Lecture 18

1 L/K finite separable extension of local fields.
Say L/K is tamely ramified if $\mathrm{char}\, k = p \nmid e_{L/K}$ ($\Leftrightarrow G_1 = \{1\}$ if L/K is Galois)!
Otherwise it is wildly ramified.

$$\begin{tikzcd}
L \arrow[d, dash] \arrow[dr, dash, "\text{- totally wildly ramified}"] & \\
 & K' \arrow[d, dash, "\text{- totally tamely ramified}"] \\
 & K_0 \\
K \arrow[ur, dash, "\text{unramified}"'] &
\end{tikzcd}$$

Theorem 14.4: $[K:\mathbb{Q}_p]<\infty$, L/K finite, $\mathcal{D}_{L/K} = (\pi_L^{\delta(L/K)})$,
Then $\delta(L/K) \geq e_{L/K} - 1$, with equality iff L/K is tamely ramified.

In particular, L/K unramified $\Leftrightarrow \mathcal{D}_{L/K} = \mathcal{O}_L$.

Proof: Ex sheet 3 $\Rightarrow \mathcal{D}_{L/K} = \mathcal{D}_{L/K_0} \cdot \mathcal{D}_{K_0/K}$

Suffices to check 2 cases.

(i) L/K unramified. Let $\alpha \in \mathcal{O}_L$ s.t. $k_L = k(\bar{\alpha})$.

Proof of Prop. 6.11 $\Rightarrow \mathcal{O}_L = \mathcal{O}_K[\alpha]$

$g(X) \in \mathcal{O}_K[X]$ min poly of α.

2 $\bar{g}(X) \in k[X]$ separable $\Rightarrow g'(\alpha) \not\equiv 0 \bmod \pi_L$

(thm 12.9) $\Rightarrow \mathcal{D}_{L/K} = (g'(\alpha)) = \mathcal{O}$

(ii) L/K totally ramified.

$[L:K]=e$, $\mathcal{O}_L=\mathcal{O}_K[\pi_L]$, π_L root of

$$g(X)=X^e+\sum_{i=0}^{e-1}a_iX^i\in\mathcal{O}_K[X] \text{ Eisenstein}$$

Then $g'(\pi_L)=\underbrace{e\pi_L^{e-1}}_{v_L\geq e-1}+\underbrace{\sum_{i=0}^{e-1}ia_i\pi_L^{i-1}}_{v_L\geq e}$

thus $v_L(g'(\pi_L))\geq e-1$. Equality iff $p\nmid e$. $\square$

Corollary 14.5: L/K extension of number fields. $\mathcal{P}\subseteq\mathcal{O}_L$, $\mathcal{P}\cap\mathcal{O}_K=\mathfrak{p}$. Then $e(\mathcal{P}/\mathfrak{p})>1$ iff $\mathcal{P}\mid\mathcal{D}_{L/K}$.

Proof: Theorem 12.10 $\Rightarrow$ $\mathcal{D}_{L/K}=\prod_{\mathfrak{p}}\mathcal{D}_{L_\mathfrak{p}/K_\mathfrak{p}}$.

Then use $e(\mathcal{P}/\mathfrak{p})=e_{L_\mathfrak{p}/K_\mathfrak{p}}$ + Theorem 14.4. $\square$

Theorem 14.6: $[K:\mathbb{Q}_p]<\infty$. There are finitely many extensions $K\subseteq L\subseteq\overline{K}$ of given degree.

Proof: By Theorems 13.3 + 13.4, suffices to consider totally ramified ext (since $\exists!$ unram. ext. of given degree).

$\{\text{Eisenstein polynomials, deg } n\} =: V$

$$\updownarrow 1:1$$

$\{(a_0,\dots,a_{n-1})\in\mathcal{O}_K^{n-1}: v_K(a_i)\geq 1, \text{ all } i,\ v_K(a_0)=1\}$.

Hence V compact.

$f\in V$, $U_f=\{f'\in V \mid f' \text{ defines same set of extensions as } f\}$

Prop 8.4 $\Rightarrow$ U_f open,

$V = \bigcup_{J \in V} U_J$ has finite open cover by compactness

$\Rightarrow$ only finitely many L.

Prop. 8.4 $\Rightarrow$ Defining same set of extensions is open

Compactness $\Rightarrow$ only finitely many L. $\square$

Eg. $K = \mathbb{Q}_p$. ζ_{p^n} primitive p^nth root of unity.

$L = \mathbb{Q}_p(\zeta_{p^n})$. The p^nth cyclotomic polynomial

$$\Phi_{p^n}(X) = X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-1)} + \ldots + 1 \in \mathbb{Z}_p[X]$$

is the min. polynomial of ζ_{p^n}.

Ex Sheet 3

- $\Phi_{p^n}(X)$ is irreducible.
- $L/\mathbb{Q}_p$ Galois, totally ramified, degree $p^{n-1}(p-1)$.
- $\pi := \zeta_{p^n} - 1$ a uniformizer of $\mathcal{O}_L$,

$$\rightsquigarrow \quad \mathcal{O}_L = \mathbb{Z}_p[\zeta_{p^n} - 1] = \mathbb{Z}_p[\zeta_{p^n}]$$

- $\mathrm{Gal}(L/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ (abelian)

$$\sigma_m \longleftrightarrow m \quad \text{where } \sigma_m(\zeta_{p^n}) = \zeta_{p^n}^m$$

Let k be max. s.t. $p^k \mid m-1$. $\zeta_{p^n}^{m-1}$ is a primitive p^{n-k}th root of unity, and hence $(\zeta_{p^n}^{m-1} - 1)$ is a uniformizer π' in $L' := \mathbb{Q}_p(\zeta_{p^n}^{m-1})$.

Thus $v_L(\sigma_m(\pi) - \pi) = v_L(\zeta_{p^n}^m - \zeta_{p^n}) = v_L(\zeta_{p^n}^{m-1} - 1) = e_{L'/L}$.

$$= \underline{e_{L/\mathbb{Q}_p}} = \frac{[L:\mathbb{Q}_p]}{[L':\mathbb{Q}_p]} = \frac{p^{n-1}(p-1)}{p^{n-k-1}(p-1)} = p^k.$$

$e_{L'/\mathbb{Q}_p}$ $[L':\mathbb{Q}_p]$ $p^{n-1}(p-1)$

Theorem 14.2 (i) $\Rightarrow$ $\sigma \in G_i$ iff $p^k \geq i+1$.

Thus

$$G_i \cong \begin{cases} (\mathbb{Z}/p^n\mathbb{Z})^\times & i \leq 0 \\ (1+p^k\mathbb{Z})/p^n\mathbb{Z} & p^{k-1}-1 < i \leq p^k - 1,\ 1 \leq k \leq n. \\ \{1\} & p^{n-1}-1 < i \end{cases}$$

VI Local class field theory

§1 Infinite Galois theory

L/K an algebraic extension of fields.

Definition 16.1: $\cdot$ L/K is separable if $\forall \alpha \in L$, min. polynomial $f_\alpha(x) \in K[X]$ for α is separable.

- L/K normal if $f_\alpha(x)$ splits in L for all $\alpha \in K$
- L/K is Galois if it is separable and normal.

Write

$$\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L). \text{ in this case}$$

If L/K finite Galois, $\rightsquigarrow$ Galois correspondence

$$\{\text{subextensions } K \subseteq K' \subseteq L\} \xleftrightarrow{1:1} \{\text{subgroups of } \mathrm{Gal}(L/K)\}$$

$$K' \longmapsto \mathrm{Gal}(L/K').$$

$(I, \leq)$ a partially ordered set. Say I is a directed set if for all $i, j \in I$, $\exists k \in I$ s.t. $i \leq k$, $j \leq k$.

Eg. $\cdot$ Any total order (Eg. $(\mathbb{N}, \leq)$)

• $(\mathbb{N}_{\geq 1}, |)$ ordered by divisibility.

Definition 16.2: Let $(I, \leq)$ directed set and $(G_i)_{i \in I}$ a collection of groups together maps $\varphi_{ij} : G_j \to G_i$, $i \leq j$, such that

$$\varphi_{ik} = \varphi_{ij} \circ \varphi_{jk} \quad \text{for } i \leq j \leq k,$$

$$\varphi_{ii} = id.$$

6

Say $((G_i)_{i \in I}, \varphi_{ij})$ is an inverse system.

The inverse limit of $((G_i)_{i \in I}, \varphi_{ij})$ is

$$\varprojlim_{i \in I} G_i = \{ (g_i)_{i \in I} \in \prod_{i \in I} G_i \mid \varphi_{ij}(g_j) = g_i \}$$

Remark: • $(\mathbb{N}, \leq)$; recovers previous def.

• $\exists$ projection maps $\psi_j : \varprojlim_{i \in I} G_i \to G_j$

• $\varprojlim_{i \in I} G_i$ satisfies a universal property

Assume G_i finite, the profinite topology on $\varprojlim_{i \in I} G_i$ is the weakest topology s.t. ψ_j are continuous $\forall j \in I$.

Proposition 16.3: Let L/K Galois.

(i) The set $I = \{ F/K \text{ finite} \mid F \subseteq L, F/K \text{ Galois} \}$ is a directed under set under $\subseteq$.

(ii) For $F, F' \in I$, $F \subseteq F'$, there is a restriction map $res_{F,F'} : Gal(F'/K) \to Gal(F/K)$ and the natural map

$$\mathrm{Gal}(L/K) \to \varprojlim_{F\in I} \mathrm{Gal}(F/K)$$

7 is an isomorphism.

Proof: Ex Sheet 4.