Rmk Hasse-Arf $\Rightarrow$ Global Kronecker-Weber

Pf Let $K|\mathbb{Q}$ be a finite abelian ext.

Write $I^t(p) = I^t(\mathfrak{q}|p)$ for any prime $\mathfrak{q}|p$ of K.

(Independent of $\mathfrak{q}$ because $I^t(\sigma\mathfrak{q}|p) = \sigma I^t(\mathfrak{q}|p)\sigma^{-1}$ and $K|\mathbb{Q}$ is abelian.)

For any prime p, let $a_p \geq 0$ be minimal s.t. $I^{a_p}(p) = 1$.

In particular, $a_p = 0 \Leftrightarrow p$ unramified in K.

Goal: $K \subseteq \mathbb{Q}(\zeta_n)$, where $n = \prod_p p^{a_p}$.

W.l.o.g. $K \supseteq \mathbb{Q}(\zeta_n)$. (Replacing K by $K\cdot\mathbb{Q}(\zeta_n)$ and noting $I^{a_p}_{\mathbb{Q}(\zeta_n)}(p) = 1$.)

$\Rightarrow [K:\mathbb{Q}] \geq [\mathbb{Q}(\zeta_n):\mathbb{Q}] = |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$.

Look at the ext. $K_\mathfrak{q}|\mathbb{Q}_p$ of local fields.

Since $I^{a_p}(K_\mathfrak{q}|\mathbb{Q}_p) = 1$, we have

$$K_\mathfrak{q} \subseteq (\mathbb{Q}_p^{ab})^{I^{a_p}} = \mathbb{Q}_p^{unram}(\zeta_{p^{a_p}}).$$

$$\Rightarrow I(p) = I(\mathfrak{q}|p) = I(K_\mathfrak{q}|\mathbb{Q}_p) = I(\mathbb{Q}_p(\zeta_{p^{a_p}})|\mathbb{Q}_p) = (\mathbb{Z}/p^{a_p}\mathbb{Z})^\times.$$

$\Rightarrow |I(p)| = |(\mathbb{Z}/p^{a_p}\mathbb{Z})^\times| \quad \forall p.$

$$\Rightarrow |\underbrace{\text{subgr. of } \mathrm{Gal}(K|\mathbb{Q}) \text{ gen. by all } I(p)}_{\substack{= \mathrm{Gal}(K|\mathbb{Q}) \text{ by problem 1} \\ \text{on pset 7 (essentially} \\ \text{because } \mathbb{Q} \text{ has no unram. ext.)}}}| \leq \prod_p |(\mathbb{Z}/p^{a_p}\mathbb{Z})^\times| = |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

$\Rightarrow [K:\mathbb{Q}] \leq |(\mathbb{Z}/n\mathbb{Z})^\times|$

$\Rightarrow K = \mathbb{Q}(\zeta_n)$. $\square$

6.6. Tamely ramified extensions

We can extend the def. of "tamely ramified" to infinite ext.:

Def A Gal. ext. $L|K$ of (nonarch.) local fields is <u>tamely ramified</u> if $I^{\varepsilon}(L|K) = 1$ $\forall \varepsilon > 0$.

$$\begin{tikzcd}[row sep=small] L \arrow[dd, dash] \arrow[dr, dash, "\text{t.r.}"'] & \\ & F \arrow[dl, dash, "\text{t.r}"] \\ K & \end{tikzcd}$$

Rmk Any Gal. ext. $L|K$ has a unique max. tamely ramified subext.: $L^{\bigcup_{\varepsilon>0} I^{\varepsilon}(L|K)}$

Thm The max. tamely ramified ext. of a local field K with residue field $\mathbb{F}_q$ is

$$K^{tame} = \bigcup_{\substack{m \geq 1 \\ \gcd(m,q)=1}} K^{unram}(\pi_K^{1/m}) = \bigcup_{\substack{m \geq 1 \\ \gcd(m,q)=1}} K(\zeta_m, \pi_K^{1/m})$$

$$= \bigcup_{t \geq 0} K(\zeta_{q^t-1}, \pi_K^{1/(q^t-1)}),$$

the splitting field of all polynomials $X^m - \pi_K$ with $\gcd(m,q)=1$.

Rmk For any $\alpha \in (K^{tame})^\times$, $m \geq 1$ s.t. $\gcd(m,q) = 1$,

$X^m - \alpha$ has m distinct roots in K^{tame}.

Pf HW. $\square$

Pf of Thm

$K^{tame}|K$ is tamely ramified

$$\left.\begin{array}{l} K(\zeta_m, \pi_K^{1/m}) \\ \quad \Big| \ \text{deg. } m \text{ (totally ram.)} \\ K(\zeta_m) \\ \quad \Big| \ \text{unram.} \\ K \end{array}\right\} \quad e = m \text{ relatively prime to } q$$

$\Rightarrow p \nmid e$

$\Rightarrow \quad I_1 = 1. \Rightarrow$ tamely ram.

$\uparrow$

I_1 is the p-Sylow subgroup of I

$L|K$ fin. tamely ram. ext. $\Rightarrow L \subseteq K^{tame}$

Let $L' = L \cap K^{unram}$.

$$\begin{array}{l} L \\ \quad \Big| \ \text{tot. ram.} \\ L' \\ \quad \Big| \ \text{unram.} \\ K \end{array} \qquad \Rightarrow L = L'(\pi_L).$$

tamely ram. $\Rightarrow e(L|K) = e(L|L') = [L:L']$ relatively prime to q.

Let $f(X) = X^e + a_{e-1}X^{e-1} + \dots + a_0 \in L'[X]$ be the min. pol. of π_L over L'. It is an Eisenstein polynomial:

$$v_{L'}(a_0) = 1, \quad v_{L'}(a_1) \geq 1, \quad \dots, \quad v_{L'}(a_{e-1}) \geq 1$$

$L'|K$ unram. $\longrightarrow$

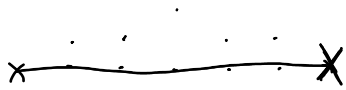
$$\begin{array}{ccc} \| & \| & \| \\ v_K(a_0) & v_K(a_1) & v_K(a_{e-1}) \end{array}$$

$f(x)$ 

Problem: $f(X) \equiv X^e \bmod \mathfrak{p}_{L'} \Rightarrow$ Can't apply Hensel's lemma directly.

Solution: "Tilt" using the substitution $Y = \pi_K^{1/e} X$.

$$g(Y) := \pi_K^{-1} f(\pi_K^{1/e} X).$$

$g(Y)$: 

$$g(Y) \equiv Y^e + \underbrace{\frac{a_0}{\pi_K}}_{\not\equiv 0} \mod \mathfrak{p}_K$$

$g(Y)$ has e roots in the residue field $\overline{\mathbb{F}}_q$ of $K^{unram} \subseteq K^{tame}$.

$$g'(Y) \equiv e Y^{e-1} \mod \mathfrak{p}_K$$

$$g'(\alpha) \equiv e\alpha^{e-1} \not\equiv 0 \mod \mathfrak{p}_K$$

$\Rightarrow$ $g(Y)$ has distinct roots mod $\mathfrak{p}_K$.

Hensel $\Rightarrow$ $g(Y)$ has e distinct roots in $\mathcal{O}_{K^{tame}}$.
(in fin. unram. ext. of K)

$$\Rightarrow \frac{\pi_L}{\pi_K^{1/e}} \in K^{tame} \Rightarrow \pi_L \in K^{tame}$$

$$\Rightarrow L \subseteq K^{tame}.$$

$\square$

Thm Let $\tau(\pi_K^{1/m}) = \zeta_m \pi_K^{1/m}$, $\tau(\zeta_m) = \zeta_m$

$\phi_q(\pi_K^{1/m}) = \pi_K^{1/m}$, $\phi_q(\zeta_m) = \zeta_m^q$.

$K(\zeta_m, \pi_K^{1/m})$
$\langle\tau\rangle \mid$
$K(\zeta_m)$
$\langle\phi_q\rangle \mid$

Then subgroup of $\mathrm{Gal}(K^{tame}|K)$ generated by τ, ϕ_q is dense. It is a semidirect product $\underbrace{\langle\tau\rangle}_{\cong\mathbb{Z}} \rtimes \underbrace{\langle\phi_q\rangle}_{\cong\mathbb{Z}}$ with $\phi_q \tau \phi_q^{-1} = \tau^q$.

Thm The max. tamely ramified abelian ext. of K is

$$K^{\text{tame, ab}} = K^{\text{unram}}\left(\pi_K^{1/(q-1)}\right),$$

$$\begin{aligned}
\mathrm{Gal}\left(K^{\text{tame, ab}}\right) &\cong \mathbb{Z}/(q-1)\mathbb{Z} \rtimes \hat{\mathbb{Z}} \\
&= \mathbb{Z}/(q-1)\mathbb{Z} \times \hat{\mathbb{Z}} \\
\Big(&\cong \mathcal{O}_K^\times / U_K^{(1)} \times \hat{\mathbb{Z}} \\
&\cong \widehat{K^\times} / U_K^{(1)} \text{ as predicted by CFT.}\Big)
\end{aligned}$$

7. Lubin-Tate theory

Now to prove that the construction of K^{ab} in 6.5 works?

Reminder: Why is $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$?

Any aut. of $\mathbb{Q}(\zeta_n)$ induces an aut. of the group ($\mathbb{Z}$-module) $\mathbb{Q}(\zeta_n)^\times \supseteq \langle \zeta_n \rangle \cong \mathbb{Z}/n\mathbb{Z}$ and the group aut. determines the aut. of $\mathbb{Q}(\zeta_n)$.

$$\Rightarrow Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \subseteq Aut_{\mathbb{Z}\text{-mod}}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times.$$

Try to generalize ...

- K = quadr. imag. number field

  Replace $\mathbb{Q}(\zeta_n)^\times$ by $E(L)$ for fin. ab. ext. $L|K$.

  $\langle \zeta_n \rangle \leadsto$ fin. subgr. ($\mathcal{O}_K$-modules)

  (<u>complex multiplication</u>)

- K nonarch. local field

  $\leadsto$ construct the group law using power series for the group operation

  (<u>Lubin-Tate theory</u>).

7.1. Formal groups

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

i) $F(X,Y) = X + Y + (\text{deg.} \geq 2 \text{ terms})$ ($\approx$ addition close to 0)

ii) $F(X,Y) = F(Y,X)$ (commutative)

iii) $\underbrace{F(X, F(Y,Z))}_{\text{only makes sense because } F(0,0)=0} = F(F(X,Y), Z)$ (associative)

Exe $\mathbb{G}_a(X,Y) = X + Y$ (additive formal group)

Exe $\mathbb{G}_m(X,Y) = (X+1)(Y+1) - 1 = X + Y + XY$

(multiplicative formal group)

so $\mathbb{G}_m(X-1, Y-1) = XY - 1$. (moved the mult. id 1 to 0).

Rmk The axioms imply $F(X,0) = X$ (identity)

and $\exists\, i(X) \in R[[X]]$: $i(X) = -X + (\text{deg.} \geq 2 \text{ terms})$

$F(X, i(X)) = 0$. (inverse).

Cor $F(X,Y) = X + Y + XY \cdot (\text{some power series in } X, Y)$.

Pf If $F(X,Y) - X - Y = (\text{deg.} \geq 2 \text{ terms})$ had a monomial of the form X^i or Y^i, then $F(X,0) \neq X$ or $F(0,Y) \neq Y$. $\square$