Algebraic Number theory

Rough solutions Sheet 3

1. We have $k_L \cong \mathbb{F}_{q^n}$, so the Teichmüller lifts are precisely the $(q^n-1)^{th}$ roots of 1 and 0 $\Rightarrow$

$\Rightarrow \quad L \supseteq K(\zeta_{q^n-1})$.

On the other hand, every element of L can be written as

$$\sum_{i>>-\infty}^{\infty} [a_i] \pi_K^i, \quad a_i \in k_L$$ (using L unramified, i.e. π_K uniformizer of L)

so $K(\zeta_{q^n-1})$ is dense in L.

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

Converse:

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

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

$M|K$ unramified by first part $\Rightarrow$

$\Rightarrow L|K$ unramified, and

$[L:K] = [k_L : k_K] \leq [k_M : k_K] = [M:K] =$

$= f$.

Since $\zeta_m = [\bar{\zeta}_m]$, where $\bar{\ }$ denotes

reduction mod π_K in $\mathcal{O}_M$,

$\bar{\zeta}_m^{q^k-1} \neq 1$ for $k<f$. Thus

$k_L \supseteq k_K(\bar{\zeta}_m) = k_M \Rightarrow k_L = k_M \Rightarrow$

$\Rightarrow L = M$.

2. $f(T) = \prod_{\sigma \in G} (T - \sigma\alpha) \Rightarrow$

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

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

$$\Rightarrow \quad v_L(f'(\alpha)) = \sum_{\sigma \neq 1} v_L(\sigma\alpha - \alpha) \overset{\text{by definition}}{=}$$

$$= \sum_{\sigma \neq 1} i_G(\sigma).$$

Next, $\displaystyle\sum_{s \in \mathbb{Z}_{\geq 0}} (\# G_s - 1) =$

$$= \sum_{s \in \mathbb{Z}_{\geq 0}} \# \left\{ \sigma \in G \;\middle|\; \begin{array}{l} \sigma \neq 1 \\ i_G(\sigma) \geq s+1 \end{array} \right\}$$

Each $\sigma \neq 1$ contributes to exactly $i_G(\sigma)$ terms in the sum, so the sum is

$$\sum_{\sigma \neq 1} i_G(\sigma).$$

It follows directly that $v_L(f'(\alpha))$ is independent of α. Finally,

$L|K$ unramified $\Leftrightarrow \# G_s = 1 \ \forall s \geq 0 \Leftrightarrow$

$\Leftrightarrow v_L(f'(\alpha)) = 0$ by the formula.

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

Let w be the ext^n to L of v_3 on $\mathbb{Q}_3$.

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

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

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

$$(T-1)^3 - 2 = T^3 - 3T^2 + 3T - 3$$

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

$= 3$, $w(1+\sqrt[3]{2}) = \frac{1}{3}$ & $e_{\mathbb{Q}_3(\sqrt[3]{2})|\mathbb{Q}_3} = 3$

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

with Galois group $G = S_3$ and uniformizer

$$\frac{\zeta_3 - 1}{1+\sqrt[3]{2}}$$

By general theory in lectures we must have $G_0(L|\mathbb{Q}_3) = S_3$ and $G_1(L|\mathbb{Q}_3) = A_3 = \mathrm{Gal}(L|K)$, which is generated by σ, determined by

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

We have

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

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

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

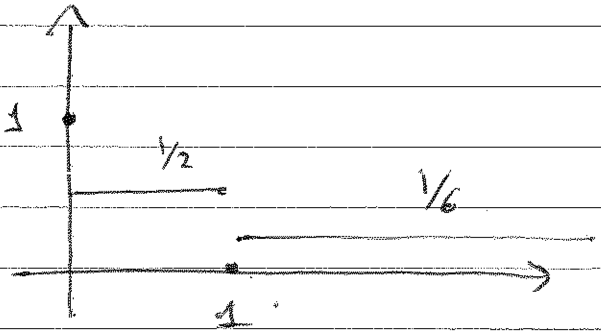
$$= 3 - 4 + 3 = 2 \implies$$

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

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

Upper numbering:

$\dfrac{1}{(G_0 : G_x)}$



$$\varphi(s) = \begin{cases} s/2 , & 0 \le s \le 1 \\ 1/2 + \frac{s-1}{6} , & s \ge 1 . \end{cases}$$

$$\psi(t) = \begin{cases} 2t , & 0 \le t \le \frac{1}{2} \\ 1 + 6(t - 1/2) , & t \ge 1/2 . \end{cases}$$

$$\Rightarrow \quad G^t(L \mid Q_3) = \begin{cases} S_3 & t = 0 \\ A_3 & 0 < t \le 1/2 \\ 1 & t > 1/2 . \end{cases}$$

(example of when G^t changes at a non-integer value of t).

4. We have

$$\mathbb{Q}_2^\times = \langle 2 \rangle \times \langle 1 + 2\mathbb{Z}_2 \rangle =$$

$$= \langle 2 \rangle \times \langle -1 \rangle \times 1 + 4\mathbb{Z}_2$$

and $(\mathbb{Q}_2^\times)^2 = \langle 4 \rangle \times 1 + 8\mathbb{Z}_2$, so

$\mathbb{Q}_2$ has 7 quadratic ext^{n}s

$\mathbb{Q}_2(\sqrt{5}) = \mathbb{Q}_2(\sqrt{-3}) = \mathbb{Q}_2(\zeta_3)$ unramified,

$\mathbb{Q}_2(\sqrt{-1})$, $\mathbb{Q}_2(\sqrt{2})$, $\mathbb{Q}_2(\sqrt{-2})$, $\mathbb{Q}_2(\sqrt{10})$,

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

The sought extension is

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

(note that an ext^n with Galois group $(\mathbb{Z}/2)^3$ has 7 quadratic subext^n, so there can only be one) Put $G = Gal(M|\mathbb{Q}_3)$.

Put $K = \mathbb{Q}_2(\sqrt{5})$, have $G_0(M|\mathbb{Q}_2) = Gal(M|K)$

~~[illegible]~~

Note that $K = \mathbb{Q}_2(\zeta_3)$ and that

$\exists!$ totally ramified ext^n of $\mathbb{Q}_2$ with

Galois group $(\mathbb{Z}/2)^2$, given by

$\mathbb{Q}_2(\sqrt{-1}, \sqrt{2})$.

But also $\mathrm{Gal}(\mathbb{Q}_2(\zeta_8) | \mathbb{Q}_2) \cong (\mathbb{Z}/8)^\times \cong$

$\cong (\mathbb{Z}/2)^2$

$\Rightarrow$ $\mathbb{Q}_2(\sqrt{-1}, \sqrt{2}) = \mathbb{Q}_2(\zeta_8)$ and we

can use the computation of ramification

groups of $M = \mathbb{Q}_2(\zeta_3, \zeta_8) = \mathbb{Q}_2(\zeta_{24})$

from lectures.

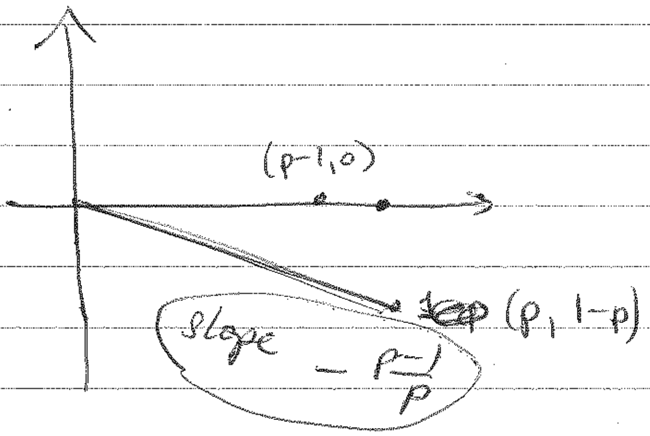
For an alternative, more direct, solution, see

Rough solutions for Q9, Sheet 3 for my

Local Fields course last year on my

website.

5. $f(X)$ has Newton polygon



~~Slope~~ $\Rightarrow$ $f(X)$ is irreducible

and $L|K$ totally ramified (use criterion

from last sheet; $f(X)$ separable since

$f'(X) = -1$ is coprime to $f(X)$):

Let α be a root of f in L, then

$v_L(\alpha) = 1-p$. Since $v_L(t) = p$,

$v_L(t\alpha) = 1$ so $t\alpha$ is a uniformizer.

<u>$L|K$ Galois</u>

If $k \in \{0, 1, \ldots, p-1\}$,

$f(\alpha+k) = (\alpha+k)^p - (\alpha+k) - t^{1-p} =$

$= f'(\alpha) = 0$, so L contains all p roots of f.

A generator σ for $G = \mathrm{Gal}(L|K) \cong \mathbb{Z}/p$ is determined by $\sigma(\alpha) = \alpha + 1$.

Have

$$i_G(\sigma) = v_L(\sigma(t\alpha) - t\alpha) =$$
$$= v_L(t(\alpha+1) - t\alpha) =$$
$$= v_L(t) = p,$$

$$\text{so: } G_s(L|K) = \begin{cases} G, & 0 \leq s \leq p-1 \\ 1, & s > p-1. \end{cases}$$

6. Set $G = \mathrm{Gal}(L|K) \cong S_4$,

$G_0 = G_0(L|K)$, $G_1 = G_1(L|K)$;

we treat them as subgroups of S_4.

G_0, G_1 normal, G/G_0 cyclic,

G_1 is the unique Sylow p-subgroup

of G_0 and G_0/G_1 also cyclic.

The only nontrivial normal p-subgroup of

S_4 is $V = \{(12)(34), (14)(23), (13)(24), id\}$

with $p=2$.

If $G_1 = 1$, then G_0 cyclic & normal $\Rightarrow G_0 = 1 \Rightarrow$

$\Rightarrow G$ cyclic and $\cong S_4$ #.

So we must have $p = 2$.

<u>Example when $K = \mathbb{Q}_2$:</u>

Take $f(T) = T^4 + 2T + 2$ and let

$L | \mathbb{Q}_2$ be the splitting field of f.

f Eisenstein $\Rightarrow$ f 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's 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 gp

S_3 & f has Galois group S_4.

7. $(J, \leq)$ is a partially ordered set.

Let $j_1, j_2 \in J$. Since $(I, \leq)$ is a directed system, $\exists i \in I$ s.t $j_1, j_2 \leq i$. By assumption, $\exists j_3 \in J$ s.t $i \leq j_3$, so $j_1, j_2 \leq j_3$.

Hence $(J, \leq)$ is a directed system.

<u>Second part</u>:

There is a continuous homomorphism

$$\Phi : \prod_{i \in I} G_i \longrightarrow \prod_{j \in J} G_j$$

$$\Phi((g_i)_{i \in I}) = (g_i)_{i \in J}.$$

which maps $\varprojlim_{i \in I} G_i$ into $\varprojlim_{j \in J} G_j$,

Call this map $\phi : \varprojlim_{i \in I} G_i \longrightarrow \varprojlim_{j \in J} G_j$

~~Assume that~~

Let $(x_i)_{i\in I} \in \varprojlim_{i\in I} G_i$.

Assume that $\phi((x_i)_{i\in I}) = (1)$, i.e

that $x_j = 1$ if $j \in J$. ~~Choose~~ Let $i \in I$,

and choose $j \in J$ with $i \leq j$.

Then $x_i = f_{ij}(x_j) = 1$, so

$x_i = 1 \ \forall i \in I \implies \phi$ injective.

<u>ϕ surjective:</u>

Let $(x_j)_{j\in J} \in \varprojlim_{j\in J} G_j$. If $i \in I$,

define $x_i = f_{ij}(x_j)$ where $j \in J$ is s.t

$i \leq j$.

This is well-defined: If $i \leq j_1, j_2$,

then $\exists j_3$ s.t $j_1, j_2 \leq j_3$, and

$$f_{ij_2}(x_{j_2}) = f_{ij_2}(f_{j_2j_3}(x_{j_3})) =$$
$$= f_{ij_3}(x_{j_3}) = f_{ij_1}(f_{j_1j_3}(x_{j_3})) =$$
$$= f_{ij_1}(x_{j_1}),$$

so it's well-defined.

We claim that $(x_i)_{i\in I} \in \varprojlim_{i\in I} G_i$:

If $i_1 \leq i_2 \in I$, then $\exists j \in J$ with $i_2 \leq j$, and

$$x_{i_1} = f_{i_1j}(x_j) = f_{i_1i_2}(f_{i_2j}(x_j)) =$$
$$= f_{i_1i_2}(x_{i_2}),$$

so $(x_i)_{i\in I} \in \varprojlim_{i\in I} G_i$

Clearly $\phi((x_i)_{i\in I}) = (x_j)_{j\in J}$, so

ϕ surjective.

<u>ϕ homeomorphism</u>:

ϕ is cts by construction, so we need to show that any open $U \subseteq \varprojlim_{i\in I} G_i$ is the preimage of an open set in $\varprojlim_{j\in J} G_j$.

By construction of the inverse limit topology, U is ~~the~~ a union of sets of the form $\pi_i^{-1}(V)$, where $\pi_i : \varprojlim_{i\in I} G_i \to G_i$ is the projection and $V \subseteq G_i$ is open, so without loss of generality we may take U to be of this form.

Pick $j \in J$ with $i \leq j$. We have a commutative diagram

$$\begin{tikzcd}
\varprojlim_{i\in I} G_i \arrow[r, "\phi"] \arrow[d, "\pi_i"] & \varprojlim_{j\in J} G_j \arrow[d, "\pi_j"] \\
G_i & G_j \arrow[l, "f_{ij}"]
\end{tikzcd}$$

so $\quad U = \pi_i^{-1}(V) =$

$$= \phi^{-1}\left(\pi_j^{-1}\left(f_{ij}^{-1}(V)\right)\right)$$

and $\pi_j^{-1}\left(f_{ij}^{-1}(V)\right)$ is open in $\varprojlim_{j\in J} G_j$.

8. (i) $\underline{\phi \text{ injective}}$:

Let $\sigma \in Gal(M|K)$. Note that

$M = \bigcup_{L\in I} L$. Thus, if $\sigma|_L = id_L \; \forall L \in I$,

then $\sigma = id$.

$$\underline{\operatorname{Im}\phi = \varprojlim_{L\in I} Gal(L|K)}$$

First, note that if $\sigma \in Gal(M|K)$ and

$L_1, L_2 \in I$ with $L_1 \subset L_2$, then

$(\sigma|_{L_2})|_{L_1} = \sigma|_{L_1} \implies$

$\Rightarrow \quad \operatorname{Im}\phi \subseteq \varprojlim_{L \in I} \operatorname{Gal}(L|K)$

Now let $(\sigma_L)_{L \in I} \in \varprojlim_{L \in I} \operatorname{Gal}(L|K)$.

Let $x \in M$ and define $\sigma(x) = \sigma_L(x)$ for any $L \in I$ with $x \in L$.

This is well-defined: If $x \in L_1, L_2$, then $\sigma_{L_1}(x) = \sigma_{L_1 L_2}(x) = \sigma_{L_2}(x)$.

Therefore $\sigma : M \to M$ is a function, and it's clearly a homomorphism and satisfies $\sigma|_L = \sigma_L$ and $\sigma|_K = \mathrm{id}$.

To show $\sigma \in \operatorname{Gal}(M|K)$, ~~note that~~ we need $\sigma(M) = M$. Note that

$\sigma(M) \supseteq \sigma|_L(L) = \sigma_L(L) = L \ \forall L \in I$,

so $\sigma(M) \supseteq \bigcup_{L \in I} L = M$.

(ii) Each $\mathrm{Gal}(L|K)$ is finite and discrete, hence compact & Hausdorff. It follows that $\prod_{L \in I} \mathrm{Gal}(L|K)$ is compact (by Tychonoff) and Hausdorff (easy to check).

<u>$\varprojlim_{L \in I} \mathrm{Gal}(L|K) \subseteq \prod \mathrm{Gal}(L|K)$ closed:</u>

Let $L_1 \le L_2$ in I. We have a continuous map

$$f_{L_1, L_2} : \prod \mathrm{Gal}(L|K) \longrightarrow \mathrm{Gal}(L_1|K)$$

$$(\sigma_L)_{L \in I} \longmapsto \sigma_{L_1} \left(\sigma_{L_2}|_{L_1} \right)^{-1}.$$

Set $X_{L_1, L_2} = f^{-1}_{L_1, L_2}(\mathrm{id}_{L_1})$.

This is closed, and

$$\varprojlim_{L \in I} \mathrm{Gal}(L|K) = \bigcap_{L_1 \le L_2} X_{L_1, L_2},$$

so the inverse limit is closed, hence compact, and Hausdorff as well.

iii) Each $Gal(M|K) \to Gal(L|K)$, $L \in I$, is cts by the definition of the Krull topology.
$\Rightarrow \phi$ is cts.

To prove that ϕ is a homeomorphism, we need to prove that every open set in $Gal(M|K)$ is the preimage of an open set in $\prod_{L \in I} Gal(L|K)$ via ϕ.

It suffices to prove this for the sets of the form $\sigma\, Gal(M|L')$ with $L'|K$ finite ~~[illegible]~~ Galois, since these form a basis for the topology on $Gal(M|K)$.

But if $\pi_{L'} : \prod \mathrm{Gal}(L|K) \longrightarrow \mathrm{Gal}(L'|K)$

is the projection, then

$$\sigma\,\mathrm{Gal}(M|L') = \phi^{-1}(\pi^{-1}(\sigma|_{L'}))$$

and $\pi^{-1}(\sigma|_{L'})$ is open in $\prod \mathrm{Gal}(L|K)$.

It follows that $\mathrm{Gal}(M|K)$ is compact and Hausdorff.

9. (i) Omitted (should hopefully be straightforward to verify)

(ii) $\overline{\mathbb{F}_q} = \bigcup_{n \in \mathbb{Z}_{\geq 1}} \mathbb{F}_{q^n}$ and the

$\mathbb{F}_{q^n}$ are all the finite subext^{n}s.

We have inclusions $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ if and only if $m \mid n$, so the directed system of finite Galois subext^{n}s of $\overline{\mathbb{F}_q} \mid \mathbb{F}_q$ is isomorphic to $(\mathbb{Z}_{\geq 1}, \mid)$

We have an isomorphism

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q) \\ 1 &\longmapsto (x \mapsto x^q) \end{aligned}$$

and if $m \mid n$, the diagram

$$\begin{tikzcd} \mathbb{Z}/n\mathbb{Z} \arrow[r, "\sim"] \arrow[d, "f_{m,n}"] & \mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q) \arrow[d] \\ \mathbb{Z}/m\mathbb{Z} \arrow[r, "\sim"] & \mathrm{Gal}(\mathbb{F}_{q^m} \mid \mathbb{F}_q) \end{tikzcd} \qquad \begin{array}{c} \sigma \\ \downarrow \\ \sigma|_{\mathbb{F}_{q^m}} \end{array}$$

commutes.

It follows that we have an isomorphism

$$\left(\mathbb{Z}/n\mathbb{Z},\ f_{m,n}\right) \longrightarrow \left(\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q),\ \mathrm{res}^{\mathbb{F}_{q^n}}_{\mathbb{F}_{q^m}}\right)$$

restriction

of directed systems, and hence an isomorphism

$$\hat{\mathbb{Z}} \xrightarrow{\sim} \mathrm{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q)$$

upon taking inverse limits, which sends 1 to $x \longmapsto x^q$.

iii) We have a natural injection $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}$, which is not surjective (e.g. since $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ by Chinese Remainder Thm)

$\mathbb{Z} \subseteq \hat{\mathbb{Z}}$ is dense, since its projection to $\mathbb{Z}/n\mathbb{Z}$ is surjective $\forall n$,

$\Rightarrow \mathbb{Z}$ non-closed subgroup.

~~corresponds to the infinite cyclic subgroup of Gal~~

~~$\mathbb{Z}$ / its generated by $x \mapsto x^q$~~

The image of $\mathbb{Z}$ in $\mathrm{Gal}(\overline{\mathbb{F}_q} | \mathbb{F}_q)$ is the cyclic subgroup generated by $x \mapsto x^q \Rightarrow$

$\Rightarrow$ fixed field is

$$\{ \alpha \in \overline{\mathbb{F}_q} \mid \alpha^q = \alpha \} = \mathbb{F}_q,$$

which is equal to the fixed field of $\hat{\mathbb{Z}}$.

10. Work inside K^{sep}. Let $|\cdot|$ be the absolute value on K & its extⁿ to K^{sep}

Since K has a unique unramified extⁿ K_d of degree d $\forall d \geq 1$, we have

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

$$= \sum_{d \mid n} \#\left(\begin{array}{c} \text{totally ramified sep ext}^n\text{s} \\ \text{of } K_d \text{ of degree } d/n \end{array} \right).$$

so it suffices to consider totally ramified ext^{n}s.

Assume that char $k \nmid n$.

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

$$E_n \cong \pi_K \mathcal{O}_K^{n-1} \times (\pi_K \mathcal{O}_K \setminus \pi_K^2 \mathcal{O}_K)$$

$$T^n + a_{n-1} T^{n-1} + \dots + a_0 \longmapsto (a_{n-1}, \dots, a_0)$$

The RHS is naturally a compact metric space under the metric

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

~~$|\;|$ the ext^n to K of the~~

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

Given $f \in E_n$ & a root α of f, continuity of roots (Q8, Sheet 2) shows that $\exists$ open $U(f,\alpha) \subseteq E_n$ containing f s.t $\forall g \in U(f,\alpha)$, there is a root β of g s.t

$$|\alpha - \beta| < |\alpha - \alpha'| \quad \forall \text{ roots } \alpha' \neq \alpha \text{ of } f.$$

Set $$U(f) = \bigcap_{\substack{\alpha \text{ root} \\ \text{of } f}} U(f,\alpha),$$ then

if $g \in U(f)$ $\exists$ bijection the roots of g & the roots of f matching up the closest roots, and by Krasner's Lemma (Q9, Sheet 2) the totally ramified ext^{n}s of K generated by the roots of g match up with those generated by the roots of f.

(Here we use char $k \nmid n$ to ensure that

f is seperable)

Since $E_n = \bigcup_{f \in E_n} U(f)$ & E_n is

compact, $\exists$ finite subcover

$U(f_1), \ldots, U(f_r) \implies \exists$ only finitely

many totally ramified ext^{n}s of deg n

generated by roots of Eisenstein polynomials,

but any totally ramified ext^n is generated

by a root of an Eisenstein poly.

When char $K = p$, $\exists$ infinitely many

separable ext^{n}s of degree p

To see this, we use Artin-Schreier theory:

<u>Thm</u> Let K be a field of characteristic p

then $L|K$ Galois of deg p $\iff$

$\iff$ L is the splitting field of an irreducible polynomial of the form

$$f_\alpha(T) = T^p - T + \alpha \quad \text{for } \alpha \in K.$$

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

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

and $T^p - T + \alpha$ & $T^p - T + \beta$ 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~~ char p.

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

<u>Pf</u>: $K \cong \mathbb{F}_q((t))$. If $y = x^p - x$ and $v_K(y) < 0$, then $v_K(x) < 0$

and hence $v_K(y) = v_K(x^p - x) =$

$= p\, v_K(x)$.

Thus, the elements t^{-n}, $n \in \mathbb{Z}_{\geq 1}$,

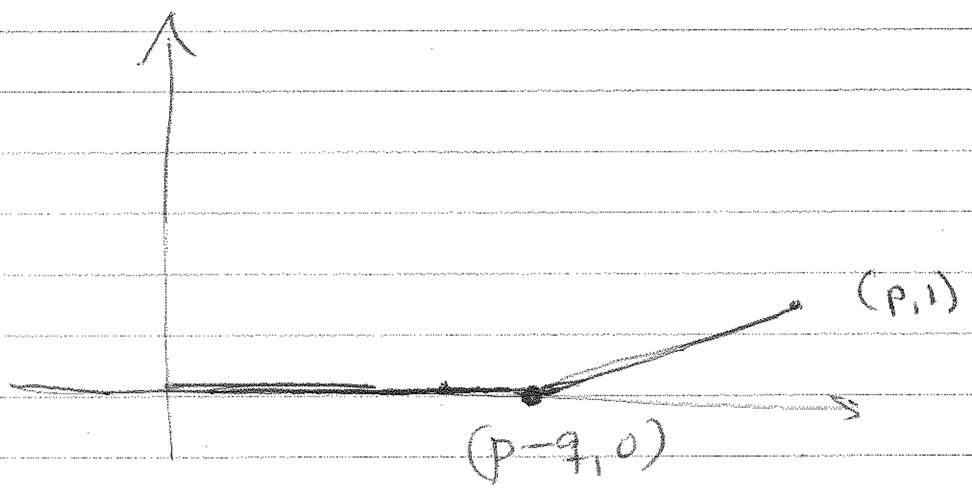
$p \nmid n$ are not in $\{y \in K \mid \exists x : x^p - x = y\}$.

It follows that there are infinitely many

distinct Galois ext^{n}s of degree p / K.

11. (i) E_p is Eisenstein for p.

(ii) The Newton polygon for q is



~~So Gal($E_p/\mathbb{Q}_q$) cont~~

~~so there are q roots of E_p with~~

so E_p has a factor g over $\mathbb{Q}_q$

which is Eisenstein of degree q, so q divides

the order of the splitting field of $E_p / \mathbb{Q}_q$

$$\Rightarrow \quad q \mid \# \mathrm{Gal}(E_p / \mathbb{Q}_q) \mid \# \mathrm{Gal}(E_p/\mathbb{Q}_q)$$

So $\mathrm{Gal}(E_p/\mathbb{Q}_q)$ contains an element of

order q, but since $q > p/2$ and q is prime the

only elements of order q are q-cycles.

(iii) We have

$$|D_n| = \left| \prod_{i \neq j} (\alpha_i - \alpha_j) \right| = \left| \prod_i \prod_{j \neq i} (\alpha_i - \alpha_j) \right| =$$

$$= \left| \prod_i n! f_n'(\alpha_i) \right| = \left| \prod_i n! \Big(\underbrace{f_n(\alpha_i)}_{=0} - \alpha_i^n / n! \Big) \right| =$$

$$= \left| \prod_i \alpha_i^n \right| = \underbrace{|\alpha_1 \ldots \alpha_n|}_{=n!}{}^n = (n!)^n.$$

So $v_p(|D_p|) = p$ which is odd,

so the discriminant of E_p is not a square

$\Rightarrow$ $Gal(E_p|\mathbb{Q}) \not\subseteq A_p$

By part (ii) $Gal(E_p|\mathbb{Q}) \supseteq A_p$, so

must have $Gal(E_p|\mathbb{Q}) = S_p$.

iv) Let G be a finite group, set

$n = \# G$ and let $p \geq \max\{n, 8\}$

be a prime.

Then $G \leq S_n$ (e.g. by ~~action~~ acting

on itself by translation) and $S_n \leq S_p$,

so if L = splitting field of $E_p / \mathbb{Q}$,

then $G \leq Gal(L|\mathbb{Q}) \Rightarrow \exists$ subfield

$K \subseteq L$ s.t. $Gal(L|K) = G$.