Lecture 16

L/K finite separable ext. of local fields.

Theorem 13.3: There exists a field K_0, $K \subseteq K_0 \subset L$ and s.t.

(i) K_0/K is unramified

(ii) L/K_0 is totally ramified.

$$\begin{tikzcd} L \arrow[d, dash, "e_{L/K}"] \\ K_0 \arrow[d, dash, "f_{L/K}"] \\ K \end{tikzcd}$$

Moreover $[K_0:K] = f_{L/K}$, $[L:K_0] = e_{L/K}$, and K_0/K is Galois.

Proof: Let $k = \mathbb{F}_q$, so that $k_L = \mathbb{F}_{q^f}$, $f = f_{L/K}$. Set $m = q^f - 1$, $[\ ]: \mathbb{F}_{q^f} \to L$ Teichmuller map for L.

Let $\zeta_m = [\alpha]$ for α a generator of $\mathbb{F}_{q^f}^\times$. ζ_m a primitive m^{th} root of unity (lecture 5).

Set $K_0 = K(\zeta_m)^{\subseteq L}$ - splitting field of $f(X) = X^m - 1 \in K[X]$, hence K_0/K is Galois.

Residue field k_0 of K_0 contains $\alpha \in \mathbb{F}_{q^f}$.

$$\Rightarrow k_0 = \mathbb{F}_{q^f} \cong k_L.$$

Let $\mathrm{res}: \mathrm{Gal}(K_0/K) \to \mathrm{Gal}(k_0/k)$ denote the natural map.

For $\sigma \in \mathrm{Gal}(K_0/K)$ we have

$$\sigma(\zeta_m) = \zeta_m \quad \text{if} \quad \sigma(\zeta_m) \equiv \zeta_m \bmod m_0$$

(Use $\sigma(\zeta_m) = [\mathrm{res}(\sigma)(\zeta_m \bmod m_0)]$)

Thus res is injective. It follows

$$|\mathrm{Gal}(K_0/K)| \leq |\mathrm{Gal}(k_0/k)| = f = f_{L/K}$$

$\Rightarrow$ $[k_0 : K] = f_{L/K}$ and res is an iso.

2 Thus K_0/K is unramified.

Since $k_0 \cong k_L$, $f_{L/K_0} = 1$ and hence L/K_0 is totally ramified. $\square$

Theorem 13.4: $k = \mathbb{F}_q$. For each $n \geq 1$, $\exists$ a unique unramified extension L/K of degree n. Moreover L/K is Galois and the natural map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_{L/k})$ is an iso. In particular $\mathrm{Gal}(L/K) \cong \langle \mathrm{Frob}_{L/K} \rangle$ is cyclic.

$\mathrm{Frob}_{L/K}(x) \equiv x^q \bmod m_L$. $\forall x \in \mathcal{O}_L$.

Proof: For $n \geq 1$, take $L = K(\zeta_m)$ where $m = q^n - 1$ and $\zeta_m \in \bar{K}^\times$ a primitive m^{th} root of unity.

As in Thm 13.3, $\mathrm{Gal}(L/K) \xrightarrow{\cong} \mathrm{Gal}(k_L/k) \cong \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$

$\Rightarrow \mathrm{Gal}(L/K)$ cyclic, generated by lift of $x \mapsto x^q$.

Uniqueness: L/K deg n unramified, then $\zeta_m \in L$ and hence $L = K(\zeta_m)$ by degree reasons. $\square$

Corollary 13.5: L/K finite Galois. The map.

$$res: Gal(L/K) \to Gal(k_L/k)$$

3 is surjective

Proof: The map res factors as

$$Gal(L/K) \twoheadrightarrow Gal(K_0/K) \cong Gal(k_L/k). \square$$

Definition 13.6: L/K finite Galois.

The inertia subgroup is

$$I_{L/K} := \ker(Gal(L/K) \twoheadrightarrow Gal(k_L/k)) \leq Gal(L/K)$$

- Since $e_{L/K} f_{L/K} = [L:K]$, hence $|I_{L/K}| = e_{L/K}$.
- $I_{L/K} = Gal(L/K_0)$ - K_0 as in Theorem 13.3

Definition 13.7: $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathcal{O}_K[x]$ is Eisenstein if $\underset{\text{norm. valuation}}{v_K}(a_i) \geq 1 \; \forall i$, $v_K(a_0) = 1$

Fact: $f(x)$ Eisenstein $\Rightarrow$ $f(x)$ irreducible.

Theorem 13.8: (i) Let L/K finite totally ramified, $\pi_L \in \mathcal{O}_L$ unit. Then the minimal polynomial of π_L is an Eisenstein and

$$\mathcal{O}_L = \mathcal{O}_K[\pi_L] \quad (\Rightarrow L = K(\pi_L))$$

(ii) Conversely, if $f(x) \in \mathcal{O}_K[x]$ is Eisenstein and α a root of f. Then $L = K(\alpha)/K$ is

6 totally ramified and α a unit of L.

Proof: (i) $[L:K] = e$

$$f(x) = x^m + a_{m-1}x^{m-1} + \dots + a_0 \in \mathcal{O}_K[x]$$

minimal polynomial for π_L. Then $m \leq e$.

Since $v_L(K^\times) = e\mathbb{Z}$, we have

$$v_L(a_i \pi_L^i) \equiv i \mod e, \quad i < m,$$

hence these terms have distinct valuations

As $\pi_L^m = -\sum_{i=0}^{m-1} a_i \pi_L^i$

we have $m = v_L(\pi_L^m) = \min_{0 \leq i \leq m-1} (i + e v_K(a_i))$

$$\Rightarrow v_K(a_i) \geq 1 \quad \forall i,$$

and hence $v_K(a_0) = 1$ and $m = e$.

Thus $f(x)$ is Eisenstein, and $L = K(\pi_L)$.

For $y \in L$, we write $y = \sum_{i=0}^{e-1} \pi_L^i b_i$, $b_i \in K$.

Then $v_L(y) = \min_{0 \leq i \leq m-1} (i + e v_K(b_i))$

Thus $y \in \mathcal{O}_L \Leftrightarrow v_L(y) \geq 0$

$$\Leftrightarrow v_K(b_i) \geq 0 \quad \forall i$$

$$\Leftrightarrow y \in \mathcal{O}_K[\pi_L].$$

(ii) Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ Eisenstein

and let $e := e_{L/K}$.

Thus $v_L(a_i) \geq e$ and $v_L(a_0) = e$.

If $v_L(\alpha) \leq 0$ we have

$$v_L(\alpha^n) < v_L\left(\sum_{i=0}^{n-1} a_i \alpha^i\right) \quad \#$$

hence $v_L(\alpha) > 0$.

For $i \neq 0$, $v_L(a_i \alpha^i) > e = v_L(a_0)$;
it follows that

$$v_L\left(-\sum_{i=0}^{n-1} a_i \alpha^i\right) = e$$

and hence $v_L(\alpha^n) = e \Rightarrow n\, v_L(\alpha) = e$.

But $n = [L:K] \geq e \Rightarrow n = e$ and

L is totally ramified. Moreover $v_L(\alpha) = 1$ $\square$

§ Structure of units

Let $[K:\mathbb{Q}_p] < \infty$, $e := e_{K/\mathbb{Q}_p}$.

Proposition 13.8: If $r > \frac{e}{p-1}$, $\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$

converges on $\pi^r \mathcal{O}_K$ and induces an iso.

$$(\pi^r \mathcal{O}_K, +) \xrightarrow{\sim} (1 + \pi^r \mathcal{O}_K, \times)$$

Proof: $v_K(n!) = e\, v_p(n!) = e\left(\frac{n - s_p(n)}{p-1}\right)$ (Ex. Sht. 1)

$$\leq e\left(\frac{n-1}{p-1}\right)$$

For $x \in \pi^r \mathcal{O}_K$, we have for $n \geq 1$,

$$v_K\left(\frac{x^n}{n!}\right) \geq nr - e\frac{(n-1)}{p-1}$$

$$= r + (n-1)\underbrace{\left(r - \frac{e}{p-1}\right)}_{>0}$$

$\Rightarrow v_K\left(\frac{x^n}{n!}\right) \longrightarrow \infty$ as $n \to \infty$.

Thus $\exp(x)$ converges.

Since $v_K\left(\frac{x^n}{n!}\right) \geq r$ for $n \geq 1$

$\exp(x) \in 1 + \pi^r \mathcal{O}_K$.

Similarly consider $\log(x) : 1 + \pi^r \mathcal{O}_K \to \pi^r \mathcal{O}_K$

$$\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} x^n.$$

check convergence as before.

Recall properties of power series:

$$\exp(X+Y) = \exp(X)\exp(Y)$$

$$\exp(\log(1+X)) = 1+X \qquad \log(\exp(X)) = X$$

Thus $\exp : (\pi^r \mathcal{O}_K, +) \Rightarrow (1 + \pi^r \mathcal{O}_K, \times)$ is an isomorphism. $\square$