THE HASSE-ARF THEOREM

25/02/2021

Definition AN EXTENSION L/K OF LOCAL FIELDS IS UNRAMIFIED IF $[L:K]=[\ell:k] \iff \pi_K$ IS INERT IN L
$e=\nu_L(\pi_K)=1$

Definition L/K IS TOTALLY RAMIFIED IF $\ell=k \iff e=\nu_L(\pi_K)=[L:K]$

K LOCAL FIELD, $\mathcal{O}_K$ VALUATION RING, π_K UNIFORMIZER $\mathcal{U}=\mathcal{O}_K^\times$
k RESIDUE FIELD

Definition FILTRATION $\{\mathcal{U}_K^{(i)}\}$ OF $\mathcal{U}$. $\mathcal{U}_K^{(i)}=1+\pi_K^i\mathcal{O}_K$

Proposition $\mathcal{U}_K/\mathcal{U}_K^{(1)}\simeq k^\times$, $\mathcal{U}_K^{(i)}/\mathcal{U}_K^{(i+1)}\simeq k \quad \forall i\geq 1$

L/K IS AN EXTENSION AND $G=\mathcal{G}al(L/K)$

Definition FILTRATION OF GALOIS GROUPS

$$G_i=\{\sigma\in G \mid \nu_L(\sigma(x)-x)\geq i+1 \quad \forall x\in\mathcal{O}_L\}=$$
$$=\{\sigma\in G \mid |\sigma(x)-x|\leq|\pi_L^i| \quad \forall x\in\mathcal{O}_L\}=$$
$$=\ker(G \longrightarrow \mathrm{Aut}_K(\mathcal{O}_L/\pi_L^{i+1}))$$
$$=\{\sigma\in G \mid \sigma(x)\equiv x \mod \pi_L^{i+1} \quad \forall x\in\mathcal{O}_L\}=$$
$i_{L/K}(\sigma)=\min_{x\in\mathcal{O}_L}\{\nu_L(\sigma(x)-x)\}$
$$=\{\sigma\in G \mid i_{L/K}(\sigma)\geq i+1\}$$

$$G_{-1}=\mathcal{G}al(L/K)=G \qquad G_0=I(L/K).$$

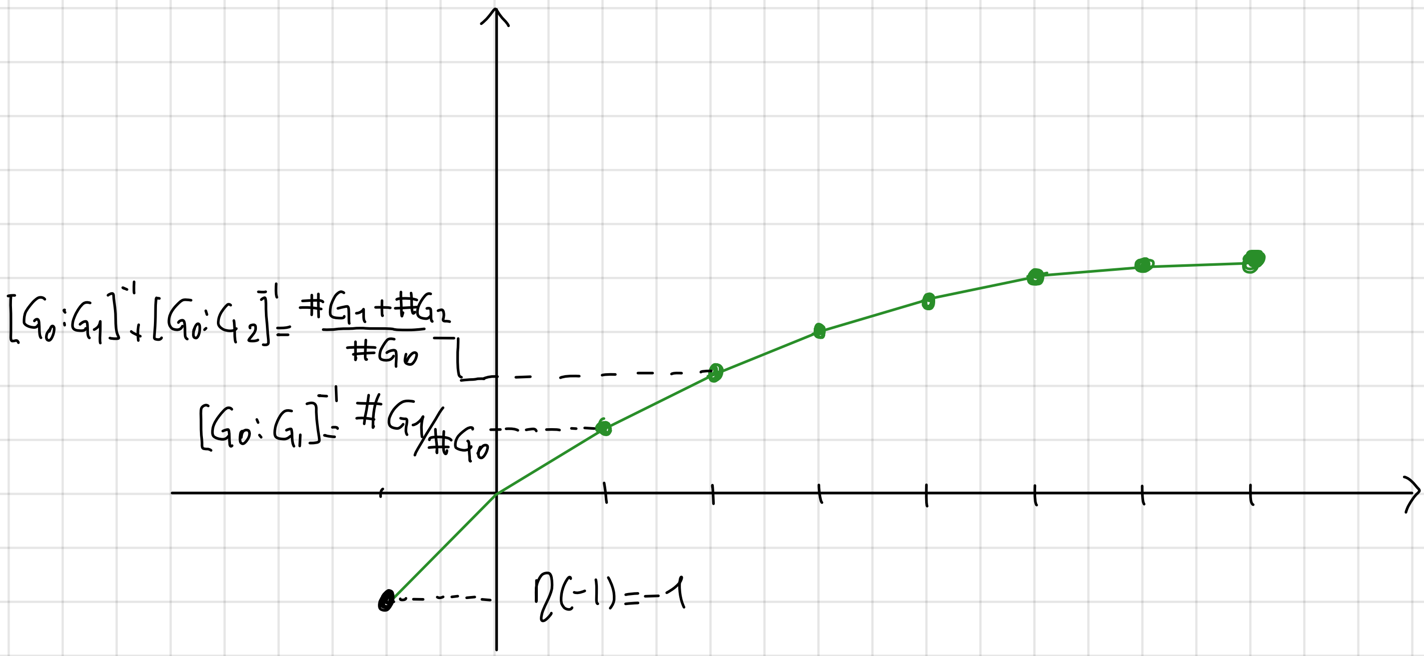
Proposition
- $G_{i+1}(L/K)\trianglelefteq G_i(L/K)$
- $G_i/G_{i+1} \hookrightarrow \mathcal{U}_L^{(i)}/\mathcal{U}_L^{(i+1)}$ IS A WELL DEFINED INJECTIVE HOMOMORPHISM
  $\sigma \longmapsto \sigma(\pi_L)/\pi_L$
  this does not depend on the choice of uniformizer
- G IS SOLVABLE

Definition (HASSE-HERBRAND TRANSITION FUNCTION)

$$\eta_{L/K}(u) = \varphi_{L/K}(u) = \int_0^u \frac{dx}{[G_0(L/K) : G_x(L/K)]}$$

This notation describes

$$\eta_{L/K}(u) = \varphi_{L/K}(u) = \begin{cases} u & -1 \le u \le 0 \\ \frac{1}{\#G_0}\left[\#G_1 + \#G_2 + \dots + \#G_m + (u-m)\#G_{m+1}\right] & m \le u \le m+1 \end{cases}$$



Remark η IS CONTINUOUS, PIECE-WISE LINEAR AND STRICTLY INCREASING. FURTHER, $\eta(s) \xrightarrow[s \to +\infty]{} +\infty$

$$\eta_{L/K}(u) = \varphi_{L/K}(u) = \left(\frac{1}{\#G_0} \sum_{\sigma \in G} \min\{i_{L/K}(\sigma), u+1\}\right) - 1$$

Remark η IS INVERTIBLE WITH INVERSE $\psi_{L/K} = \varphi_{L/K}^{-1}$
IT'S INVERSE IS CONTINUOUS, PIECEWISE LINEAR, INCREASING AND CONVEX

IF $v \in \mathbb{Z}$ THEN $m \le u = \psi_{L/K}(v) \le m+1$

$$\#G_0 v = \#G_1 + \#G_2 + \dots + \#G_m + (u-m)\#G_{m+1}$$

$$u = \frac{1}{\#G_{m+1}}\left(\#G_0 v - \#G_1 - \dots - \#G_m + m\#G_{m+1}\right)$$

Definition UPPER NUMBERING $G^{v} = G_{\psi(v)}$ $G^{\varphi(u)} = G_u$

Theorem (Herbrand) LET $M/L/K$

I. $\varphi_{M/K} = \varphi_{L/K} \circ \varphi_{M/L}$

II. $\psi_{M/K} = \psi_{M/L} \circ \psi_{L/K}$

III. UPPER NUMBERING IS ADAPTED TO QUOTIENTS

$$(G/H)^{v} = G^{v}H/H \quad \forall v$$
$$(G/H)_{s} = G_{\psi_{L/K}(s)} H/H \quad \forall s$$

IV. LOWER NUMBERING IS ADAPTED TO SUBGROUPS

$$H_n = H \cap G_n$$

Definition A BREAK IN THE UPPER NUMBERING FILTRATION $\{G^{v}\}_{v \in \mathbb{R}_{>-1}}$ OF G IS DEFINED TO BE ANY $v \in \mathbb{R}_{>-1}$ SUCH THAT

$$G^{v} \neq G^{v+\varepsilon} \quad \forall \varepsilon > 0$$

Remark IF $u_0 \in \mathbb{R}_{>-1}$ IS NOT A BREAK IN THE LOWER FILTRATION, THEN

$$G_{u_0+\varepsilon_0} = G_{u_0} \quad \text{SOME } \varepsilon_0 > 0$$

$G_{u_0+\varepsilon} = G_{u_0}$ FOR ALL $0 < \varepsilon < \varepsilon_0$ AS φ IS STRICTLY INCREASING

$$\varphi_{L/K}([u_0, u_0+\varepsilon_0]) = [s_0, s_0+\delta_0]$$

some δ_0. Here $\varphi(u_0) = s_0$, $\varphi(u_0+\varepsilon_0) = s_0+\delta_0$

THEN $G^{v_0} = G^{v_0+\delta_0}$ AND $G^{v_0} = G^{v_0+\delta}$ $\forall \delta < \delta_0$

THEN $\varphi(u_0)$ IS NOT A BREAK IN THE UPPER FILTRATION

THEN $s_0 \notin B^{u}_{L/K} \Rightarrow \psi(s_0) = u_0 \notin B^{\ell}_{L/K}$ AND

$$u_0 \notin B^{\ell}_{L/K} \Rightarrow \varphi(u_0) = s_0 \notin B^{u}_{L/K}$$

Theorem (Hasse-Arf) L/K FINITE ABELIAN EXTENSION WITH SEPARABLE RESIDUE EXTENSION ℓ/k THEN

$$B^{u}_{L/K} \subseteq \mathbb{Z} \cap \mathbb{R}_{>-1}$$

Proof I STEP REDUCE TO THE TOTALLY RAMIFIED CASE

We can suppose L/K totally ramified because otherwise we can replace the Galois group with the inertia subgroup (Because all the jumps can happen only for $m \geq 0$)

$$\begin{array}{l} L \\ | \\ L^0 \\ | \\ K \end{array} \qquad G_0 \to |$$

IF L^0/K IS THE MAXIMAL UNRAMIFIED EXTENSION OF K INSIDE L, THEN $G^t(L^0/K) = G^t(L/K) \quad t \geq -1$ SINCE

$$\psi_{L/K}(s) = \psi_{L/L^0}(\psi_{L^0/K}(s)) \underset{\uparrow}{=} \psi_{L/L^0}(s)$$

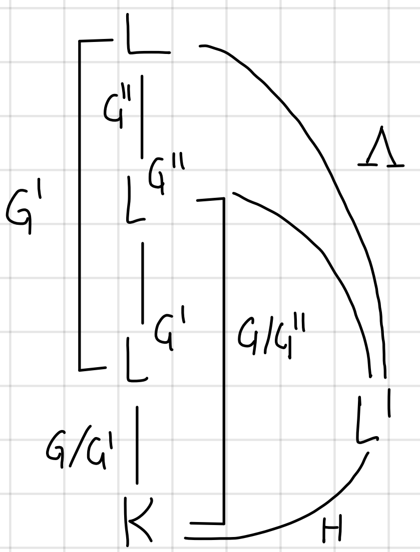
this comes from $\psi_{L^0/K}(s) = \eta^{-1}_{L^0/K}(s) = \int_0^s [G^0(L^0/K) : G^w(L^0:K)]\, dw$

But $G^0(L^0/K) = G_0(L^0/K) = I(L^0/K) = \{1\}$ as the extension is unramified. Then $\psi_{L^0/K}(s) = s$

II STEP SUPPOSE L/K TOTALLY RAMIFIED AND REDUCE TO CYCLIC CASE

$G' = G^v$ AND $G'' = G^{v+\varepsilon}$ FOR ε SMALL ENOUGH SO THAT $G' \neq G''$

↳ the "next ramification grop"



G/G'' SPLITS IN A PRODUCT OF CYCLIC SUBGROUPS

$G/G'' = H_1 \times H_2 \times \dots \times H_j \quad H_i$ cyclic

$\exists$ H BETWEEN THE H_i'S FOR WHICH THE IMAGE OF G' IS NOT $\{1\}$

$$G \longrightarrow G/G'' = H \times \Lambda$$
$$G' \longmapsto$$

$$H^v = (G/\Lambda)^v = G^v\Lambda/\Lambda = G'\Lambda/\Lambda = \frac{G'\,Gal(L/L')}{Gal(L/L')} = \frac{G'}{G' \cap Gal(L/L')} = H' \neq 1$$

$$H^{v+\varepsilon} = (G/\Lambda)^{v+\varepsilon} = \frac{G''\,Gal(L/L')}{Gal(L/L')} = \frac{G''}{G'' \cap Gal(L/L')} = G''/G'' = \{1\}$$

Claim $\#G = \#Gal(L/K) = \prod_{n \geq 0} [G_{\psi(n)} : G_{\psi(n)+1}]$

L/K CYCLIC TOTALLY RAMIFIED EXTENSION

THIS WOULD IMPLY THAT $G_{\psi(n)+1} = G_{\psi(n+1)} \quad \forall n \geq 0$

$$\psi(n+1) = \frac{1}{\#G_{n+1}} (\#G_0 \cdot (n+1) - \#G_1 - \#G_2 - \dots - n\#G_{n+1}]$$

$$\psi(n) = \frac{1}{\#G_{n+1}} (\#G_0 \cdot n - \#G_1 - \#G_2 - \dots - (n-1)\, G_{n+1}]$$

$$\psi(n+1) = \psi(n) + \frac{\#G_0}{\#G_{n+1}} \geq \psi(n) + 1 \implies G_{\psi(n)+1} \supseteq G_{\psi(n+1)}$$

THEN $\#G = \prod_{n\geq 0} [G_{\psi(n)} : G_{\psi(n+1)}] = [G_0 : G_{\psi(1)}][G_{\psi(1)} : G_{\psi(2)}] \cdots$

$\Rightarrow G_{\psi(n)+1} = G_{\psi(n+1)} \Longleftrightarrow$ Hasse-Arf

<u>Hasse-Arf</u> IF THERE IS AN INTEGER SUCH THAT $G_m \neq G_{m+1}$ THEN $\varphi(m)$ IS AN INTEGER

<u>Proof</u> SUPPOSE $\varphi(m) \notin \mathbb{Z}$, $\exists\, n \in \mathbb{Z}$ SUCH THAT $n \leq \varphi(m) \leq n+1$

$\psi(n) \leq m \leq \psi(n+1)$

$m \in \mathbb{Z} \Rightarrow \varphi(n)+1 \leq m \quad m+1 \leq \psi(n+1)$

$G_{\psi(n)+1} \supseteq G_m \supseteq G_{m+1} \supseteq G_{\psi(n+1)} \Rightarrow G_m = G_{m+1} \Rightarrow \varphi(m) \in \mathbb{Z}$ ↯

<u>Claim</u> $\#G = \prod_{n\geq 0} [G_{\psi(n)} : G_{\psi(n)+1}] = \prod_{n\geq 0} \dfrac{[G_0 : G_{\psi(n)+1}]}{[G_0 : G_{\psi(n)}]}$

<u>Fact</u> $\#G = \prod_{n\geq 0} [G_{\psi(n)} : G_{\psi(n+1)}]$

$\#G = \prod_{n\geq 0} [G_n : G_{n+1}] = \prod \dfrac{[G_0 : G_{n+1}]}{[G_0 : G_n]} \qquad G_{m+1} = \{1\}$

$= \dfrac{\cancel{[G_0 : G_1]}\ \cancel{[G_0 : G_2]}\ \cancel{[G_0 : G_3]}}{[G_0 : G_0]\ \cancel{[G_0 : G_1]}\ \cancel{[G_0 : G_2]}} \cdots \dfrac{\cancel{[G_0 : G_m]}\ [G_0 : G_{m+1}]\ \cancel{[G_0 : G_{m+2}]}}{\cancel{[G_0 : G_{m-1}]}\ \cancel{[G_0 : G_m]}\ \cancel{[G_0 : G_{m+1}]}} \cdots$

$= [G_0 : G_{m+1}] = \#G_0$ totally ramified

HASSE ARF IS THEREFORE PROVING THAT THE LAST BREAK ν FOR WHICH $G_\nu \neq \{1\}$ AND $G_{\nu+1} = \{1\}$ LIES IN AN INTERVAL OF THE FORM $[\psi(n) ; \psi(n)+1]$

<u>eg</u> CYCLIC OF ORDER p $\qquad G_0 = G_1 = G_2 = \ldots = G_t \neq G_{t+1} = \{1\}$

$$\psi(x) = \begin{cases} x & x \leq t \\ t + p(x-t) & x \geq t \end{cases}$$

$$\prod_{n\geq 0} \frac{[G_0 : G_{\psi(n)+1}]}{[G_0 : G_{\psi(n)}]} = \frac{[G_{\psi(0)} : G_{\psi(t)+1}]}{[G_{\psi(0)} : G_{\psi(t)}]}$$

LAST TIME WE PROVED

HASSE-ARF THEOREM $\overset{(I)}{\iff}$ $\overset{(II)}{G_{\psi(n+1)} = G_{\psi(n)+1}} \quad \forall n$

$\overset{(III)}{\iff}$ IF μ IS THE LARGEST INTEGER FOR WHICH $G_\mu \neq 1$ $\Rightarrow \mu = \psi(n)$ FOR SOME $n \in \mathbb{N}$

$\overset{(IV)}{\iff}$ IF μ IS THE LARGEST INTEGER FOR WHICH $G_\mu \neq 1$ $\Rightarrow \varphi(\mu) = \eta(\mu) \in \mathbb{Z}$

$Gal(L/K) = G = \langle g \rangle$ CYCLIC CASE $\qquad V = \ker(N : L^\times \longrightarrow K^\times)$

Theorem (Hilbert's theorem 90) L/K GALOIS. $v \in L^\times$ HAS NORM 1 $\Rightarrow \exists x \in L^\times$ SUCH THAT $v = \frac{g(x)}{x}$

i.e.,

$$\overline{V} = \frac{[\ker(N : L^\times \longrightarrow K^\times)]}{\{g(x)/x \mid x \in L^\times\}} \text{ IS TRIVIAL}$$

Proof Claim: $\overline{V} \simeq H^1(G, L^\times)$ I COHOMOLOGY GROUP

Proof $H^1(G, L^\times) = \frac{\{\text{crossed maps}\}}{\{\text{Principal crossed maps}\}}$

$\varphi : G \longmapsto L^\times \quad \varphi(g_1 g_2) = g_1(\varphi(g_2))\varphi(g_1)$

IS PRINCIPAL IF IT IS OF THE FORM $g \longmapsto \frac{g(x)}{x}, x \in L^\times$

$G = \langle g \rangle$ φ IS CROSSED MAP $\Rightarrow \varphi(g)$ has norm 1

$$N_{L/K}(\varphi(g)) = \prod_{\sigma \in G} \sigma(\varphi(g)) = \prod_{\sigma \in G} \sigma(\varphi(g)) \frac{\varphi(\sigma)}{\varphi(\sigma)} =$$

$$= \prod_{\sigma \in G} \frac{\varphi(\sigma(g))}{\varphi(\sigma)} = \prod_{i=0}^{\#G-1} \frac{\varphi(g^i \cdot g)}{\varphi(g^i)} = \prod_{i=0}^{\#G-1} \frac{\varphi(g^{i+1})}{\varphi(g^i)} = 1$$

$\Rightarrow \mathcal{U} : \{\text{crossed maps}\} \longrightarrow V$ IS A HOMOMORPHISM

$\mathcal{U}$ IS SURJECTIVE IF $x \in L^\times$ HAS NORM 1 THEN $\psi(1) = 1$
$\psi(g^r) = \prod_{i=0}^{r-1} g^i(x) \quad 0 \leq r \leq \#G - 1$ defines a crossed map such that $\psi(g) = x$

$$\Psi(\sigma g^r) = \Psi(g^m g^r) = \prod_{i=0}^{m+r-1} g^i(x) = \prod_{i=0}^{r-1} g^m(g^i(x)) \prod_{i=0}^{m-1} g^i(x)$$

$$= g^m \Psi(g^r) \Psi(g^m) \Rightarrow \Psi \text{ CROSSED MAP}$$

$$\mathcal{U}^{-1}\left(\left\{ \frac{g(x)}{x} \mid x \in L^\times \right\}\right) = \{\text{Principal crossed maps}\}$$

$$\Psi(g^r) = \prod_{i=0}^{r-1} g^i\left(\frac{g(x)}{x}\right) = \prod_{i=0}^{r-1} \frac{g^{i+1}(x)}{g^i(x)} = \frac{g^r(x)}{x}$$

$$\Rightarrow V \simeq H^1(G, L^\times)$$

Now we can prove the theorem (All crossed maps are principal)

φ CROSSED MAP $y \in L^\times$ $\qquad x = \sum_{\sigma \in G} \varphi(\sigma)\sigma(y)$

IF $\exists y$ SUCH THAT $x \neq 0 \Rightarrow \varphi$ IS PRINCIPAL

$$\forall \tau \in G \quad \tau(x) = \sum_{\sigma \in G} \tau\varphi(\sigma)\tau\sigma(y) = \frac{1}{\varphi(\tau)} \sum_{\sigma \in G} \varphi(\tau\sigma)\tau\sigma(y) = \frac{x}{\varphi(\tau)}$$

WE CAN FIND SUCH A y BECAUSE THE FAMILY $\{\sigma : L^\times \to L^\times \mid \sigma \in G\}$ IS LINEARLY INDEPENDENT $/L$.

$$\Rightarrow \sum \varphi(\sigma)\sigma : L \longrightarrow L \text{ IS NOT THE ZERO MAP} \qquad \square$$

$$V = \ker(N : L^\times \to K^\times) = \left\{ \frac{g(x)}{x} \mid x \in L^\times \right\} \qquad W = \left\{ \frac{g(x)}{x} \mid x \in \mathcal{U}_L \right\}$$

($\mathcal{U}_L = \mathcal{O}_L^\times$)

$W \leq V$ AND $\forall i \geq 0 \quad V_i = V \cap \mathcal{U}_L^i, \; W_i = W \cap \mathcal{U}_L^i$

FILTRATION: WE WILL STUDY QUOTIENTS V_i / W_i

Proposition π_L UNIFORMIZER FOR L

a) $\theta : G \longrightarrow V/W, \; \sigma \longmapsto \left[\frac{\sigma(\pi)}{\pi}\right]$ IS AN ISOMORPHISM

b) IT RESPECT QUOTIENTS $[G_i \hookrightarrow V_i / W_i]$

Proof
- $\sigma \in G$, $\sigma(\pi)/\pi \in V$
- $N_{L/K}(\theta(\sigma)) = \prod_{\tau \in G} \tau(\theta(\sigma)) = \prod \tau\sigma(\pi)/\tau(\pi) = 1$
- $v_L(\theta(\sigma)) = v_L(\sigma(\pi)) - v_L(\pi) = 0 \Rightarrow \theta(\sigma) \in \mathcal{U}_L$

× θ IS A HOMOMORPHISM

$$\underbrace{\frac{\tau\sigma(\pi)}{\pi}}_{\theta(\tau\sigma)}\ \underbrace{\frac{\pi^2}{\sigma(\pi)\tau(\pi)}}_{1/\theta(\sigma)\theta(\tau)} = \frac{\tau\sigma(\pi)}{\sigma(\pi)}\cdot\frac{1}{\tau(\pi)/\pi} = \frac{\sigma(\tau(\pi)/\pi)}{\tau(\pi)/\pi} \in W$$

$\Rightarrow \theta(\tau\sigma) = \theta(\sigma)\theta(\tau) \bmod W$

× θ INJECTIVE Suppose $\frac{g^r(\pi)}{\pi} \in W \Rightarrow \exists u \in \mathcal{U}_L$

$$\theta(g^r) = \theta(g)^r = \left(\frac{g(\pi)}{\pi}\right)^r = \frac{g(u)}{u}$$

$$\Rightarrow g\left(\frac{\pi^r}{u}\right) = \frac{\pi^r}{u} \Rightarrow \frac{\pi^r}{u} \in K \Rightarrow [L:K] \mid r \Rightarrow g^r = 1$$

× θ SURJECTIVE Every element of V has form $\frac{g(u\pi^i)}{u\pi^i}$ some $u \in \mathcal{U}_L$, $i \in \mathbb{Z}$.

$$g(u\pi^i)/u\pi^i \underset{\text{IN } V/W}{=} g(\pi^i)/\pi^i = \theta(g^i)$$

$\Rightarrow V/W$ IS CYCLIC

b) $\sigma \in G_i \Rightarrow \frac{\sigma(\pi)}{\pi} \in \mathcal{U}_L^i$ BY DEFINITION OF G_i $\square$

WE SUPPOSE THAT THE RESIDUE FIELD OF K, k IS NOT THE PRIME FIELD, $k \neq \mathbb{F}_p$

Lemma $G_m = 0 \Leftrightarrow V_m / W_m = 0$

($\Leftarrow$) TRIVIAL $G_m \hookrightarrow V_m / W_m$

($\Rightarrow$) WE WILL PROCEED BY DESCENDING INDUCTION ON m.
$G_m = 0$ FOR m LARGE ENOUGH

Claim SAME IS TRUE FOR V_m / W_m, i.e., $V_m = W_m$ $m \gg 0$

INDEED, AS L/K IS SEPARABLE, THEN $\exists t$, $Tr_{L/K}(t) = 1$
$M = \max\{0, \_\_, v_L(t)\} \Rightarrow V_m = W_m$ $\forall m > M$.
$x \in V_m$

$$y = t + \sum_{i=1}^{\#G-1} x g(x) g^2(x) \cdot \ldots \cdot g^{i-1}(x) g^i(t)$$

$$y - 1 = t + \sum x g(x) g^2(x) \cdot \ldots \cdot g^{i-1}(x) g^i(t) - \underbrace{1}_{\sum_{i=0}^{\#G-1} g^i(t)}$$

$$= \sum_{i=1}^{\#G-1} \left(x g(x) \cdot \ldots \cdot g^{i-1}(x) - 1\right) g^i(t)$$

SINCE $x \in \bar{V}_m$ $m > \max\{0, \_, \nu_L(t)\}$
$\nu_L(y-1) > 0 \Rightarrow y \in \mathcal{U}_L^1$. THEN

$$\frac{y}{g(y)} = \frac{xy}{xg(y)} = \frac{xy}{x g(t) + x \sum_{i=1}^{\#G-1} g(x) \cdot \ldots \cdot g^i(x) \cdot g^{i+1}(t)}$$

THE DENOMINATOR IS

$$x g(t) + x \sum_{i=1}^{\#G-1} g(x) \cdot \ldots \cdot g^i(x) \cdot g^{i+1}(t) =$$
$$= x g(t) + x \sum_{i=2}^{\#G} g(x) \cdot \ldots \cdot g^{i-1}(x) g^i(t)$$
$$= \sum_{i=1}^{\#G-1} x g(x) \cdot \ldots \cdot g^{i-1}(x) g^i(t) + \overbrace{N(x)}^{=1} t = y$$

$$\frac{y}{g(y)} = \frac{xy}{y} = x \in \bar{W}_m \Rightarrow \bar{V}_m = \bar{W}_m \quad \forall m > M$$

Now let $G_m = \{1\}$ and assume $\bar{V}_{m+1} / \bar{W}_{m+1} = 0$
we want to show $\bar{V}_m = \bar{W}_m$

$$\begin{array}{ccc} & & | \\ G_m & \hookrightarrow & \bar{V}_m / \bar{W}_m \\ | & & | \\ G_{m+1} & \hookrightarrow & \bar{V}_{m+1} / \bar{W}_{m+1} \\ | & & | \end{array}$$

$$(G_m = \{1\}) + (\bar{V}_{m+1} / \bar{W}_{m+1} = \{1\}) \Rightarrow \bar{V}_m / \bar{W}_m = \{1\}$$

Lemma $n+1 = \lceil \varphi_{L|K}(m) \rceil$ IF $\bar{V}_{m+1} / \bar{W}_{m+1} = \{1\}$ AND
$G_{\psi(n+1)} = \{1\} \Rightarrow \bar{V}_m / \bar{W}_m = \{1\}$

Proof $\psi(n+1) \geq m$ WITH EQUALITY $\Leftrightarrow \varphi(m) \in \mathbb{Z}$

I) $\varphi(m) \in \mathbb{Z} \Rightarrow \psi(n+1) = m$ OR $\varphi(m) = n+1$

PROP 8/9
L/K GALOIS EXTENSION
TOTALLY RAMIFIED

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & V_{m+1} & \longrightarrow & V_m & \longrightarrow & G_m / G_{m+1} & & \\ & & \downarrow & & \downarrow & & \downarrow \theta_m & & \\ 0 & \longrightarrow & \mathcal{U}_L^{m+1} & \longrightarrow & \mathcal{U}_L^m & \longrightarrow & \mathcal{U}_L^m / \mathcal{U}_L^{m+1} & \longrightarrow & 0 \\ & & \downarrow N & & \downarrow N & & \downarrow N_m & & \\ 0 & \longrightarrow & \mathcal{U}_K^{n+1} & \longrightarrow & \mathcal{U}_K^n & \longrightarrow & \mathcal{U}_K^n / \mathcal{U}_K^{n+1} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

$\sigma \mapsto [\sigma(\pi)/\pi]$

IF $k = \bar{k}$ OR $G_{m+1} = \{1\}$

$V_{m+1}/W_{m+1} = \{1\}$ BY ASSUMPTION $\Rightarrow$

$$V_m \longrightarrow G_m/G_{m+1} \longrightarrow (V_m/W_m)\Big/(V_{m+1}/W_{m+1}) = V_m/W_m$$

IS JUST THE CANONICAL QUOTIENT MAP

$$G_m = G_{\psi(n+1)} = \{1\} \Rightarrow V_m/W_m = 0$$

- $\varphi(m) \notin \mathbb{Z} \Rightarrow n < \varphi_{L/K}(m) < n+1 \qquad \psi_{L/K}(n) < m < \psi_{L/K}(n+1)$

WE KNOW $V_m/V_{m+1} \subset U_L^m/U_L^{m+1}$ AND $V_{m+1} = W_{m+1}$
TO SHOW $V_m = W_m$ IT SUFFICES TO SHOW THAT THEY HAVE SOME IMAGE IN U_L^m/U_L^{m+1}

$x \in U_L^m \quad U_L^{\psi_{L/K}(n+1)} \subseteq U_L^m$ AND $N_L : U_L^{\psi_{L/K}(n+1)} \longrightarrow\!\!\!\!\rightarrow U_K^{n+1}$

$\Rightarrow N(xy^{-1}) = 1 \Rightarrow xy^{-1} \in V_m$ AS $\psi_{L/K}(n+1) \geq m+1 \Rightarrow y \in U_L^{m+1}$
$\Rightarrow x \equiv xy^{-1} \bmod U_L^{m+1} \Rightarrow V_m \longrightarrow\!\!\!\!\rightarrow U_L^m/U_L^{m+1}$

FOR W_m WE KNOW THAT $V_m/W_m \longrightarrow\!\!\!\!\rightarrow (U_L^m/U_L^{m+1})/W_m$
THEN THE LATTER IS CYCLIC
BUT $U_L^m/U_L^{m+1} \simeq (k,+)$ THIS IS NOT CYCLIC $\Rightarrow$ IMAGE OF W_m NOT TRIVIAL

$$x \in W_m \setminus U_L^{m+1} \Rightarrow \exists y \in U_L \quad x = \frac{g(y)}{y}$$

AND WE MAY ASSUME $y \in U_L^1$ BY MODIFYING IT WITH AN ELEMENT OF U_K $\quad y = 1+z, \; \nu_L(z) > 0$

$$\forall a \in U_K \quad y_a = 1+az \quad x_a = g(y_a)/y_a$$

$$\gamma : U_L^m/U_L^{m+1} \longrightarrow \underbrace{\mathfrak{m}^m/\mathfrak{m}^{m+1}}^{\text{1-DIMENSIONAL VECTOR-SPACE OVER } k}$$

$\mathfrak{m}$ maximal ideal of valuation ring $\mathcal{O}_L$

$$1+u\pi^m \longmapsto u\pi^m \bmod \mathfrak{m}^{m+1}$$

<u>Claim</u> $\gamma(x_a) = a\gamma(x)$ AND $x_a \in W_m \Rightarrow W_m \longrightarrow\!\!\!\!\rightarrow U_L^m/U_L^{m+1}$

<u>Proof</u> $$x_a - 1 = \frac{g(y_a) - y_a}{y_a} = \frac{1+ag(z) - (1+az)}{y_a} = \frac{a(g(z)-z)}{y_a} =$$
$$= \frac{ag(y)-y}{y_a} = a\frac{y}{y_a}(x-1)$$

$$\nu_L(x_a - 1) = \nu_L(a) + m \geq m \Rightarrow x_a \in W_m$$

$$\gamma(x_a) = a\gamma(x) \text{ BECAUSE } y/y_a \in \mathcal{U}_L^!$$

Theorem μ LARGEST INTEGER FOR WHICH $G_\mu \neq \{1\} \Rightarrow \varphi_{L/K}(\mu) \in \mathbb{Z}$

Proof SUPPOSE $\notin \mathbb{Z} \Rightarrow \exists\, \nu \in \mathbb{Z} : \nu < \varphi(\mu) < \nu + 1$
$\mu < \psi(\nu+1) \Rightarrow G_{\psi(\nu+1)} = 0 \Rightarrow V_\mu / W_\mu = 0 \Rightarrow \underset{\overset{\shortparallel}{0}}{G_\mu} \hookrightarrow \frac{V_\mu}{W_\mu}$ ↯

eg CYCLOTOMIC EXTENSIONS OF $\mathbb{Q}_p$ $\quad n = p^m$
ζ = PRIMITIVE p^m-TH ROOT OF UNITY

$$G = Gal(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p) \simeq (\mathbb{Z}/n\mathbb{Z})^\times \quad [\mathbb{Q}_p(\zeta) : \mathbb{Q}_p]\, \phi(n) = p^{m-1}(p-1)$$

NOW IF $0 \leq \nu \leq m$ WE DEFINE $G(\nu)$ TO BE THE SUBGROUP OF G ISOMORPHIC TO $H \leq (\mathbb{Z}/n\mathbb{Z})^\times$ SUCH THAT ALL ITS ELEMENTS REDUCE TO 1 MODULO p^ν

$$Gal(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p(\zeta_{p^\nu})) \simeq G(\nu) \quad \text{AND}$$

$$G_\mu = \begin{cases} G & \mu = 0 \\ G(1) & 1 \leq \mu \leq p-1 \\ G(2) & p \leq \mu \leq p^2 - 1 \\ \vdots & \\ \{1\} & \mu \geq p^{m-1} \end{cases}$$

LARGEST INTEGER FOR WHICH $G_\mu \neq \{1\}$

$$\varphi(p^{m-1} - 1) = \sum_{i=1}^{p^m-1} \frac{\#G_i}{\#G_0} = \sum_{i=1}^{p-1} \frac{\#G(1)}{\#G} + \sum_{i=p}^{p^2-1} \frac{\#G(2)}{\#G} + \cdots$$

$$= \sum_{j=1}^{m-1} \sum_{i=1}^{p^{j-1}(p-1)} \frac{p^{m-j}}{p^{m-1}(p-1)} = \sum_{j=1}^{m-1} p^{j-1}(p-1)\frac{p^{1-j}}{p-1} = \sum_{j=1}^{m-1} 1$$

$$= m - 1 \in \mathbb{Z}$$

eg k ALGEBRAICALLY CLOSED FIELD, $k[[x]]$ RING OF FORMAL POWER SERIES

$$K = frac(k[[x]]) = k((x))$$

$P(t) = t^{p^n} - t - x \in K[t]$ IS NOT IRREDUCIBLE

$$L = K[t]/(P(t)) \underset{u=\frac{1}{t}}{\simeq} K[u]/(u^{p^n} + x u^{p^n-1} - x)$$

SEPARABLE EISENSTEIN POLYNOMIAL
Proposition 17 in Serre Ch 1

L/K GALOIS

$$Gal(L/K) \simeq \mathbb{F}_{p^n}$$

$a \in \mathbb{F}_{p^n} : t \longmapsto a + t \qquad u \longmapsto \dfrac{au}{1+au}$

The integral closure of $k[[x]]$ in L is

$$k[[x]][u]/(u^{p^n} + u^{p^n-1}x - x)$$

DVR WITH UNIFORMIZER u. THE RAMIFICATION INDEX OF THIS EXTENSION IS p^n

$$u^{p^n} = x(\underbrace{1 - u^{p^n-1}}_{\text{UNIT}})$$

$$v_L\left(\frac{u}{1+au} - u\right) = v_L\left(u\left(\frac{1-(1+au)}{1+au}\right)\right) = 2$$

$\Rightarrow$ IT FOLLOWS $G = \mathbb{F}_p = G_0 = G_1 \supsetneq G_2 = \{1\}$

$L = K[t]/(t^p - t - x^{-m})]$ $\quad (p, m) = 1$

$[G = G_0 = \cdots = G_m \supsetneq G_{m+1} = \{1\}$

$$\varphi(m) = \sum_{i=1}^{m} \frac{\#G_i}{\#G_0} = \sum_{i=1}^{m} 1 = m \in \mathbb{Z}$$