Local Fields Ex Sheet 3

1. (i) By definition, $e_{L|K} = v_L(\pi_K)$,

so $e_{L|K} v_K = v_L|_K$. It follows that $e_{L|K}^{-1} v_L|_K = v_K$.

Since $e_{L|K}^{-1} v_L$ is a valuation on L, we must have $e_{L|K}^{-1} v_L = w$ by uniqueness of extension. Hence

$$w(\pi_L) = e_{L|K}^{-1} v_L(\pi_L) = e_{L|K}^{-1}.$$

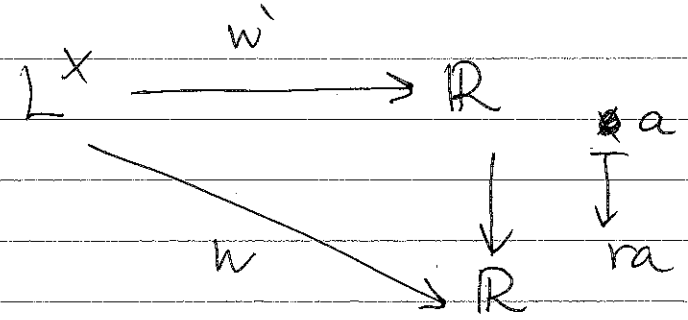
The equality $w(\pi_L) = \min_{x \in \mathfrak{m}_L} w(x)$ is clear since any element of $\mathfrak{m}_L$ has the form $\pi_L y$, $y \in \mathcal{O}_L$.

(ii) Since w' is equivalent to w,

there exists an $r \in \mathbb{R}_{>0}$ s.t

$$rw'(x) = w(x) \quad \text{for all } x \in L.$$

We then have a commutative diagram



so $a \longmapsto ra$ induces an isomorphism

$$\frac{w'(L^\times)}{w'(K^\times)} \xrightarrow{\sim} \frac{w(L^\times)}{w(K^\times)}$$

the latter group is $\frac{e_{L|K}^{-1}\mathbb{Z}}{\mathbb{Z}}$ by (i),

so $\left(w'(L^\times) : w'(K^\times)\right) = e_{L|K}$.

Now take $M/L/K$, w_K a valuation on K (in the given equivalence class), w_L its extension to L and w_M its extension to M.

Then

$$e_{M|K} = \left(w_M(M^\times) : w_K(K^\times)\right) =$$

$$= \left(w_M(M^\times) : w_L(L^\times)\right)\left(w_L(L^\times) : w_K(K^\times)\right)$$

$$= e_{M|L}\, e_{L|K} \quad .$$

2. We have $\mathcal{k}_L \cong \mathbb{F}_{q^n}$. Let $\bar{\alpha} \in \mathcal{k}_L$ be s.t $\mathcal{k}_L = \mathcal{k}_K(\bar{\alpha})$.

Let $\bar{f}$ be the minimal polynomial of $\bar{\alpha}$ / $\mathcal{k}_K$.

Then $\bar{f}(x) \mid x^{q^n-1} - 1$, say

$\bar{f}(x)\bar{g}(x) = x^{q^n-1} - 1$, and

both factors are monic and coprime

(since $x^{q^n-1} - 1$ has no repeated roots).

By Hensel's Lemma, we can lift

the factorization of $x^{q^n-1} - 1$ in $\mathcal{k}_K[X]$

to a factorization

$$f(x)g(x) = x^{q^n-1} - 1$$

in $\mathcal{O}_K[x]$, with $\overline{f}(x) = f(x) \bmod \pi_K$,

and we can lift $\overline{\alpha}$ to a root α

of $f(x)$.

Moreover, $f(x)$ is irreducible of degree n

(all this by Hensel's Lemma).

Summing up, $[K(\alpha):K] = n =$

$= [L:K]$ so $K(\alpha) = L$, and α is

a (q^n-1)th root of unity.

[illegible]

Since $\mathbb{F}_{q^n}$ contains all (q^n-1)th roots

of unity (and there are q^n-1 of them),

L contains all (q^n-1)th roots of 1 by Hensel's Lemma.

Therefore

$$L \supseteq K(\zeta_{q^n-1}) \supseteq K(\alpha) = L \implies$$

$$\implies L = K(\zeta_{q^n-1}).$$

Converse:

Let n be the order of q in $(\mathbb{Z}/m\mathbb{Z})^\times$, so $m \mid q^n-1$ but $m \nmid q^k-1$ if $k<n$.

Then $L = K(\zeta_m) \subseteq K(\zeta_{q^n-1}) =: M$,

which is unramified/K by the first part

$\implies L/K$ unramified.

It remains to compute $[L:K] = [k_L : k_K]$.

Since $k_L \subseteq k_M$, we have

$\mathcal{O}_L \cong \mathbb{F}_q^k$ for some $k \in \{1, \dots, n\}$.

If $k < n$, then $L \subseteq K(\zeta_{q^k-1}) \Rightarrow$

$\Rightarrow \zeta_m \in K(\zeta_{q^k-1})$. $\Rightarrow \zeta_m \bmod \pi_K \in \mathbb{F}_q^k$.

Consider $\zeta_m \in M$. All the (q^n-1)th roots of 1 reduce modulo π_K to distinct (q^n-1)th roots of 1. In particular, if $\zeta_m \bmod \pi_K \in \mathbb{F}_q^k$, then, since ζ_m is a (q^n-1)th root of 1, ζ_m would have to be a (q^k-1)th root of 1, but it isn't.

Thus $k = n$, so $L = M$ and $[L:K] = n$.

3. Set $L = K(\sqrt[m]{a})$.

Claim: It suffices to prove that $L|K$ is tamely ramified when $\mu_m \subseteq K$

(μ_m = group of mth roots of unity).

Pf: Let $K' = K(\mu_m)$, $L' = K'(\sqrt[m]{a})$.

By Q2 $K'|K$ is unramified, so

$$e_{L|K} \mid e_{L'|K} = e_{L'|K'} e_{K'|K} = e_{L'|K'}.$$

Thus if $e_{L'|K'}$ is coprime to p, so is $e_{L|K}$. □.

So assume that $\mu_m \subseteq K$. Then, by Kummer theory, $[L:K] \mid m \Rightarrow e_{L|K} \mid m$, so $e_{L|K}$ is coprime to p.

(The Kummer theory fact is the following:

First, note that $L|K$ is Galois, since the roots

of $x^m - a$ are $\alpha, \alpha\zeta, \dots, \alpha\zeta^{m-1}$,

$\alpha = \sqrt[m]{a}$, ζ primitive mth root of 1.

Then we have an injective homomorphism

$$\begin{aligned} \mathrm{Gal}(L|K) &\longrightarrow \mu_m \\ \sigma &\longmapsto \frac{\sigma\alpha}{\alpha} \end{aligned}$$

Pf: Independence of α: of $x^m - a$

If $\alpha\zeta^i$ is another root, then

$$\frac{\sigma(\alpha\zeta^i)}{\sigma\alpha\zeta^i} = \frac{\sigma(\alpha)}{\alpha} \cdot \frac{\zeta^i}{\zeta^i} = \frac{\sigma(\alpha)}{\alpha}.$$

Homomorphism:

$$\frac{\sigma\tau\alpha}{\alpha} = \frac{\sigma(\tau\alpha)}{\tau\alpha} \cdot \frac{\tau\alpha}{\alpha} = \frac{\sigma\alpha}{\alpha} \cdot \frac{\tau\alpha}{\alpha}$$

by above, since $\tau\alpha = \alpha\zeta^i$ for some i.

Injectivity:

α generates $L|K$, so σ is determined by $\sigma(\alpha)$.

□

4. Using Q3 and induction,

$L|K$ is tamely ramified if it

can be written as

$L = T(\sqrt[m_1]{a_1}, \dots, \sqrt[m_r]{a_r})$ for

m_i coprime to p.

Converse:

We may assume that $K = T$, so

$L|K$ is totally ramified, say of degree

m, coprime to p.

We have $\pi_L^m = \pi_K \varepsilon$ for some $\varepsilon \in \mathcal{O}_L^\times$.

Since $k_L = k_K$, $\exists \eta \in \mathcal{O}_K^\times$ and $u \in 1 + \pi_L \mathcal{O}_L$

such that $\varepsilon = \eta u$.

The polynomial $x^m - u \in \mathcal{O}_L[x]$ reduces

to $x^m - 1 \in k_L[x]$, which is separable

and has a root in k_L $(x = 1)$.

By Hensel's Lemma $\exists \beta \in \mathcal{O}_L^\times$ with

$\beta^m = u$.

Summing up, we have

$$\pi_L^m = \pi_K \eta \beta^m \Rightarrow$$

$$\Rightarrow \left(\pi_L \beta^{-1}\right)^m = \pi_K \eta .$$

$\pi_L \beta^{-1}$ is a uniformizer of L, so

$L = K(\pi_L \beta^{-1})$.

Now set $a = \pi_K \eta$, then $L = K(\sqrt[m]{a})$,

$\sqrt[m]{a} = \pi_L \beta^{-1}$.

<u>Remark</u>: We have proved something

slightly stronger, namely that

$L|K$ is tamely ramified $\Leftrightarrow$

$\Leftrightarrow$ $L = T(\sqrt[m]{a})$ for some $a \in T$,

where $m = e_{L|K}$.

5. Let $e = e_{K|\mathbb{Q}_p}$ and let π be a uniformizer of K.

Claim: If $n > \frac{e}{p-1}$, and $x \in \pi^n \mathcal{O}_K$, then $\exp(x) \in 1 + \pi^n \mathcal{O}_K = U_K^{(n)}$.

Pf: $\exp(x) = 1 + x + \frac{x^2}{2!} + \dots$

so it suffices to prove that $w\left(\frac{x^m}{m!}\right) > w(x)$ $\forall m \geq 2$, where w is the extension of v_p to K.

The condition $n > \frac{e}{p-1}$ and $x \in \pi^n \mathcal{O}_K$ translates into $w(x) > \frac{1}{p-1}$. Then

$$w\left(\frac{x^m}{m!}\right) - w(x) = (m-1)\, w(x) - \frac{m - s_p(m)}{p-1} \geq$$

$$\geq (m-1)\left(w(x) - \frac{1}{p-1}\right) > 0,$$

where $s_p(m)$ is the sum of the p-adic digits of m.

This proves the claim. $\square$

Next:

Claim: If $n > \frac{e}{p-1}$, and $x \in \pi^n \mathcal{O}_K$, then $\log(1+x) \in \pi^n \mathcal{O}_K$.

Pf: $\log(1+x) = x - \frac{x^2}{2} + \cdots$.

so it suffices to prove that $w\left(\frac{x^m}{m}\right) > w(x)$ $\forall m \geq 2$. But $w\left(\frac{x^m}{m}\right) \geq w\left(\frac{x^m}{m!}\right)$ $\forall m$, so we're done by the proof of the previous claim. $\square$.

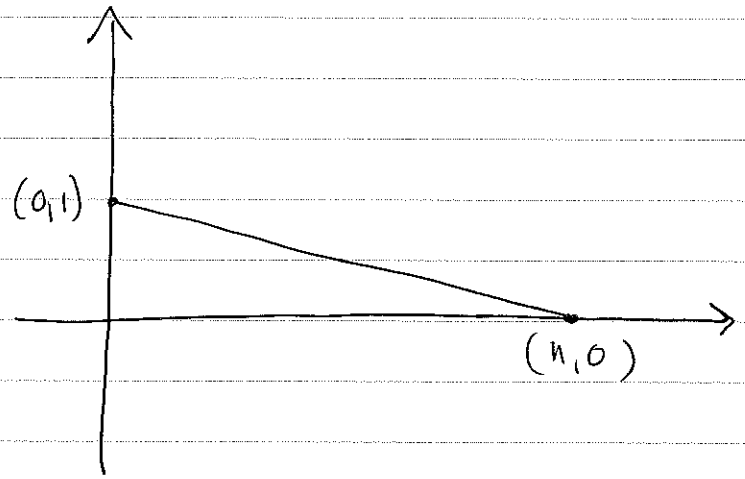
It follows that we get cts maps

$$\pi^n \mathcal{O}_K \underset{\log}{\overset{\exp}{\rightleftarrows}} 1 + \pi^n \mathcal{O}_K = U_K^{(n)}$$

$\forall n > \frac{e}{p-1}$.

They are homomorphisms with respect to addition on $\pi^n \mathcal{O}_K$ and multiplication on $1+\pi^n \mathcal{O}_K$, and mutual inverses, so $\left(U_K^{(n)}, \times\right) \cong \left(\pi^n \mathcal{O}_K, +\right) \cong \left(\mathcal{O}_K, +\right)$ $\forall n > \frac{e}{p-1}$.

6. i) The Newton polygon of f is



Let α be a root of f (in some algebraic closure of K, say). Let w be the extension of v_K to $K(\alpha)$. Then $w(\alpha) = 1/n$, so

$$e^{-1}_{K(\alpha)|K} \leq w(\alpha) = 1/n \Rightarrow$$

$$\Rightarrow n \leq e_{K(\alpha)|K} \leq [K(\alpha) : K].$$

But $[K(\alpha) : K] \leq n$ since $\deg f = n$, so we must have $[K(\alpha) : K] = n$ and f irreducible.

(ii) It suffices to show that the polynomial

$$f_n(x) = \Phi_{p^n}(x+1)$$

is Eisenstein. By Q6, Ex Sheet 2, it is monic with constant term p, so it suffices to show that

$$f_n(x) \equiv x^{p^{n-1}(p-1)} \mod p.$$

We have

$$f_n(x) = (x+1)^{p^{n-1}(p-1)} + \dots + (x+1)^{p^{n-1}} + 1 \equiv$$

$$\equiv \left(x^{p^{n-1}}+1\right)^{(p-1)} + \dots + \left(x^{p^{n-1}}+1\right) + 1 \equiv$$

$$\equiv f_1\left(x^{p^{n-1}}\right) \mod p$$

So it suffices to prove this for $n=1$.

But

$$f_1(x) = \frac{(x+1)^p - 1}{x} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1} \equiv x^{p-1}$$

$\mod p$.

iii) The criterion is that f has a single line segment of slope k/n, where k is coprime to n.

In this case, let $a, b \in \mathbb{Z}$ be s.t $ak + bn = 1$, then if α is a root of f, and w is the extension of v_K to $K(\alpha)$, we have

$$w(\alpha^a \pi_K^b) = \frac{ak}{n} + b = \frac{1}{n}$$

and $\alpha^a \pi_K^b \in K(\alpha)$, so now the same proof as in i) shows that $[K(\alpha) : K] = e_{K(\alpha)|K} = n$, so f is irreducible and $K(\alpha)|K$ is totally ramified.

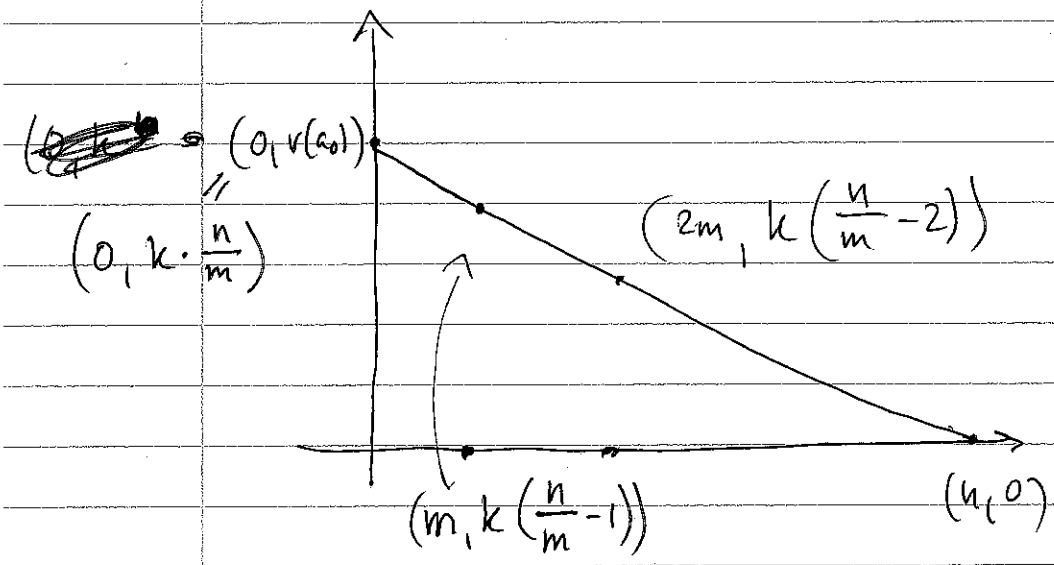
One can reformulate this criterion as saying that the Newton polygon of f

ξ has a single line segment (which must happen if f is irreducible) & and there are no points on this line segment with integer coordinates other than $(n,0)$ and $(0, v_k(a_0))$.

If this doesn't happen (and the Newton poly of f has a single line segment), then ($\exists$ minimal $m \mid n$ s.t $m \in \{1, \dots, n-1\}$, and

$$k = \frac{v(a_0)m}{n} \in \mathbb{Z} \qquad v = v_k$$

Newton polygon:



The polynomial $\left(X^m - \pi_K^k\right)^{\frac{n}{m}}$ is not irreducible, and has this Newton polygon.

7. i) Suffices to prove this for $s \in \mathbb{Z}_{\geq 0}$.

Then $\sigma \in G_s$ if and only if

σ acts trivially on $\mathcal{O}_L / \pi_L^{s+1} \mathcal{O}_L$,

which implies that G_s is normal.

$\left(= \ker\left(G \longrightarrow \mathrm{Aut}\left(\mathcal{O}_L / \pi_L^{s+1}\mathcal{O}_L\right)\right)\right)$.

ii) We have $f(X) = \prod_{\sigma \in G} (X - \sigma\alpha)$, so

$$f'(X) = \sum_{\sigma \in G} \prod_{T \neq \sigma} (X - T\alpha)$$

It follows that

$$f'(\alpha) = \prod_{\sigma \neq 1} (\alpha - \sigma\alpha) \quad \Rightarrow$$

$\Rightarrow$

$$v_L(f'(\alpha)) = \sum_{\sigma \neq 1} v_L(\sigma\alpha - \alpha) = \sum_{\sigma \neq 1} i_{L|K}(\sigma).$$

↑ by definition

Next,

$$\sum_{s \in \mathbb{Z}_{\geq 0}} (\#G_s - 1) = \sum_{s \in \mathbb{Z}_{\geq 0}} \#\left\{\sigma \in G \mid \begin{array}{l} \sigma \neq 1, \\ i_{L|K}(\sigma) \geq s+1 \end{array}\right\}$$

Each $\sigma \neq 1$ contributes to exactly $i_{L|K}(\sigma)$ terms in the sum on the RHS, so the sum is equal to $\sum_{\sigma \neq 1} i_{L|K}(\sigma)$.

It follows directly from the formula that $v_L(f'(\alpha))$ is independent of the choice of α, since both $\sum_{\sigma \neq 1} i_{L|K}(\sigma)$ and $\sum_{s \in \mathbb{Z}_{\geq 0}} (\#G_s - 1)$ are. Finally, $L|K$ unramified $\Leftrightarrow$

$\Leftrightarrow \#G_s = 1 \ \forall s \in \mathbb{Z}_{\geq 0} \Leftrightarrow v_L(f'(\alpha)) = 0$

by the formula.

8. Put $K = \mathbb{Q}_3(\zeta_3)$, $L = \mathbb{Q}_3(\zeta_3, \sqrt[3]{2})$.

Let w be the extension to L of v_3.

We know that $[K : \mathbb{Q}_3] = 2$,

with $w(\zeta_3 - 1) = \frac{1}{2}$, so $e_{K|\mathbb{Q}_3} = 2$.

We have $\mathbb{Q}_3(\sqrt[3]{2}) = \mathbb{Q}_3(1+\sqrt[3]{2})$.

the minimal polynomial of $1+\sqrt[3]{2}$ / $\mathbb{Q}_3$ is

$$(X-1)^3 - 2 = X^3 - 3X^2 + 3X - 3.$$

this is Eisenstein, so $[\mathbb{Q}_3(\sqrt[3]{2}) : \mathbb{Q}_3] = 3$,

$w(1+\sqrt[3]{2}) = \frac{1}{3}$ and $e_{\mathbb{Q}_p(\sqrt[3]{2})|\mathbb{Q}_p} = 3$.

Moreover, $\mathbb{Q}_3(\sqrt[3]{2})$ is not Galois since

$\zeta_3 \notin \mathbb{Q}_3(\sqrt[3]{2})$.

It follows that $L|\mathbb{Q}_3$ is totally ramified,

with Galois group S_3 and uniformizer

$\frac{\zeta_3 - 1}{1+\sqrt[3]{2}}$. By the general theory in

lectures, we must have $G_0(L|\mathbb{Q}_3) = S_3$

and $G_1(L|\mathbb{Q}_3) = A_3 = Gal(L|K)$, which

is generated by σ, determined by

$$\sigma(\zeta_3) = \zeta_3, \quad \sigma(\sqrt[3]{2}) = \zeta_3 \sqrt[3]{2}.$$

We have

$$i_{L|\mathbb{Q}_3}(\sigma) = v_L\left(\sigma\left(\frac{\zeta_3 - 1}{1+\sqrt[3]{2}}\right) - \frac{\zeta_3 - 1}{1+\sqrt[3]{2}}\right) =$$

$$= v_L(\zeta_3 - 1) + v_L\left(\frac{1}{1+\zeta_3\sqrt[3]{2}} - \frac{1}{1+\sqrt[3]{2}}\right) =$$

$$= 3 + v_L\left(\frac{\sqrt[3]{2} - \zeta_3\sqrt[3]{2}}{(1+\zeta_3\sqrt[3]{2})(1+\sqrt[3]{2})}\right) =$$

$$= 3 - 4 + 3 = 6 \quad \Rightarrow$$

$\Rightarrow \sigma \notin G_s(L|\mathbb{Q}_3) \ \forall s \in \mathbb{Z}_{\geq 2}$, so

$G_s(L|\mathbb{Q}_3) = 1$ for all $s \in \mathbb{Z}_{\geq 2}$.

9. $p > 2$

We have $\mathbb{Q}_p^\times = \langle p \rangle \times \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p) \cong$

$$\cong \mathbb{Z} \times \mathbb{Z}/(p-1) \times \mathbb{Z}_p$$

$$\Rightarrow \quad \mathbb{Q}_p^{\times 2} \cong 2\mathbb{Z} \times 2\mathbb{Z}/(p-1) \times \mathbb{Z}_p$$

Note that any quadratic extension of $\mathbb{Q}_p$ is of the form $\mathbb{Q}_p(\sqrt{a})$ for $a \in \mathbb{Q}_p^\times \setminus \mathbb{Q}_p^{\times 2}$, and that $\mathbb{Q}_p(\sqrt{a}) = \mathbb{Q}_p(\sqrt{b}) \iff ab^{-1} \in \mathbb{Q}_p^{\times 2}$.

So $\mathbb{Q}_p$ has three quadratic extensions, given by $\mathbb{Q}_p(\zeta_{p^2-1})$ (the unramified one), $\mathbb{Q}_p(\sqrt{p})$ and $\mathbb{Q}_p(\zeta_{p^2-1}, \sqrt{p})$ (both ramified).

It follows that $\mathbb{Q}_p(\sqrt{p}, \zeta_{p^2-1})$ is the unique ext^n with Galois gp $(\mathbb{Z}/2)^2$.

Put $L = \mathbb{Q}_p(\sqrt{p}, \zeta_{p^2-1})$, $K = \mathbb{Q}_p(\zeta_{p^2-1})$.

We have $e_{L|\mathbb{Q}_p} = 2$, $f_{L|\mathbb{Q}_p} = 2$, so

$G_0(L|\mathbb{Q}_p) = Gal(L|K) = \langle \sigma \rangle$, where

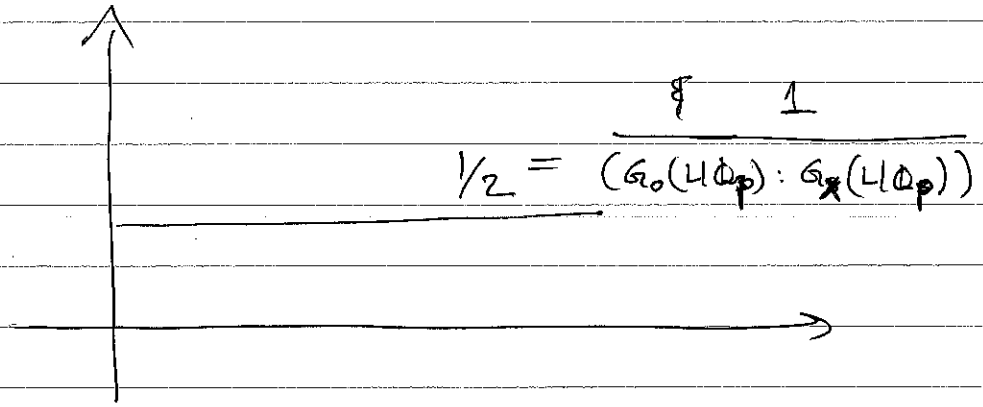
$\sigma(\sqrt{p}) = -\sqrt{p}$. $\left(L = K(\sqrt{p}) \right)$.

$\sqrt{p}$ is a uniformiser in L, so

$$i_{L|\mathbb{Q}_3}(\sigma) = v_L(\sigma(\sqrt{p}) - \sqrt{p}) =$$

$$= v_L(2\sqrt{p}) = 1 \Rightarrow$$

$\Rightarrow G_s(L|\mathbb{Q}_p) = 1 \quad \forall s \in \mathbb{Z}_{\geq 1}$ (also follows by general theory); indeed $\forall s \in \mathbb{R}_{>0}$.



$$\Rightarrow \eta_{L|\mathbb{Q}_p}(s) = \int_0^s \frac{1}{2}\, dx = s/2 \quad \text{for } s \geq 0.$$

$\Rightarrow \psi_{L|\mathbb{Q}_p}(s) = 2s$, so $G^s(L|\mathbb{Q}_p) = G_{2s}(L|\mathbb{Q}_p) =$

$= 1 \quad \forall s > 0$ (also follows by general theory).

$\underline{p=2}$:

$\mathbb{Q}_2^\times \cong \langle 2 \rangle \times (1+2\mathbb{Z}_2) \cong \langle 2 \rangle \times \langle -1 \rangle \times \mathbb{Z}_2$

(here $\mathbb{Z}_2 \cong 1+4\mathbb{Z}_2$, generated by $5 \in 1+4\mathbb{Z}_2$)

Have 7 quadratic ext'ns:

$\mathbb{Q}_2(\sqrt{5})$ (unramified), $\mathbb{Q}_2(\sqrt{-1})$, $\mathbb{Q}_2(\sqrt{2})$, $\mathbb{Q}_2(\sqrt{-2})$, $\mathbb{Q}_2(\sqrt{10})$, $\mathbb{Q}_2(\sqrt{-10})$, $\mathbb{Q}_2(\sqrt{-5})$ (ramified).

The sought extension is $M = \mathbb{Q}_2(\sqrt{5}, \sqrt{-1}, \sqrt{2})$

Put $K = \mathbb{Q}_2(\sqrt{5})$.

Have $G_0(M/\mathbb{Q}_2) = \mathrm{Gal}(M/K)$

$\underline{\text{Uniformizer of } M}$

Let w be the extension of v_2 to M.

$M = K(\sqrt{2}, \sqrt{-1})$.

$\sqrt{2}+\sqrt{-1}-1$ and $\sqrt{2}-\sqrt{-1}-1$

are conjugate over K, so have the same valuation

Have

$$(\sqrt{2}+\sqrt{-1}-1)(\sqrt{2}-\sqrt{-1}-1) = 4-2\sqrt{2}$$

and $w(4-2\sqrt{2}) = w(2\sqrt{2}) = 3/2 \Rightarrow$

$\Rightarrow w(\sqrt{2}+\sqrt{-1}-1) = 3/4$.

Set $\alpha = \sqrt{2}+\sqrt{-1}$.

Then $w(2/(\alpha-1)) = 1-3/4 = 1/4$ so

it's a uniformizer.

If $\sigma \in Gal(M/K)$, we have

$$\begin{aligned} i_{M/\mathbb{Q}_2}(\sigma) &= v_M(\sigma(2/\alpha-1) - 2/\alpha-1) = \\ &= v_M\left(\frac{2}{\sigma(\alpha-1)(\alpha-1)} \cdot (\alpha-\sigma(\alpha))\right) = \\ &= 4 - 4\cdot 2\cdot 3/4 + v(\alpha-\sigma(\alpha)) = \\ &= v(\alpha-\sigma(\alpha)) - 2 . \end{aligned}$$

We have $Gal(M/K) = \{1, \sigma_1, \sigma_2, \sigma_3\}$ with

$\sigma_1(\sqrt{2}) = -\sqrt{2}$, $\sigma_1(\sqrt{-1}) = \sqrt{-1}$, $\sigma_2(\sqrt{2}) = \sqrt{2}$,

$\sigma_2(\sqrt{-1}) = -\sqrt{-1}$, $\sigma_3 = \sigma_2\sigma_1$.

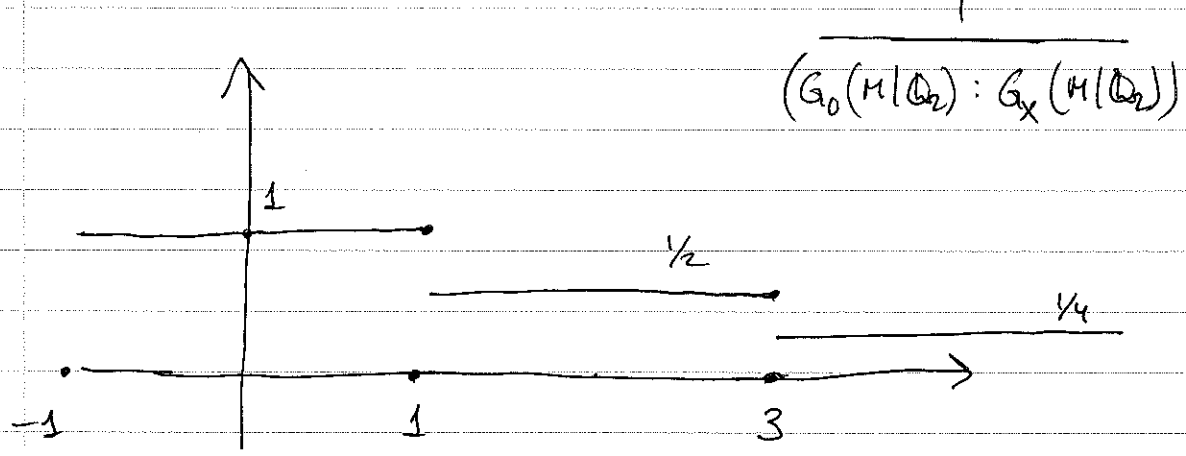
Then one computes

$$v_L(\sigma\alpha - \sigma_1\alpha) = 6, \quad v_L(\alpha - \sigma_2\alpha) = v_L(\alpha - \sigma_3(\alpha)) = 4$$

So

$$G_s(M|\mathbb{Q}_2) = \begin{cases} Gal(M|\mathbb{Q}_2) & s = -1 \\ Gal(M|K) & -1 < s \leq 1 \\ \langle \sigma_1 \rangle & +1 < s \leq 3 \\ 1 & s > 3 \end{cases}$$

Upper numbering:



$$\frac{1}{(G_0(M|\mathbb{Q}_2) : G_x(M|\mathbb{Q}_2))}$$

$$\eta_{M|\mathbb{Q}_2}(s) = \begin{cases} s & -1 \leq s \leq 1 \\ 1 + \frac{s-1}{2} & 1 \leq s \leq 3 \\ 2 + \frac{s-3}{4} & s \geq 3 \end{cases}$$

$$\psi_{M|\mathbb{Q}_2}(t) = \begin{cases} t & -1 \leq t \leq 1 \\ 2t-1 & 1 \leq t \leq 2 \\ 4t-5 & t \geq 2 \end{cases}$$

So

$$G^t(M|\mathbb{Q}_2) = G_{\psi_{M|\mathbb{Q}_2}(t)}(M|\mathbb{Q}_2) =$$

$$= \begin{cases} Gal(M|\mathbb{Q}_2) & t = -1 \\ Gal(M|K) & -1 < t \leq 1 \\ \langle \sigma_1 \rangle & 1 < t \leq 2 \\ 1 & t > 2 \end{cases}$$

10. Set $G = Gal(L|K) \cong S_4$,

$G_0 = G_0(L|K)$, $G_1(L|K) =: G_1$.

We treat them as subgroups of S_4.

They are both normal, G/G_0 is cyclic, G_1 is the unique Sylow p-subgroup of G_0, and G_0/G_1 is also cyclic (it embeds into

k_L^x)

the only nontrivial normal 2-subgroup of S_4 is $V = \{(12)(34), (14)(23), (13)(24), id\}$ with $p=2$.

If $G_1 = 1$, then G_0 is cyclic $\Rightarrow$

$\Rightarrow G_0 = 1 \Rightarrow G$ cyclic and $\cong S_4$, a contradiction, so we must have $p=2$.

Example when $K = \mathbb{Q}_2$.

Take $f(x) = x^4 + 2x + 2$ and let $L/\mathbb{Q}_2$ be the splitting field of f. f is Eisenstein, so irreducible. Its resolvent cubic (or, one of them) is $g(y) = y^3 - 8y - 4$, whose Newton polygon has a single slope $-2/3$, so it is irreducible. The discriminant of g is $-4(-8)^3 - 27(-4)^2 = 2^4(2^7 - 27)$ and

$2^7 - 27 \equiv 5 \bmod 8$, which is not a square, so g has Galois group $S_3 \Rightarrow$

$\Rightarrow f$ has Galois group S_4.

11. Write $m = m' p^n$ with $(m', p) = 1$.

Then $\mathbb{Q}_p(\zeta_m) = \mathbb{Q}_p(\zeta_{m'}) \cdot \mathbb{Q}_p(\zeta_{p^n})$

and so

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_m) | \mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{Q}_p(\zeta_{m'}) | \mathbb{Q}_p) \times$$

$$\times \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n}) | \mathbb{Q}_p) \cong$$

$$\cong \mathbb{Z}/k\mathbb{Z} \times (\mathbb{Z}/p^n)^\times$$

where k is the order of p in $(\mathbb{Z}/m'\mathbb{Z})^\times$.

To compute the ramification groups, we use the following fact:

Claim: Let K be a local field, $\overline{K}$ an algebraic closure of K. Let $L|K$ be an unramified ext^n and let $M|K$ be a totally ramified Galois ext^n, with $L, M \subseteq \overline{K}$.

Then $Gal(LM|L) \cong Gal(M|K)$ via restriction, and via restriction we have

$$G_s(LM|K) \cong G_s(M|K) \quad \text{and}$$

$$G^t(LM|K) \cong G^t(M|K)$$

for all $s, t > -1$.

Proof: We have $L \cap M = K$ since $L \cap M$ is both unramified and totally ramified $/K$. Galois theory then gives us $Gal(LM|L) \cong Gal(M|K)$.

Let $\pi \in M$ be a uniformizer and note that it is also a uniformizer of LM, and $v_{LM}|_M = v_M$. $LM|L$ is totally ramified, and $L = T_{LM/K}$,

so $G_s(LM|K) = G_s(LM|L) \quad \forall s > -1$

(from lectures).

Then note that $G_{LM} = G_L[\pi]$ and $G_M = G_K[\pi]$,

so it follows that

$$i_{LM|L}(\sigma) = i_{LM|K}(\sigma|_M)$$

for all $\sigma \in Gal(LM|L)$.

It follows that $G_s(M|K) \cong G_s(LM|L) =$

$= G_s(LM|K)$ for all $s > -1$ via restriction.

For the upper numbering, note that it follows that

$$\frac{1}{(G_0(LM|K) : G_x(LM|K))} = \frac{1}{(G_0(M|K) : G_x(M|K))}$$

for all $x \in (-1, \infty)$, so $\eta_{LM|K}(s) = \eta_{M|K}(s)$

for all $s \in [-1, \infty)$, and hence

$$G^t(LM|K) = G_{\psi_{LM|K}(t)}(LM|K) = G_{\psi_{M|K}(t)}(M|K) =$$

$$= G^t(M|K) \text{ for all } t > -1.$$

□

We now return to cyclotomic fields.

Using the results in lectures for $\mathbb{Q}_p(\zeta_{p^n}) \mid \mathbb{Q}_p$, we get

$$G_s(\mathbb{Q}_p(\zeta_m) \mid \mathbb{Q}_p) = \begin{cases} \mathrm{Gal}(\mathbb{Q}_p(\zeta_m) \mid \mathbb{Q}_p), & s = -1 \\ \mathrm{Gal}(\mathbb{Q}_p(\zeta_m) \mid \mathbb{Q}_p(\zeta_{m'})), & -1 < s \leq 0 \\ \mathrm{Gal}(\mathbb{Q}_p(\zeta_m) \mid \mathbb{Q}_p(\zeta_{m'p})), & 0 < s \leq p-1 \\ \vdots & \vdots \\ \mathrm{Gal}(\mathbb{Q}_p(\zeta_m) \mid \mathbb{Q}_p(\zeta_{m'p^{n-1}})), & p^{n-2}-1 < s \leq p^{n-1}-1 \\ 1, & s > p^{n-1}-1 \end{cases}$$

the ramification groups in the upper numbering were stated in lectures.

12. Let $x \in U_K^{(1)}$ and $a \in \mathbb{Z}_p$.

Then $\mathbb{Z}_p$-module structure on $U_K^{(1)}$ is defined by

$$x^a := \sum_{n=0}^{\infty} \binom{a}{n} (x-1)^n$$

From Q8, Ex Sheet 2, we see that $x^{ab} = (x^a)^b$ and $x^{a+b} = x^a x^b$, and that it extends the abelian group structure. Moreover, one easily sees that $(xy)^a = x^a y^a$ $\forall x, y \in U_K^{(1)}$, and $a \in \mathbb{Z}_p$, using the fact that it's true for $a \in \mathbb{Z}$ and density of $\mathbb{Z} \subseteq \mathbb{Z}_p$.

Second part:

char $K = 0$:

By Q5, $U_K^{(n)} \cong (\mathcal{O}_K, +) \cong \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$ for sufficiently large n. Note that these

are actually isomorphisms of $\mathbb{Z}_p$-modules:

First, $x \in U_K^{(n)} \Rightarrow x^a = 1 + (x-1)\sum_{n=1}^{\infty} \binom{a}{n}(x-1)^n \in$

$\in U_K^{(n)}$,

so $U_K^{(n)}$ is a sub-$\mathbb{Z}_p$-module of $U_K^{(1)}$ $\forall n \geq 1$.

Second, $\exp(ax) = \exp(x)^a$ $\forall x \in \pi_K^n \mathcal{O}_K$, $n > \frac{e_{K|\mathbb{Q}_p}}{p-1}$, and $a \in \mathbb{Z}_p$, by the usual "true for $a \in \mathbb{Z}_{\geq 0}$ + density argument", so exp is a $\mathbb{Z}_p$-module isomorphism $\pi_K^n \mathcal{O}_K \cong U_K^{(n)}$.

Since $U_K^{(1)}/U_K^{(n)}$, it follows that $U_K^{(1)}$ is a finitely generated $\mathbb{Z}_p$-module of rank $[K:\mathbb{Q}_p]$

$\Rightarrow U_K^{(1)} \cong \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$ for some $a \in \mathbb{Z}_{\geq 0}$, by the structure theorem.

We then have

$$K^\times \cong \langle \pi_K \rangle \times \mathcal{O}_K^\times \cong \langle \pi_K \rangle \times [\mathbb{F}_q^\times] \times U_K^{(1)} \cong$$

$$\cong \mathbb{Z} \times \mathbb{Z}/q-1 \times \mathbb{Z}/p^a \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$$

where $[k_K^\times] \subseteq \mathcal{O}_K^\times$ denotes the subgroup of non-zero Teichmüller lifts.

<u>char $K = p$:</u>

Again one has

$$K^\times \cong \langle \pi_K \rangle \times [k_K^\times] \times U_K^{(1)} \cong$$

$$\cong \mathbb{Z} \times \mathbb{Z}/q-1 \times U_K^{(1)},$$

so it suffices to show that $U_K^{(1)} \cong \mathbb{Z}_p^{\mathbb{Z}_{\geq 0}}$ as $\mathbb{Z}_p$-modules.

We have $K \cong \mathbb{F}_q((t))$. Set $\pi_K = t$, we have $U_K^{(1)} = 1 + t\mathbb{F}_q[[t]]$.

Put $f = \log_p q$ (so $q = p^f$) and let $w_1, \dots, w_f$ be an $\mathbb{F}_p$-basis for $\mathbb{F}_q$.

Define $g_n : \mathbb{Z}_p^f \longrightarrow U^{(n)}$ by

$$g_n(a_1, \dots, a_f) = \prod_{i=1}^{f} (1 + w_i t^n)^{a_i},$$

for each $n \in \mathbb{Z}_{\geq 1}$ s.t $(n,p)=1$.

Claim 1) If $m = np^s$, $s \in \mathbb{Z}_{\geq 0}$, then

$$U^{(m)} = g_n(p^s \mathbb{Z}_p^f) U^{(m+1)}$$

2) $(a_1, \dots, a_f) \in p\mathbb{Z}_p^f \iff g_n(p^s a_1, \dots, p^s a_f) \in U^{(m+1)}$.

Pf: Write $\omega = \sum_{i=1}^{f} b_i \omega_i$, $b_i \in \mathbb{Z}$ s.t $b_i \equiv a_i \bmod p$. Then

$$g_n(a_1, \dots, a_f) \equiv \prod_{i=1}^{f} (1+\omega_i t^n)^{b_i} \equiv$$

$$\equiv 1 + \omega t^n \bmod t^{n+1}.$$

$$\Rightarrow g_n(p^s a_1, \dots, p^s a_f) = g_n(a_1, \dots, a_f)^{p^s} \equiv$$

$$\equiv 1 + \omega^{p^s} t^m \bmod t^{m+1}$$

The map $\mathbb{Z}_p^f \longrightarrow \mathbb{F}_q$

$$(a_1, \dots, a_n) \longmapsto \omega^{p^s}$$

is surjective, so we get $g_n(p^s \mathbb{Z}_p^f) U^{(m+1)} = U^{(m)}$, i.e 1). Furthermore, one has

$g_n(p^s a_1, \dots, p^s a_f) \equiv 1 \bmod t^{m+1} \Leftrightarrow$

$\Leftrightarrow \omega = 0 \Leftrightarrow a_i \equiv 0 \bmod p \ \forall i \Leftrightarrow$

$\Leftrightarrow (a_1, \dots, a_f) \in p\mathbb{Z}_p^f$, which is 2). $\square$.

Set $A = \prod_{(n,p)=1} \mathbb{Z}_p^f$, and let

$g : A \longrightarrow U^{(1)}$ be given by

$$g\left((a_1^{(n)}, \dots, a_f^{(n)})_n\right) = \prod_{(n,p)=1} g_n(a_1^{(n)}, \dots, a_f^{(n)})$$

This products converges since $g_n(a_1^{(n)}, \dots, a_f^{(n)}) \in$
$\in U^{(n)}$.

Let $m = np^s$, $s \geq 0$. with $(n,p) = 1$. We have
$g_n(\mathbb{Z}_p^f) \subseteq g(A)$, so by part 1) of
the claim g is surjective onto $U^{(1)}/U^{(m)}$ for
all $m \Rightarrow g(A) \subseteq U^{(1)}$ is dense.

We give A the product topology; then
A is compact (by Tychonoff's thm) and

Hausdorff, and one can check that g is continuous. It follows that $g(A) \subseteq U_q^{(1)}$ is closed, hence $g(A) = U^{(1)}$.

It remains to prove that g is injective.

Let $\{(a_1^{(n)}, \dots, a_f^{(n)})_n \in \prod_{(n,p)=1} \mathbb{Z}_p^f$ be nonzero; and let n be s.t. $(a_1^{(n)}, \dots, a_f^{(n)}) \neq 0$. Then $\exists s \in \mathbb{Z}_{\geq 0}$ and $(b_1^{(n)}, \dots, b_f^{(n)}) \in \mathbb{Z}_p^f \setminus p\mathbb{Z}_p^f$ s.t. $a_i^{(n)} = p^s b_i^{(n)}$ $\forall i$.

If $m = np^s$, part 2) of the claim implies that $g_n(a_1^{(n)}, \dots, a_f^{(n)}) \in U^{(m)}$, $g_n(a_1^{(n)}, \dots, a_f^{(n)}) \notin U^{(m+1)}$

Pick n s.t. $(a_1^{(n)}, \dots, a_f^{(n)}) \neq 0$ and the number $m = m(n)$ is smallest (note that they are all distinct). Then, for all $n' \neq n$,

$$g_{n'}(a_1^{(n')}, \dots, a_f^{(n')}) \in U^{(m+1)},$$

and so $g((a_1^{(k)}, \dots, a_f^{(k)})_k) \equiv g_n(a_1^{(n)}, \dots, a_f^{(n)})$

$\not\equiv 0 \mod U^{(m+1)}$,

so $\ker g = 1$. This finishes the proof.

13. Since K has a unique unramified ext^n K_d of degree d for all $d \geq 1$, we have

$$\#(\text{separable ext}^n\text{s of } K \text{ of deg } n) =$$

$$= \sum_{d|n} \#(\text{totally ramified sep ext}^n\text{s of } K_d \text{ of degree } n/d)$$

So it suffices to consider totally ramified extensions.

Assume $\mathrm{char}\, K \nmid n$.

Let $E_n = \{$ Eisenstein polys of deg $n\}$

$$E_n \cong \pi_K \mathcal{O}_K^{n-2} \times (\pi_K \mathcal{O}_K \setminus \pi_K^2 \mathcal{O}_K)$$

via $x^n + a_{n-1}x^{n-1} + \dots + a_0 \mapsto (a_{n-1}, \dots, a_0)$

the RHS is naturally a compact metric space under the metric

$$d((a_{n-1},\dots,a_0),(b_{n-1},\dots,b_0)) = \max_{i=0,\dots,n-1} |a_i - b_i|$$

Each $f \in E_n$ gives rise to at most n distinct ramified ext^{n}s of K obtained by adjoining a root of f.

Given $f \in E_n$ and a root α of f, (Q9, Ex Sheet 2) continuity of roots shows that $\exists$ open $U(f,\alpha) \subseteq E_n$ s.t

$f \in$

such that for all $g \in U(f,\alpha)$, there is a root β of g s.t

$$|\alpha - \beta| < |\alpha - \alpha'|$$

for all roots $\alpha' \neq \alpha$ of f.

Set $U^{(f)} = \bigcap_{\alpha \text{ root of } f} U(f,\alpha)$; then if $g \in U(f)$, there is a bijection between the roots of g and f matching up the "closest roots", and by Krasner's Lemma the totally ramified ext'ns of K generated by the roots of g match up with those generated by the roots of f. Here we use $\mathrm{char}\, K \nmid n$ to ensure that f is seperable

Since $E_n = \bigcup_{f \in E_n} U(f)$ and E_n is compact, $\exists$ finite subcover $U(f_1), \ldots, U(f_r)$

$\Rightarrow$ there are only finitely many totally

ramified ext^n of deg n generated by roots of Eisenstein polynomials.

But any totally ramified ext^n of $\mathbb{Q}$ is generated by the root of an Eisenstein polynomial, so there are only finitely many such extensions.

When $\operatorname{char} k = p$, there are infinitely many separable ext^n's of deg p.

To see this, we use Artin-Schreier theory

K

Thm: Let K be a field of characteristic p. $L|K$ is Galois of degree p $\Leftrightarrow$ $\Leftrightarrow$ L is the splitting field of an irreducible polynomial $f_\alpha(x) = X^p - X + \alpha$ for $(\alpha \in K)$.

$x^p - x + \alpha$ is irreducible $\iff$

$\alpha \notin \{y \in K \mid \exists x \in K \text{ s.t } y = x^p - x\}$,

and $x^p - x + \alpha$ and $x^p - x + \beta$ have the same splitting field $\iff$ $\alpha = a + b\beta$ for some $a, b \in \mathbb{F}_p$, $b \neq 0$.

Now let K be a local field of characteristic p.

Claim: $K / \{y \in K \mid \exists x \in K \text{ s.t } y = x^p - x\}$ is infinite.

Pf: $K \cong \mathbb{F}_q((t))$. If $y = x^p - x$ and $v_K(y) < 0$, then $v_K(x) < 0$ and hence $v_K(y) = v_K(x^p - x) = p v(x)$. Thus, the elements t^{-n}, $n \in \mathbb{Z}_{\geq 1}$, $(n, p) = 1$

lie in distinct equivalence classes modulo $\{y \in k \mid \exists x : x^p - x = y\}$. □

It follows that there are infinitely many distinct Galois ext^{n}s of degree p over K, using the previous thm.