'/K) := \bigcap_{\substack{\tilde{K}/K \\ \text{fin subext}}} N(\tilde{K}/K) \subseteq K^\times$

Lemma 1. L the unique unram extn of K of deg $n \in \mathbb{Z}_{\geq 1}$. Suppose $\theta \in \Theta^{\breve{K},\times}_{\pi,\pi'}$ for $\pi, \pi' \in L$ uniformisers. Then $\theta \in \mathcal{O}_L \Leftrightarrow N_{L/K}(\pi) = N_{L/K}(\pi')$.

Pf: Numerical Lemma: $\frac{\theta(n)}{\theta} = \frac{\pi'_n}{\pi_n}$, i.e. $\frac{\theta^{\varphi^n}}{\theta} = \frac{\pi'^{\varphi^{n-1}} \cdot \ldots \cdot \pi'}{\pi^{\varphi^{n-1}} \cdot \ldots \cdot \pi}$

L/K is Galois with $Gal(L/K) = \{1, \varphi, \ldots, \varphi^{n-1}\} \Rightarrow$ RHS $= \frac{N_{L/K}(\pi')}{N_{L/K}(\pi)}$

Lemma.
For all k, the fixed field of $\breve{K}$ under φ^k is the unique ur ext of deg k, and $N_{L/K}$ surjects onto $\{x \in K^\times \mid v_K(x) \in n\mathbb{Z}\}$.

Construction: Let $x \in K^\times$ be given s.t. $v_K(x) \geq 1$, and let L be the unique ur extn of deg $n = v_K(x)$, let π be a uniformiser of L s.t. $N_{L/K}(\pi) = x$. Such a π exists by the lemma.

Def. $K^m_x := L^m_f$ for $f \in \mathcal{O}_L[[X]]$, $f(X) = \pi X + (\deg \geq 2)$, $f \equiv X^q \pmod{m_L}$

Lemma 2. K^m_x is independent of the choice of f. (Not indep of choice of x.)

Pf: Suppose π' is another choice. $\Rightarrow N_{L/K}(\pi) = N_{L/K}(\pi') = x$

$\exists\ [\theta]_{f,f'}: \mu_{f,m} \xrightarrow{\sim} \mu_{f',m}$ with $\theta \in \Theta^{\breve{K},x}_{\pi,\pi'}$. Then by Lemma 1: $\theta \in \mathcal{O}_L^\times$

$\Rightarrow [\theta]_{f,f'} \in \mathcal{O}_L[[X]]$

Lemma 3. $\sigma \in Art_K(x)$. Then σ is characterised as the Galois automorphism in $W(K^{LT}/K)$ s.t. 1) $\sigma|_{K^{ur}}(x) = \varphi^{v_K(x)}$

2) $\sigma|_{K^m_x} = id \quad \forall m \geq 1$

$$\begin{tikzcd}
 & K^{LT} \arrow[dl, dash] \arrow[dr, dash] & \\
\bigcup_{m\geq 1} K^m_x \arrow[dr, dash] & & K^{ur} \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

Pf: $v_K(x) = n \Rightarrow Art_K(x)$ is given by 1), and

$\alpha \longmapsto [x\pi_n]_{f,f(-n)}(\alpha)$ for any $\alpha \in \mu^\times_{f,m}$.

$f \in \mathcal{O}_L[[X]]$, and the fixed field of φ^n over $\breve{K}$ is L. $\Rightarrow f^{(-n)} = f$

Also $\pi_n = \pi^{\varphi^{n-1}} \cdot \ldots \cdot \pi^{\varphi} \cdot \pi = N_{L/K}(\pi) = x$. $\Rightarrow \pi_{-n} = x^{-1}$ by the Numerical Lemma.

$\Rightarrow [x\pi_n]_{f,f(-n)}(\alpha) = [x x^{-1}]_{f,f}(\alpha) = [1]_{f,f}(\alpha) = \alpha$.

Cor. $Art_K: K^\times \xrightarrow{\sim} W(K^{LT}/K)$ induces an iso $K^\times/(x) \times U^m_K \longrightarrow Gal(K^m_x/K)$

Pf: Since $\bigcup K^m_x$ and K^{ur} are linearly disjoint over K, we can use Galois thy for each individually. Need to determine the fixed field of $\langle x \rangle$ resp. U^m_K.

$\langle x \rangle$: Lemma 2 $\Rightarrow$ x acts as the n-Frob, i.e. φ^n for $n = -v_K(x)$. $\Rightarrow (K^{ur})^{\varphi^n} = L$ is the fixed fd.

U^m_K: We have shown that Art_K extends $\rho_{f,m}$ from the totally ramified tower,

$$\rho_{f,m}: \underbrace{\left(\mathcal{O}_K/m^m_K\right)^\times}_{\mathcal{O}_K^\times/U^m_K} \xrightarrow{\sim} Gal(L^m_f/L)$$

We have seen that $\langle x\rangle \cdot U_K^m$ corresponds to the field extn K_x^m.

Prop. $N(K_x^m/K) = \langle x\rangle \cdot U_K^m$.

Def. $g \in \mathcal{O}_L[[X]] \Rightarrow N(g) \in \mathcal{O}_L[[X]]$ s.t. $N(g)\circ f = \prod_{\alpha\in\mu_{f,1}} g(X +_{F_f} \alpha)$. Coleman norm operator.

Thm. (Coleman) $\exists!\, N(g)$.

Pf: [Schneider] or [Iwasawa].

Cor. $N(g_1 \cdot g_2) = N(g_1)\cdot N(g_2)$ by uniqueness. □

Def. $N^0(g) = \mathrm{id}$, $N^m(g) := \left(N^{m-1}\left(N(g)^{\varphi^{m-1}}\right)\right)^{\varphi}$ for $m \geq 1$. □

Lemma A. $m\geq 1$: $N^m(g)\circ f_m = \prod_{\alpha\in\mu_{f,m}} g(X +_{F_f} \alpha)$

Pf: $m=1$: defining property.

$m\geq 2$: tedious induction. □

Lemma B. 1) $N(g) \equiv g^{\varphi} \pmod{m_L}$, in part $N(\mathcal{O}_L[[X]]^\times) \subseteq \mathcal{O}_L[[X]]^\times$

2) $m\geq 1$, $g \equiv 1 \pmod{m_L^m} \Rightarrow N(g) \equiv 1 \ (m_L^{m+1})$

3) $g\in \mathcal{O}_L[[X]]^\times$, $m \geq 1 \Rightarrow \dfrac{N^m(g)}{N^{m-1}(g)} \equiv 1 \pmod{m^m}$

Pf, tedious. □

Seen: $\mathrm{Gal}(K_x^m/K) \simeq K^\times / \langle x\rangle U_K^m$.

Once Prop is proven, this can be rephrased as $\mathrm{Gal}(K_x^m/K) \simeq K^\times / N(K_x^m/K)$.

PF OF PROP: $L' := K_x^m$. We know that $\alpha\in\mu_{f,m}^\times$ is a prim elt of L_f^m/L and a uniformiser.

$\Rightarrow (L')^\times \simeq \langle\alpha\rangle \times \mathcal{O}_{L'}^\times$, i.e. α splits $0 \to \mathcal{O}_{L'}^\times \to (L')^\times \underset{\langle\alpha\rangle}{\overset{v_{L'}}{\rightleftarrows}} \mathbb{Z} \to 0$. (non-canonically)

Step 1. $N_{L'/K}(\alpha) = N_{L/K}\big(\underbrace{N_{L'/L}(\alpha)}_{\text{Prop. on } L'/L}\big) = N_{L/K}\left(\pi^{\varphi^{m-1}}\right) = N_{L/K}(\pi) = x$.

construction

$\mathrm{Gal}(L/K) = \{1, \varphi, \ldots, \varphi^{n-1}\}$

Gal conjugates have the same norm

L_f^m
|
L
|
K

Step 2. Remains to show $N(\mathcal{O}_{L'}^\times) = U_K^m$.

L_f^m/L is tot ram, α is a uniformiser $\Rightarrow \mathcal{O}_{L_f^m} = \mathcal{O}_L[\alpha]$ (proven as a part of the "$ef = \deg$" formula)

For any $u\in\mathcal{O}_{L'}^\times$ $\exists g\in \mathcal{O}_L[X]$ s.t. $u = g(\alpha)$. Let $u_i := N^i(g)(0)$

$\Rightarrow u_i = \prod_{\alpha\in\mu_{f,i}} g(\alpha)$

$$\frac{u_m}{u_{m-1}} = \prod_{\alpha \in \mu^{\times}_{f,m}} g(\alpha) = \prod_{\substack{\text{Gal orbit} \\ \text{of } \alpha}} g(\sigma\alpha) = N_{L'/L}(\alpha)$$

Lemma B $\Rightarrow$ $\frac{u_m}{u_{m-1}^{\varphi}} \in 1 + m_L^m$

$$\Rightarrow N_{L'/K}(u) = N_{L/K}\left(\frac{u_m}{u_{m-1}}\right) = N_{L/K}\left(\frac{u_m}{u_{m-1}^{\varphi}}\right) \in N_{L/K}(1 + m_L^m) \subseteq 1 + m_K^m =: U_K^m$$

We still need $\supseteq$.