7.5. Torsion

Choose a uniformizer and let F_π be the corresponding L-T module. (Determined by π up to isom. of formal $\mathcal{O}_K$-modules.)

Def Let $F_\pi(n) = \{ \lambda \in \mathfrak{m}_{\bar{K}} \mid \underbrace{\pi^n \underset{F_\pi}{\bullet} \lambda}_{= \pi \underset{F}{\cdot} \cdots \pi \underset{F}{\cdot} \lambda = e^n(\lambda)} = 0 \}$

be the set of π^n-torsion elements for $n \geq 0$.

$0 = F_\pi(0) \subseteq F_\pi(1) \subseteq F_\pi(2) \subseteq \dots$

Let $F_\pi^1(n) = F_\pi(n) \setminus F_\pi(n-1)$ for $n \geq 1$.

Rmk $F_\pi(n) = \text{"}e^{-1}(F_\pi(n-1))\text{"}$, $F_\pi^1(n) = \text{"}e^{-1}(F_\pi^1(n-1))\text{"}$.

Ex $K = \mathbb{Q}_p$, $\pi = p$, $e(X) = (X+1)^p - 1$

$\rightsquigarrow X \underset{F_\pi}{+} Y = (X+1)(Y+1) - 1$

$a \underset{F_\pi}{\bullet} X = (X+1)^a - 1$

$F_\pi(n) = \{ \lambda \in \mathfrak{m}_{\bar{K}} \mid (\lambda+1)^{p^n} = 1 \}$

$= \mu_{p^n} - 1$

p^n-th roots of unity

$(F_\pi(n), \underset{F}{+}) \cong (\mu_{p^n}, \cdot)$ as groups

$F_\pi^1(n) = \mu_{p^n}^1 - 1$

primitive p^n-th roots of unity.

Lemma For any $n \geq 1$:

a) $|F_\pi^1(n)| = q^{n-1}(q-1)$

b) For any $\lambda_n \in F_\pi^1(n)$,

$K(\lambda_n)$ is a totally ramified separable degree $q^{n-1}(q-1)$ extension of K with uniformizer λ_n.

Cor $|F_\pi(n)| = |F_\pi^1(n)| + |F_\pi^1(n-1)| + \dots + |F_\pi^1(1)| + |F_\pi(0)| = (q^{n-1}+\dots+1)(q-1)+1 = q^n$.

Pf of Lemma

Induction over n:

$\underline{n=1}$: $F_\pi^1(1) = \{ 0 \neq \lambda_1 \in \mathfrak{m}_{\bar{K}} \mid e(\lambda_1) = 0 \}$

$$\Updownarrow$$

$$\lambda_1^{q-1} + \pi = 0 \Leftrightarrow f(\lambda_1) = 0$$

$f(X) := X^{q-1} + \pi \in K[X]$ is an Eisenstein polynomial of degree $q-1$. $\Rightarrow$ For any root λ_1 of $f(X)$, the ext. $K(\lambda_1)|K$ is tot. ram. of degree $q-1$ with uniformizer λ_1. In particular, $\lambda_1 \in \mathfrak{m}_{\bar{K}}$, so $F_\pi^1(1)$ is the set of all roots of $f(X)$.

$f'(X) = (q-1)X^{q-2}$ has no nonzero roots

$\Rightarrow f(X), f'(X)$ have no roots in common

$\Rightarrow f(X)$ is separable, has $q-1$ distinct roots

$\Rightarrow K(\lambda_1)|K$ is separable and $|F_\pi^1(1)| = q-1$.

$\underline{n-1 \to n}$: $F_\pi^1(n) = \{ \lambda_n \in \mathfrak{m}_{\bar{K}} \mid \underbrace{\lambda_{n-1} := e(\lambda_n) \in F_\pi^1(n-1)} \}$

$$\Updownarrow$$

$$\lambda_n^q + \pi\lambda_n = \lambda_{n-1} \Leftrightarrow f(\lambda_n) = 0.$$

Fix any $\lambda_{n-1} \in F_\pi^1(n-1)$.

$f(X) := X^q + \pi X - \lambda_{n-1} \in K(\lambda_{n-1})[X]$ is an Eisenstein polynomial of degree q.

$\Rightarrow$ For any root λ_n of $f(X)$, the ext. $K(\lambda_n)|K(\lambda_{n-1})$ is tot. ram. of degree q with uniformiser λ_n.
In particular, $\lambda_n \in \mathfrak{p}_{\bar{K}}$, so $F^1_\pi(n)$ is the set of <u>all</u> roots of $f(X)$.

Also, $K(\lambda_n)|K$ is by induction a tot. ram. ext. of degree $q \cdot q^{n-2}(q-1) = q^{n-1}(q-1)$.

$$f'(X) = q X^{q-1} + \pi$$

$$\Rightarrow q f(X) - X f'(X) = \underbrace{\pi(q-1)X - q\lambda_{n-1}}_{\text{\underline{linear} pol. in } K(\lambda_1)[X]}.$$

$\Rightarrow$ All common roots of $f(X)$ and $f'(X)$ lie in $K(\lambda_{n-1})$.
But $f(X)$ has no roots in $K(\lambda_{n-1})$ because
$[K(\lambda_n) : K(\lambda_{n-1})] = q > 1$ for any root λ_n of $f(X)$.

$\Rightarrow$ $f(X)$ is separable, hence has q distinct roots.

$\Rightarrow$ $K(\lambda_n)|K(\lambda_{n-1})$ separable, $|F^1_\pi(n)| = \underbrace{q}_{\substack{q \text{ roots } \lambda_n \\ \text{of } f(X)}} \cdot \underbrace{q^{n-2}(q-1)}_{\substack{\text{for each} \\ \lambda_{n-1} \in F^1_\pi(n-1)}}$

$\Rightarrow$ $K(\lambda_n)|K$ separable by induction

$\square$

Thm The $\mathcal{O}_K$-module $F_\pi(n)$ is isomorphic to $\mathcal{O}_K/\mathfrak{p}_K^n$.

Pf Let $\lambda_n \in F_\pi(n) \setminus F_\pi(n-1)$.

The kernel of the $\mathcal{O}_K$-mod. $\mathcal{O}_K \longrightarrow F_\pi(n)$
$$a \longmapsto a \cdot_{F_\pi} \lambda_n$$
is an ideal $\mathfrak{p}_K^m$ of $\mathcal{O}_K$. $(m \geq 0)$

The kernel contains π_K^r if and only if $\pi_K^r \cdot_{F_\pi} \lambda_n = 0$.
$$\Updownarrow$$
$$r \geq n$$

$\Rightarrow$ The kernel is $\mathfrak{p}_K^n$.

$\Rightarrow$ Injective hom. $\underbrace{\mathcal{O}_K/\mathfrak{p}_K^n}_{\text{size } q^n} \hookrightarrow \underbrace{F_\pi(n)}_{\text{size } q^n}$.

$\Rightarrow$ Surjective. $\square$

7.6. Maximal abelian extension

<u>Def</u> Let $K_{\pi,n} = K(F_\pi(n))$ be the smallest extension of K containing all elements of $F_\pi(n)$.

<u>Rmk</u> $K_{\pi,n}$ is independent of the choice of L-T series.
(It might depend on the choice of π, though!)

<u>Pf</u> Let $e(X), \tilde{e}(X)$ be L-T series for π.

By Thm B from section 7.3, there are power series $f, f^{-1} \in \mathcal{O}_K[[X]]$ inducing an isomorphism

$$F_e \underset{f^{-1}}{\overset{f}{\rightleftarrows}} F_{\tilde{e}} \text{ of formal } \mathcal{O}_K\text{-modules.}$$

Let $\lambda \in F_e(n)$. $\Rightarrow f(\lambda) \in F_{\tilde{e}}(n)$.

$$\Rightarrow \lambda = \underbrace{f^{-1}}_{\substack{\text{power series} \\ \text{with coeff. in } \mathcal{O}_K}}(f(\lambda)) \in K(F_{\tilde{e}}(n)).$$

$$\Rightarrow K(F_e(n)) \subseteq K(F_{\tilde{e}}(n)).$$

Similarly, ... ? ... . $\square$

<u>Ex</u> $K = \mathbb{Q}_p$, $\pi = p \rightsquigarrow K_{p,n} = \mathbb{Q}_p(\zeta_{p^n})$.

Thm a) $K_{\pi,n}|K$ is a totally ramified Galois ext. with

$$\mathrm{Gal}(K_{\pi,n}|K) \longrightarrow \mathrm{Aut}_{\mathcal{O}_K\text{-mod}}(\underbrace{F_\pi(n)}_{\mathcal{O}_K/\mathfrak{p}_K^n}) \cong (\mathcal{O}_K/\mathfrak{p}_K^n)^\times = \mathcal{O}_K^\times/U_K^{(n)}$$

$$\sigma \longmapsto \sigma|_{F_\pi(n)}$$

b) We have $K_{\pi,n} = K(\lambda_n)$ for any $\lambda_n \in F_\pi'(n)$.

Pf W.l.o.g. $e(X) = X^q + \pi X$.

$K_{\pi,n}$ is the splitting field of the degree q^n polynomial $e^n(X)$, which has q^n roots (all in $\mathfrak{p}_{\bar{K}}$) according to the Lemma in 6.5.

$\Rightarrow K_{\pi,n}|K$ is Galois.

The map Gal $\to$ Aut is well-defined:

$\sigma|_{F_\pi}$ permutes el. of F_π $\left\{ \forall x \in F_\pi(n):\ e^n(x) = 0 \Rightarrow \sigma(e^n(x)) = 0 \Rightarrow \sigma(x) \in F_\pi(n) \right.$, where $\sigma(e^n(x)) = e^n(\sigma(x))$

$\sigma|_{F_\pi}$ hom. of $\mathcal{O}_K$-mod. $\left\{ \begin{array}{l} \forall x,y \in F_\pi(n):\ \sigma(F_\pi(x,y)) = F_\pi(\sigma(x),\sigma(y)) \text{ because } F_\pi \in \mathcal{O}_K[[X,Y]] \\ \forall a \in \mathcal{O}_K,\ x \in F_\pi(n):\ \sigma([a]_{F_\pi}(x)) = [a]_{F_\pi}(\sigma(x)) \text{ because } [a]_{F_\pi} \in \mathcal{O}_K[[X]] \end{array} \right.$

The map is injective because the elements of $F_\pi(n)$ generate $K_{\pi,n}$.

$$\Rightarrow [K_{\pi,n} : K] = |\mathrm{Gal}| \leq |\mathrm{Aut}| = |(\mathcal{O}_K/\mathfrak{p}_K^n)^\times| = q^{n-1}(q-1)$$

$$[K_{\pi,n} : K] \geq [K(\lambda_n) : K] \underset{\uparrow}{=} q^{n-1}(q-1)$$

Lemma in 6.5.

$\Rightarrow K_{\pi,n} = K(\lambda_n)$, which is tot. ram. of deg. $q^{n-1}(q-1)$, and the map is indeed an isomorphism. $\square$

Cor $K_\pi := \bigcup_{n\geq 0} K_{\pi,n}$ is a totally ramified Galois ext. of K with Galois group $\mathcal{O}_K^\times$.

Pf $\mathrm{Gal}(K_\pi|K) = \varprojlim_{n\geq 0} \underbrace{\mathrm{Gal}(K_{\pi,n}|K)}_{(\mathcal{O}_K/\mathfrak{p}_K^n)^\times}$,

where the restriction map $\mathrm{Gal}(K_{\pi,n}|K) \twoheadrightarrow \mathrm{Gal}(K_{\pi,m}|K)$ $(n\geq m)$

is the quotient map $(\mathcal{O}_K/\mathfrak{p}_K^n)^\times \twoheadrightarrow (\mathcal{O}_K/\mathfrak{p}_K^m)^\times$.

$\square$

Thm $I^t(K_{\pi,n}|K) = \mathrm{Gal}(K_{\pi,n}|K_{\pi,t})$ $\quad \forall t\leq n$

$$\begin{array}{ccc} I^t(K_{\pi,n}|K) & = & \mathrm{Gal}(K_{\pi,n}|K_{\pi,t}) \\ \cap & & \| \\ \mathrm{Gal}(K_{\pi,n}|K) & & \\ \| & & \\ \mathcal{O}_K^\times/U_K^{(n)} & \supseteq & U_K^{(t)}/U_K^{(n)} \end{array}$$

$I^t(K_\pi|K) = \mathrm{Gal}(K_\pi|K_{\pi,t})$ $\quad \forall t\geq 0$

$$\begin{array}{ccc} I^t(K_\pi|K) & = & \mathrm{Gal}(K_\pi|K_{\pi,t}) \\ \cap & & \| \\ \mathcal{O}_K^\times & \supseteq & U_K^{(t)} \end{array}$$

Pf Let $\underset{\neq\ id}{\sigma} \in \mathrm{Gal}(K_{\pi,n}|K)$ corr. to $a \in \mathcal{O}_K^\times/U_K^{(n)}$

(so $\sigma(\lambda_n) = a \underset{F_\pi}{\cdot} \lambda_n$).

Goal: $\underset{\text{compute}}{i_{K_{\pi,n}|K}}(\sigma) = v_{K_{\pi,n}}(\sigma(\underset{\text{uniformizer}}{\lambda_n}) - \lambda_n)$

$= v_{K_{\pi,n}}(a \underset{F}{\cdot} \lambda_n - \lambda_n)$.

If $a \in U_K^{(1)}$, then

$i_{K_{\pi,n}|K}(\sigma) = 1$ because

$$a \cdot_F \lambda_n - \lambda_n = a\lambda_n - \lambda_n + (\text{deg.} \geq 2 \text{ terms in } \lambda_n)$$

$$\equiv \underbrace{(a-1)}_{\not\equiv 0 \bmod \lambda_n}\lambda_n \mod \lambda_n^2 .$$

If $a \in U_K^{(t)} \setminus U_K^{(t+1)}$, say $a = 1 + b\cdot\pi_K^t$, $b \in \mathcal{O}_K^\times$,

then $i_{K_{\pi,n}|K}(\sigma) = q^t$ because

$$a \cdot_F \lambda_n - \lambda_n = \lambda_n +_F \underbrace{(a-1)}_{b\cdot\pi_K^t} \cdot_F \lambda_n - \lambda_n$$

$$= \lambda_n +_F \underbrace{b \cdot_F \underbrace{e^t(\lambda_n)}_{\lambda_{n-t} \in F_\pi(n-t) \setminus F_\pi(n-t-1)}}_{\lambda'_{n-t} \in F_\pi(n-t) \setminus F_\pi(n-t-1)} - \lambda_n$$

Cor in 7.1

$$= \cancel{\lambda_n} + \lambda'_{n-t} - \cancel{\lambda_n}$$

$$+ \lambda_n \cdot \lambda'_{n-t} \cdot (\text{power series in } \lambda_n, \lambda'_{n-t} \text{ with coefficients in } \mathcal{O}_K)$$

so $v_{K_{\pi,n}}(a \cdot_F \lambda_n - \lambda_n) = v_{K_{\pi,n}|K}(\lambda'_{n-t})$

$$= q^t v_{K_{\pi,n-t}}(\lambda'_{n-t}) = q^t .$$

Rest is exactly like for cyclotomic ext.

Cor The maximal abelian extension of K is

$$K^{ab} = K^{unram} \cdot K_\pi .$$

Pf See the Thm in 6.5. $\square$

Rmk $Gal(K^{unram} \cdot K_\pi) = Gal(K^{unram}/K) \times Gal(K_\pi/K)$

$$= \hat{\mathbb{Z}} \times \mathcal{O}_K^\times .$$

Thm The map

$$K^\times = \mathbb{Z} \times \mathcal{O}_K^\times \longrightarrow \hat{\mathbb{Z}} \times \mathcal{O}_K^\times = Gal(K^{ab}/K)$$
$$a \cdot \pi^n \mapsto (n, a)$$

is independent of the choice of uniformiser.

Rmk It's the Artin reciprocity map.

Idea of pf If $e(X), \tilde{e}(X)$ are L-T series for $\pi, \tilde{\pi}$, then $F_e, F_{\tilde{e}}$ might not be isomorphic as formal $\mathcal{O}_K$-modules. But they become isomorphic over the completion of K^{unram}.

See Neukirch V, Thm 2.2, Cor. 2.3, Thm 5.5.

"$\square$"