Local Fields Example Sheet 4

1. $(J, \leq)$ 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 $i \leq j_3$.

Therefore $\exists j_3 : j_1, j_2 \leq j_3$, and hence $(J, \leq)$ is a directed system.

Second part:

There is a natural ~~map~~ continuous homomorphism

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

$$(g_i)_{i \in I} \longmapsto (g_i)_{i \in J}$$

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

Call this map ϕ.

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

Assume that ~~...~~ $x_j = 1$ if $j \in J$.

~~Choose~~ Pick $i \in I$, and choose $j \in J$ with

$i \leq j$. Then $x_i = f_{ij}(x_j) = 1$, so

$x_i = 1 \ \forall i \in I$, so ϕ is 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 such that

$i \leq j$.

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

$\exists\, j_3 \in J$ with $j_1, j_2 \leq j_3$, and

$f_{ij_2}(x_{j_2}) = f_{ij_2}(f_{j_2j_3}(x_{j_3})) =$

$= f_{ij_3}(x_{j_3}) = f_{ij_1}(f_{j_1j_3}(x_{j_3})) = f_{ij_1}(x_{j_1})$.

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

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

$$x_{i_1} = f_{i_1 j}(x_j) = f_{i_1 i_2}(f_{i_2 j}(x_j)) = $$
$$= f_{i_1 i_2}(x_{i_2}).$$

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

ϕ is surjective.

<u>ϕ is a homeomorphism</u>:

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

By construction of the inverse limit topology, U is the union of sets of the form $\pi_i^{-1}(V)$, where $\pi_i : \varprojlim_{i\in I} G_i \longrightarrow G_i$ is the projection and $V \subseteq G_i$ is open, so without loss of generality we may take $\mathcal{U}$ to be of this form. Pick $j \in J$ with $i \leq j$. We have a commutative diagram

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

and so $\mathcal{U} = \pi_i^{-1}(V) = \phi^{-1}(\pi_j^{-1}(f_{ij}^{-1}(V)))$

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

2. (i)

ϕ is injective

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

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

then $\sigma = id$.

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

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

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

$(\sigma|_{L_2})|_{L_1} = \sigma|_{L_1}$. Thus $\mathrm{Im}\,\phi \subseteq \varprojlim_{L \in I} Gal(L|K)$

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

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 σ is a function $M \to M$.

It is clearly a homomorphism, and satisfies $\sigma|_L = \sigma_L$. To show that it is in $Gal(M|K)$ we need to show that $\sigma(M) = M$. But

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

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

(ii) ~~Each~~ Each $Gal(L|K)$ is finite and discrete, hence compact and Hausdorff.

It follows that $\prod_{L \in I} Gal(L|K)$ is compact (by Tychonoff's thm) and Hausdorff (easy to check).

The subset $\varprojlim_{L \in I} Gal(L|K) \subseteq \prod_{L \in I} Gal(L|K)$ is closed (by the argument in Q12,

~~E~~Example Sheet 1), so it is also compact and Hausdorff.

iii) Each $Gal(M|K) \longrightarrow Gal(L|K)$ is continuous (for $L \in I$), since if $\bar{\sigma} \in Gal(L|K)$ is a point with lift $\sigma \in Gal(M|K)$, the preimage of $\bar{\sigma}$ is $\sigma Gal(M|L)$, which is open by definition.

It follows that ~~...~~ ϕ is continuous. To prove that it is a homeomorphism onto its image, 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 sets of the form $\sigma \, \mathrm{Gal}(M|L')$ with $L'|K$ finite

(not necessarily Galois) since these were defined

to be a basis for the Krull topology.

Let L be the Galois closure of L' in M.

Then $\sigma \, \mathrm{Gal}(M|L')$ is the preimage of

$\sigma|_L \, \mathrm{Gal}(L|L') \subseteq \mathrm{Gal}(L|K)$ under the

restriction map $\mathrm{Gal}(M|K) \to \mathrm{Gal}(L|K)$,

so $\sigma \, \mathrm{Gal}(M|L')$ is the preimage of

$$\left(\prod_{\substack{L'' \in I \\ L'' \neq L}} \mathrm{Gal}(L''|K) \right) \times \sigma|_L \, \mathrm{Gal}(L|L') \subseteq$$

$$\subseteq \prod_{L'' \in I} \mathrm{Gal}(L''|K)$$ under ϕ, and

this set is open.

3. We need to prove that

$$L = M^{Gal(M|L)} \quad \text{and}$$

$$H = Gal(M|M^H)$$

for all subext^{n}s $L|K$ and all closed subgroups H.

<u>$L = M^{Gal(M|L)}$</u>

First, note that $L \subseteq M^{Gal(M|L)}$ directly from the definitions. We need to prove the converse.

Let $x \in M^{Gal(M|L)}$ and let L' be the Galois closure of $K(x)$ in M. Then the image of $Gal(M|L)$ in $Gal(L'|K)$ is $Gal(L'|L \cap L')$ (by field theory; any automorphism of L' fixing $L \cap L'$ may be ~~t~~extended to an automorphism of M fixing L).

It follows that $x \in (L')^{Gal(L'|L\cap L')}$.

By usual finite Galois theory $(L')^{Gal(L'|L\cap L')} =$

$= L \cap L'$, so $x \in L$ as desired.

$H = Gal(M|M^{\#})$.

We have $H \subseteq Gal(M|M^{\#})$ directly from the definitions. Since H is closed it suffices to show that H is dense in $Gal(M|M^{\#})$, which amounts to proving that H has the same image as $Gal(M/M^{\#})$ in $Gal(L/K)$ for every finite Galois subext^n L/K of M/K.

From the definitions, ~~then~~,

$$Im\left(Gal(M/M^{\#}) \longrightarrow Gal(L/K)\right) =$$

$= Gal(L/L^H)$

(using $Gal(M/K) \twoheadrightarrow Gal(L/K)$).

Also, $L^H = L^{Im(H \to Gal(L/K))}$ by definitions,

$\Rightarrow Im(H \to Gal(L/K)) = Gal(L/L^H)$

by usual finite Galois theory. This finishes the proof.

4. (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 $m | n$, so the directed system of finite Galois subext^{n}s of $\overline{\mathbb{F}_q} / \mathbb{F}_q$ is isomorphic to $(\mathbb{Z}_{\geq 1}, |)$.

We have an isomorphism

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

and if m/n, the diagram

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \\ \downarrow f_{m,n} & & \downarrow \quad \begin{array}{c}\sigma \\ \downarrow \\ \sigma|_{\mathbb{F}_{q^m}}\end{array} \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \end{array}$$

commutes. It follows that we have an isomorphism

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

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 $x \mapsto x^q$.

iii) $\hat{\mathbb{Z}}$ is a compact Hausdorff group.

The natural map $\mathbb{Z} \to \hat{\mathbb{Z}}$ is injective, so $\hat{\mathbb{Z}}$ is infinite. It follows that $\hat{\mathbb{Z}}$ has no isolated points: if it did, every point would be isolated (since it is a topological group) so it would be discrete. But a compact and infinite space can't be discrete.

By the Baire category theorem $\hat{\mathbb{Z}}$ is therefore uncountable, so we must have $\mathbb{Z} \neq \hat{\mathbb{Z}}$.

If $\mathbb{Z} \subseteq \hat{\mathbb{Z}}$ is closed, it would be compact and Hausdorff and infinite, so by the same argument it would have to be uncountable, which is a contradiction.

Therefore $\mathbb{Z}$ is a non-closed subgroup.

$\mathbb{Z}$ is generated by 1, so its image in $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is generated by $x \mapsto x^q$

$\Rightarrow$ the fixed field is $\{x \in \overline{\mathbb{F}_q} \mid x^q = x\} = \mathbb{F}_q$.

5. Since $K|\mathbb{Q}$ is Galois, it is the splitting field of some polynomial $f \in \mathbb{Q}[x]$. Now consider the subextension of $K_p|\mathbb{Q}_p$ generated by the roots of f. Since it contains K, it is dense. On the other

hand it is complete, hence closed, so it has to be all of $K_\mathfrak{p}$. It follows that $K_\mathfrak{p} | \mathbb{Q}_p$ is Galois.

<u>Next part</u>:

$$\mathrm{Gal}(K_\mathfrak{p} | \mathbb{Q}_p) \longrightarrow \mathrm{Gal}(K | \mathbb{Q})$$
$$\sigma \longmapsto \sigma|_K$$

If $\sigma|_K = \mathrm{id}$, then $\sigma = \mathrm{id}$ since $K \subseteq K_\mathfrak{p}$ is dense and σ is continuous.

If $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ is in the image, then $\{x \in \mathcal{O}_K \mid v_\mathfrak{p}(x) > 0\}$ is preserved by σ, but this set is $\mathfrak{p}$ by construction of $v_\mathfrak{p}$.

Conversely, assume that $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ is such that $\sigma(\mathfrak{p}) = \mathfrak{p}$. By the construction of $v_\mathfrak{p}$, we have $v_\mathfrak{p}(\sigma(x)) = v_\mathfrak{p}(x)$ $\forall x \in K$. It follows that σ is an isometry of K for the (equivalence class of) metric(s) given by $v_{\mathfrak{p}}$, and hence that it extends to an element of $\mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$.

6. (i) Write $g(X) = a_1 X + a_2 X^2 + \ldots$, $a = a_1$.

We will construct polynomials

$$h_n(X) = b_1 X + \ldots + b_n X^n$$

inductively such that

$$g(h_n(X)) \equiv X \mod X^{n+1};$$

the desired power series $h(X)$ is then

$$h(X) = b_1 X + b_2 X + \ldots$$

$\underline{n=1}$: Set $h_1(X) = b_1 X$ with $b_1 = a^{-1}$.

Then $g(h_1(X)) \equiv a(a^{-1}X) \equiv X \mod X^2$.

Induction step, $n > 1$

Assume that we have constructed $h_{n-1}(X)$ such that $g(h_{n-1}(X)) \equiv X \mod X^n$, or in other words $g(h_{n-1}(X)) \equiv X + c_n X^n \mod X^{n+1}$ for some $c_n \in R$.

Consider $h_n(X) = h_{n-1}(X) + b_n X^n$.

We have

$$h_n(X)^k = (h_{n-1}(X) + b_n X^n)^k \equiv$$

$$\equiv \left.\begin{cases} h_{n-1}(X)^k & \text{if } k>1 \\ h_{n-1}(X) + b_n X^n & \text{if } k=1 \end{cases}\right\} \mod X^{n+1}.$$

so

$$g(h_n(X)) = \sum_{k \geq 1} a_k h_n(X)^k \equiv$$

$$= \sum_{k\geq 1} a_k \left(h_{n-1}(X) + b_n X^n\right)^k \equiv$$

$$\equiv \left(\sum_{k\geq 1} a_k h_{n-1}(X)^k\right) + a_1 b_n X^n \equiv$$

$$\equiv X + c_n X^n + a_1 b_n X^n \mod X^{n+1}$$

Now set $b_n = -a_1^{-1} c_n$.

ii) Put $f(X) = F(X,0)$. We have

$$f(f(X)) = F(F(X,0),0) = F(X, F(0,0)) =$$

$$= F(X,0) = f(X)$$

using associativity for the second equality and $F(X,Y) \equiv X+Y \mod (X,Y)^2$ for the third.

By part i), $\exists h(X)$ such that $f(h(X)) = X$.

Thus $f(f(h(X))) = f(h(X)) = X$ as desired.

$f(X) =$

iii) By part ii),

$$F(X,Y) = X+Y+\sum_{m,n\geq 1} a_{mn} X^m Y^n$$

for some $a_{mn} \in R$. As in part i) we construct $i_k(X)$, $k=1,2,\dots$ inductively such that $i_k(X) = b_1 X + \dots + b_k X^k$, $b_1 = -1$, and $F(X, i_k(X)) \equiv 0 \mod X^{k+1}$; the desired $i(X)$ is then $b_1 X + b_2 X^2 + \dots$.

$\underline{k=1}$: $i_1(X) = -X$,

$$F(X,-X) = X+(-X)+\sum_{m,n\geq 1} a_{mn} X^m (-X)^n \equiv$$

$$\equiv 0 \mod X^2.$$

$\underline{k>1}$: $i_k(X) = i_{k-1}(X) + b_k X^k$. We have

$$X^m (i_{k-1}(X) + b_k X^k)^n \equiv X^m i_{k-1}(X)^n$$

$$\mod X^{k+1}$$

If $m \geq 1$, so

$$F(X, i_k(X)) \equiv X + (i_{k-1}(X) + b_k X^k) +$$

$$+ \sum_{m,n\geq 1} a_{mn} X^m i_{k-1}(X)^n \equiv$$

$$\equiv F(X, i_{k-1}(X)) + b_k X^k \mod X^{k+1}.$$

Since $F(X, i_{k-1}(X)) \equiv 0 \mod X^k$,

$F(X, i_{k-1}(X)) \equiv c_k X^k \mod X^{k+1}$ for some $c_k \in R$.

Now set $b_k = -c_k$.

$\underline{F = \widehat{\mathbb{G}}_m}$

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

If $(1+X)(1+i(X)) - 1 = 0$, then

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

7. We have $N(LM|K) \subseteq N(L|K)$, $N(M|K)$,

$N((L\cap M)|K)$,

so it suffices to show that

$$\frac{N(L|K)}{N(LM|K)} \cap \frac{N(M|K)}{N(LM|K)} = 1 \quad \text{and}$$

$$\frac{N((L\cap M)|K)}{N(LM|K)} = \frac{N(L|K)}{N(LM|K)} \cdot \frac{N(M|K)}{N(LM|K)}$$

The diagram

$$\begin{tikzcd} K^\times/N(LM|K) \arrow[r, "\mathrm{Art}_K", "\sim"'] \arrow[d, "\substack{\text{natural}\\ \text{quotient}\\ \text{map}}"'] & \mathrm{Gal}(LM|K) \arrow[d, "\sigma \mapsto \sigma|_L"] \\ K^\times/N(L|K) \arrow[r, "\mathrm{Art}_K", "\sim"'] & \mathrm{Gal}(L|K) \end{tikzcd}$$

commutes, so Art_K identifies the group

$N(L|K)/N(LM|K)$ with $\mathrm{Gal}(LM/L)$,

and similarly replacing L by M ~~or~~ or $L\cap M$.

The desired ~~equalities~~ ~~as~~ identities are thus translated into

$$\mathrm{Gal}(LM/L) \cap \mathrm{Gal}(LM/M) = 1 \quad \text{and}$$

$$\mathrm{Gal}(LM/L \cap M) = \mathrm{Gal}(LM/L)\,\mathrm{Gal}(LM/M),$$

both of which hold by Galois theory.

8. Choose a uniformizer π of K and write

$$K^\times \cong \langle \pi \rangle \times \mathcal{O}_K^\times \quad \text{(algebraically and topologically)}.$$

If $H \leq K^\times$ is open of finite index, then

$H \supseteq \langle \pi^m \rangle \times U_K^{(n)}$ for some $m, n \in \mathbb{Z}_{\geq 1}$.

To see this, first note that $H \supseteq U_K^{(n)}$ for some n since H is open. Then, since

$K^\times/H$ is finite, the map $\langle\pi\rangle \longrightarrow K^\times/H$

must have a nontrivial kernel.

By a theorem stated in lectures, the field $L_{\pi,n}$ of π^n-division points of a Lubin-Tate formal $\mathcal{O}_K$-module F has

$$N(L_{\pi,n}|K) = \langle\pi\rangle \times U_K^{(n)}.$$

It was also stated in lectures that

$N(K_m|K) = \langle\pi^m\rangle \times \mathcal{O}_K^\times$, where $K_m|K$ is the unique unramified ext^n of degree m.

By Q7 on this sheet,

$$N(K_m L_{\pi,n}|K) = N(K_m|K) \cap N(L_{\pi,n}|K) =$$
$$= \langle\pi^m\rangle \times U_K^{(n)},$$

so $\quad H \supseteq N(K_m L_{\pi,n}|K)$.

We have

$$K^\times / N(K_m L_{\pi,n}|K) \xrightarrow[\mathrm{Art}_K]{\sim} \mathrm{Gal}(K_m L_{\pi,n}|K)$$

so by Galois theory $K^\times / H \xrightarrow[\mathrm{Art}_K]{\sim} \mathrm{Gal}(L|K)$

for some subextension $L|K$ of $K_m L_{\pi,n}|K$.

But we know from the main thm of local class field theory that the kernel of $K^\times \longrightarrow \mathrm{Gal}(L|K)$ is $N(L|K)$, so $H = N(L|K)$.

<u>Last part</u>:

By Questions 5 and 12 (essentially), we have $K^\times \cong \mathbb{Z} \times \mathbb{Z}/(q-1) \times \mathbb{Z}/p^a \times \mathbb{Z}_p^d$ algebraically and topologically, where $d = [K:\mathbb{Q}]$.

If $H \subseteq K^\times$ has finite index $= N$ say, then $H \supseteq N\mathbb{Z} \times N(\mathbb{Z}/(q-1) \times \mathbb{Z}/p^a) \times N\mathbb{Z}_p^d$, which is open (see Q8, Ex Sheet 1), so H is open.

9. <u>A rough sketch</u>: (Q9) $p > 2$:

We have $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}/_{p-1} \times \mathbb{Z}_p$,

so $(\mathbb{Q}_p^\times)^2 \cong 2\mathbb{Z} \times \mathbb{Z}/\left(\frac{p-1}{2}\right) \times \mathbb{Z}_p$

and $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong (\mathbb{Z}/2)^2$; this has to be the only subgroup of $\mathbb{Q}_p^\times$ with this property.

(as any other such subgroup would have to be contained in $(\mathbb{Q}_p^\times)^2$).

Local class field theory gives us the corresponding unique abelian ext^n K / the upper ramification groups are given under the isomorphism

$$\mathrm{Gal}(K|\mathbb{Q}_p) \xleftarrow[\mathrm{Art}_{\mathbb{Q}_p}]{\sim} \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$$

by $$G^s(K|\mathbb{Q}_p) \xleftarrow[\mathrm{Art}_{\mathbb{Q}_p}]{\sim} \frac{(\mathbb{Q}_p^\times)^2(1+p^s\mathbb{Z}_p)}{(\mathbb{Q}_p^\times)^2}$$

$(s \in \mathbb{Z}_{\geq 1})$

and $(\mathbb{Q}_p^\times)^2(1+p^s\mathbb{Z}_p) = (\mathbb{Q}_p^\times)^2$, and

$$G^0(K|\mathbb{Q}_p) \xleftarrow[\mathrm{Art}_{\mathbb{Q}_p}]{\sim} \frac{(\mathbb{Q}_p^\times)^2\mathbb{Z}_p^\times}{(\mathbb{Q}_p^\times)^2} \simeq \mathbb{Z}/2 .$$

<u>$p=2$:</u> $(\mathbb{Q}_2^\times)^2 \simeq \mathbb{Z} \times \mathbb{Z}/2 \times \mathbb{Z}_2$, so

$(\mathbb{Q}_2^\times)^2 \simeq 2\mathbb{Z} \times 1 \times 2\mathbb{Z}_2$ and

$\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2 \simeq (\mathbb{Z}/2)^3$;

local class field theory gives us a unique ext^n $K|\mathbb{Q}_2$ with $\mathrm{Gal}(K|\mathbb{Q}_2) \cong (\mathbb{Z}/2)^3$ (the one with $N(K|\mathbb{Q}_2) = (\mathbb{Q}_2^\times)^2$).

We have $\mathrm{Gal}(K|\mathbb{Q}_2) \xleftarrow[\mathrm{Art}_{\mathbb{Q}_2}]{\sim} \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ and ($s \in \mathbb{Z}_{\geq 0}$)

$$G^s(K|\mathbb{Q}_2) \underset{\mathrm{Art}_{\mathbb{Q}_2}}{\cong} \begin{cases} \dfrac{(\mathbb{Q}_2^\times)^2\mathbb{Z}_2^\times}{(\mathbb{Q}_2^\times)^2}, & s = 0,1 \\ \dfrac{(\mathbb{Q}_2^\times)^2(1+4\mathbb{Z}_2)}{(\mathbb{Q}_2^\times)^2}, & s = 2 \\ (\mathbb{Q}_2^\times)^2/(\mathbb{Q}_2^\times)^2, & s \geq 3. \end{cases}$$

Q13: First char $k = 0$.

By ~~induction~~ Galois theory and the fact that any finite ext^n of degree n is contained in a Galois ext^n of degree $\leq n!$, it suffices to prove that there are only finitely many Galois ext^n of bounded degree.

By induction and the fact that Galois groups of local fields are solvable, it suffices to prove that K only has finitely many cyclic (or abelian) ext^ns of degree n.

This follows from local class field theory:

If L/K is cyclic of ~~degree~~, n, then $N(L/K) \supseteq (K^\times)^n$. Since

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

by Q12, Ex Sheet 3, we see that $(K^\times)^n$ has finite index in $K^\times$, so there can only be finitely many such L.

~~(2)~~ char $K = p$:

First we prove that if $p \nmid n$ then there are only finitely many extensions of degree n. Let $L|K$ be such an ext^n. Then $L|K$ is tamely ramified (Q3, Ex Sheet 3) so by Q4, Ex Sheet 3, and its proof, $L = T(\sqrt[m]{a})$ for some $a \in T$ (T/K the maximal unramified subext^n of L/K) and $m | n$. (and hence $p \nmid m$).

By the proof ~~the~~ of Q3, Ex Sheet 3, the Galois closure $L' = T(\mu_m, \sqrt[m]{a})$ of $L|K$ ~~has~~ is tamely ramified.

Using the same reduction as in the proof of Q13 on Ex Sheet 3, ~~we may~~ if then suffices to prove that there are only finitely many totally ramified Galois ext^n's of bounded degree coprime to p.

As in the char 0 case we may then reduce to showing that there are only finitely many abelian extensions of degree n coprime to p.

Then

$$K^\times \cong \mathbb{Z} \times \mathbb{Z}/_{q-1} \times \mathbb{Z}_p^{\mathbb{Z}_{\geq 0}}$$

by Q12, Ex Sheet 3, so

$$(K^\times)^n \cong n\mathbb{Z} \times n(\mathbb{Z}/_{q-1}) \times \mathbb{Z}_p^{\mathbb{Z}_{\geq 0}}$$

and so has finite index in $K^\times$ (and is open)

We now finish the proof as in the char 0 case.

The (algebraic and topological) isomorphism

$$K^\times \cong \mathbb{Z} \times \mathbb{Z}/_{q-1} \times \mathbb{Z}_p^{\mathbb{Z}_{\geq 0}}$$

also shows, together with local class field theory, that K has infinitely many Galois ext^{n}s of degree p:

Writing
$$K^\times \cong \mathbb{Z} \times \mathbb{Z}/_{q-1} \times \prod_{i \in \mathbb{Z}_{\geq 0}} \mathbb{Z}_p \quad ,$$

the subgroups
$$G_j \cong \mathbb{Z} \times \mathbb{Z}/_{q-1} \times \Big(\prod_{\substack{i \in \mathbb{Z}_{\geq 0} \\ i \neq j}} \mathbb{Z}_p \times p\mathbb{Z}_p \Big)$$

for $j \in \mathbb{Z}_{\geq 0}$ are distinct, open and of index p.

10. i) $X^{p-1} - \zeta p$ is Eisenstein of degree $p-1$, so $K_\zeta | \mathbb{Q}_p$ is totally ramified of degree $p-1$.

If α is a root of $X^{p-1} - \zeta p$ in K_ζ, then the other roots are $\alpha\zeta^i$, $i = 0, \dots, p-2$, which are also in K_ζ, so $K_\zeta | \mathbb{Q}_p$ is Galois.

ii) By the proof of Q4, Ex Sheet 3,

$$K = \mathbb{Q}_p\left(\sqrt[p-1]{a}\right) \text{ for some } a \in \mathbb{Q}_p^\times,$$

so by the argument in i) $K | \mathbb{Q}_p$ is Galois.

In fact, the Galois group is $\cong \mathbb{Z}/p-1$.

This follows from Kummer theory: If ~~β is a root of~~ $\beta = \sqrt[p-1]{a}$ (i.e a choice of $(p-1)$th root of a), then

$$\mathrm{Gal}(K|\mathbb{Q}_p) \xrightarrow{\sim} \mu_{p-1}$$
$$\bar{\sigma} \longmapsto \frac{\sigma\beta}{\beta}$$

(see the proof of Q3, Ex Sheet 3).

Thus $K|\mathbb{Q}_p$ is abelian. We have

$$N(K|\mathbb{Q}_p) = N_{K|\mathbb{Q}_p}(\pi_K) \cdot N_{K|\mathbb{Q}_p}(\mathcal{O}_K^\times)$$

Since $K|\mathbb{Q}_p$ is totally ramified, $(\mathbb{Z}_p^\times : N_{K|\mathbb{Q}_p}(\mathcal{O}_K^\times)) = p-1$, so we must have $N_{K|\mathbb{Q}_p}(\mathcal{O}_K^\times) = 1 + p\mathbb{Z}_p$.

$N_{K|\mathbb{Q}_p}(\pi_K)$ is a uniformizer in $\mathbb{Q}_p$.

We conclude that $N_{K|\mathbb{Q}_p}(\pi_K) \bmod (1+p\mathbb{Z}_p)$ is independent of the choice of π_K, and determines $N(K|\mathbb{Q}_p)$, and hence $K|\mathbb{Q}_p$, uniquely.

Therefore $\dfrac{N_{K|\mathbb{Q}_p}(\pi_K)}{p} \in \mathbb{Z}_p^\times / 1+p\mathbb{Z}_p$ determines

$K|\mathbb{Q}_p$ uniquely.

For K_ζ, we may take π_{K_ζ} to be a root of $X^{p-1} - \zeta p$. Then $N_{K_\zeta|\mathbb{Q}_p}(\pi_{K_\zeta}) = -\zeta p$,

so $\dfrac{N_{K_\zeta|\mathbb{Q}_p}(\pi_{K_\zeta})}{p} = -\zeta$.

~~As ζ ranges over~~ the elements $(-\zeta)_{\zeta \in \mu_{p-1}}$ are a set of coset representatives of $\mathbb{Z}_p^\times / 1 + p\mathbb{Z}_p$, so the K_ζ are distinct, and any totally ramified $K|\mathbb{Q}_p$ of degree $p-1$ has to equal K_ζ for some $\zeta \in \mu_{p-1}$.

iii) $N(\mathbb{Q}_p(\zeta_p)|\mathbb{Q}_p) = \langle p \rangle \times (1 + p\mathbb{Z}_p)$,

so $\mathbb{Q}_p(\zeta_p) = K_{-1}$, by the calculation in part ii).

11. Suppose that $L \subseteq L_{n,\pi} M$, and suppose that $[M:K] = m$. As in the solution of Q8 on this sheet,

$$N(L_{n,\pi} M | K) = \langle \pi^m \rangle \times U_K^{(n)}, \text{ so}$$

so $N(L|K) \supseteq N(L_{n,\pi} M | K) \supseteq U_K^{(n)}$.

Conversely, assume that $N(L|K) \supseteq U_K^{(n)}$. ~~Since~~ As in the solution of Q8, $\exists m \in \mathbb{Z}_{\geq 1}$ s.t $\pi^m \in N(L|K) \Rightarrow \langle \pi^m \rangle \times U_K^{(n)}$, so if $K_m | K$ is the unramified ext^n of degree m, then $N(K_m L_{n,\pi} | K) \subseteq N(L|K)$ and hence $L \subseteq K_m L_{n,\pi}$.

12. We have $N(L_{n,\pi_i}|K) = \langle \pi_i \rangle \times U_K^{(n)}$,

so $L_{n,\pi_1} = L_{n,\pi_2} \iff \pi_1 \in \langle \pi_2 \rangle U_K^{(n)} \iff$

$\iff \pi_1 = \pi_2 u$ for some $u \in U_K^{(n)}$.

Next, assume $\pi_1 \neq \pi_2$. Write $\pi_1 = \pi_2 u$.

We have $u \neq 1$, so choose n s.t $u \notin U_K^{(n)}$.

If $L_{\pi_1} = L_{\pi_2}$, then $L_{n,\pi_2} \subseteq L_{\pi_1}$, so

$\exists m : L_{n,\pi_2} \subseteq L_{m,\pi_1} \Longrightarrow$

$\Longrightarrow \langle \pi_1 \rangle \times U_K^{(m)} \subseteq \langle \pi_2 \rangle \times U_K^{(n)}$

$\Longrightarrow \pi_1 \in \langle \pi_2 \rangle \times U_K^{(n)}$ $\#$.

Thus $L_{\pi_1} \neq L_{\pi_2}$.

<u>Last part:</u> Write $\pi_1 = \pi_2 u$ again, $u \in \mathcal{O}_K^\times$.

Then $\exists m \in \mathbb{Z}_{\geq 1} : u^m \in U_K^{(n)}$ (since $(\mathcal{O}_K^\times : U_K^{(n)})$ is finite), so $\pi_1^m \equiv \pi_2^m \mod U_K^{(n)}$, and

$$\langle \pi_1^m \rangle \times U_K^{(n)} = \langle \pi_2^m \rangle \times U_K^{(n)}.$$

It follows that $L_{n,\pi_1} M = L_{n,\pi_2} M$, where

M is the unramified ext^n of K of degree m.

13. i)

<u>Case 1:</u> $a \in (\mathbb{Q}_p^\times)^2$. $(\Leftrightarrow K = \mathbb{Q}_p)$.

In this case $b \in N_{K|\mathbb{Q}_p}(K^\times)$ $\forall b \in \mathbb{Q}_p$.

If $a = \alpha^2$, $\alpha \in \mathbb{Q}_p^\times$, then

$$a\left(\frac{1}{\alpha}\right)^2 + b.0^2 = 1, \quad \forall b \in \mathbb{Q}_p,$$

so $(a,b)_p = 1$ $\forall b \in \mathbb{Q}_p$.

<u>Case 2:</u> $a \notin (\mathbb{Q}_p^\times)^2$.

Assume that $(a,b)_p = 1$, i.e $\exists x, y \in \mathbb{Q}_p$ s.t

$ax^2+by^2=1$.

If $y \neq 0$, we have $b = \left(\frac{1}{y}\right)^2 - a\left(\frac{x}{y}\right)^2 =$
$= N_{K|\mathbb{Q}_p}\left(\frac{1}{y} + \frac{x}{y}\sqrt{a}\right)$, so $b \in N_{K|\mathbb{Q}_p}(K)$.

If $y = 0$, we have $a \in (\mathbb{Q}_p^\times)^2$, a contradiction.

For the converse, assume that $b = N(x+y\sqrt{a}) =$
$= x^2 - ay^2$
for some $x, y \in \mathbb{Q}_p$.

If $x \neq 0$, $a\left(\frac{y}{x}\right)^2 + b\left(\frac{1}{x}\right)^2 = 1$, so
$(a,b)_p = 1$.

If $x = 0$, we have $b = -ay^2$. We want to find $u, v \in \mathbb{Q}_p$ s.t $au^2 + bv^2 = 1 \iff$
$\iff a(u^2 - y^2v^2) = 1 \iff a(u+vy)(u-vy) = 1$,
which is solved e.g. by $u = \frac{1+a^{-1}}{2}$,
$v = \frac{a^{-1}-1}{2y}$

Second part:

If $a \in (\mathbb{Q}_p^\times)^2$, $(a,b)_p = (a,-ab)_p = 1$

for all $b \in \mathbb{Q}_p^\times$.

If $a \notin (\mathbb{Q}_p^\times)^2$, set $K = \mathbb{Q}_p(\sqrt{a})$.

$$(a,b)_p = 1 \iff b \in N_{K|\mathbb{Q}_p}(K^\times) \iff$$

$$\iff -ab \in N_{K|\mathbb{Q}_p}(K^\times)$$

$$(\text{since } -a = N_{K|\mathbb{Q}_p}(\sqrt{a}))$$

$$\iff (a,-ab)_p = 1$$

so $(a,b)_p = (a,-ab)_p$.

<u>Bilinearity</u>

We want to prove that $(a,b)_p(a,c)_p = (a,bc)_p$;

this suffices since symmetry of $(\,,)_p$ is

clear from the definition.

If $a \in (\mathbb{Q}_p^\times)^2$ then both sides are always $=1$.

Assume that $a \notin (\mathbb{Q}_p^\times)^2$. We have $(K = \mathbb{Q}_p(\sqrt{a}))$

$$(a, bc)_p = 1 \iff bc \in N_{K|\mathbb{Q}_p}(K^\times) \iff$$

$$\iff b \in N_{K|\mathbb{Q}_p}(K^\times) \text{ and } c \in N_{K|\mathbb{Q}_p}(K^\times) \ \underline{\underline{\text{or}}}$$

$$c, b \notin N_{K|\mathbb{Q}_p}(K^\times), \text{ since}$$

$$\mathbb{Q}_p^\times / N_{K|\mathbb{Q}_p}(K^\times) \cong \mathbb{Z}/2$$

$$\iff (a,b)_p = (a,c)_p = 1 \ \underline{\underline{\text{or}}}$$

$$(a,b)_p = (a,c)_p = -1$$

$$\iff (a,b)_p (a,c)_p = 1,$$

so $(a, bc)_p = (a,b)_p (a,c)_p$ as desired.

(ii) $\underline{p > 2}$:

$$\mathbb{Q}_p^\times = \langle p \rangle \times \langle \zeta_{p-1} \rangle \times (1 + p\mathbb{Z}_p)$$

$$(\mathbb{Q}_p^\times)^2 = \langle p^2 \rangle \times \langle \zeta_{p-1}^2 \rangle \times (1 + p\mathbb{Z}_p)$$

We get a basis p, ζ_{p-1}.

We have $N(\mathbb{Q}_p(\sqrt{p})|\mathbb{Q}_p) = \langle -p \rangle \times (\mathbb{Z}_p^\times)^2$

($(\mathbb{Z}_p^\times)^2$ is the only index 2 subgroup of $\mathbb{Z}_p^\times$,

and $\mathbb{Q}_p(\sqrt{p})|\mathbb{Q}_p$ is ramified, and

$N_{\mathbb{Q}_p(\sqrt{p})|\mathbb{Q}_p}(\sqrt{p}) = -p$)

so $\zeta_{p-1} \notin N(\mathbb{Q}_p(\sqrt{p})|\mathbb{Q}_p)$, and

$p \in N(\mathbb{Q}_p(\sqrt{p})|\mathbb{Q}_p) \Leftrightarrow -1 \in N(\mathbb{Q}_p(\sqrt{p})|\mathbb{Q}_p)$

$\Leftrightarrow p \equiv 1 \mod 4$.

So $(p,p)_p = (-1)^{\frac{p-1}{2}}$, $(p, \zeta_{p-1})_p = -1$.

We have $N(\mathbb{Q}_p(\sqrt{\zeta_{p-1}})|\mathbb{Q}_p) = \langle p^2 \rangle \times \mathbb{Z}_p^\times$,

so $\zeta_{p-1} \in N(\mathbb{Q}_p(\sqrt{\zeta_{p-1}})|\mathbb{Q}_p) \Rightarrow$

$\Rightarrow (\zeta_{p-1}, \zeta_{p-1})_p = 1$.

Matrix $\begin{pmatrix} \frac{p-1}{2} & 1 \\ 1 & 0 \end{pmatrix}$ (entries in $\mathbb{F}_2$)

Determinant $= 1$, so $(\ ,\ )_p$ is non-degenerate.

$\underline{p=2:}$ Basis $2, \cancel{5}\ 5, \cancel{-1}\ -1$ (see Q9, Ex Sheet 3)

$\underline{K = \mathbb{Q}_2(\sqrt{2})}$

We have $N_{K|\mathbb{Q}_2}(1+\sqrt{2}) = -1$, $N_{K|\mathbb{Q}_2}(\sqrt{2}) = -2$

$\Rightarrow \quad N(K|\mathbb{Q}_2) = \langle -2 \rangle \times \langle -1 \rangle \times (1 + 8\mathbb{Z}_2)$

$\Rightarrow \quad 2, -1 \in N(K|\mathbb{Q}_2)$, $5 \notin N(K|\mathbb{Q}_2) \Rightarrow$

$\Rightarrow \quad (2,2)_2 = (2,-1)_2 = 1$, $(2,5)_2 = -1$.

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

K ~~has~~ is unramified, so $N(K|\mathbb{Q}_2) = \langle 4 \rangle \times \mathbb{Z}_2^\times$

so $-1, 5 \in N(K|\mathbb{Q}_2)$, $2 \notin N(K|\mathbb{Q}_2) \Rightarrow$

$(5,5)_2 = (5,-1)_2 = 1$.

$\underline{K = \mathbb{Q}_2(\sqrt{-1})}$

$N(K|\mathbb{Q}_2) = \langle 2 \rangle \times \cancel{\ldots}(1 + 4\mathbb{Z}_2)$

$\left(N_{K|\mathbb{Q}_2}(1+\sqrt{-1}) = 2,\ N_{K|\mathbb{Q}_2}(2+\sqrt{-1}) = 5 \right)$

so $2, 5 \in N(K|\mathbb{Q}_2)$, $-1 \notin N(K|\mathbb{Q}_2)$;

$(-1,-1)_2 = -1$.

Matrix $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ (entries $\mathbb{F}_2$).

So det $= 1$, so non-degenerate.

14. Let $\sigma \in S_n$. If $\sigma(I) = I$, then σ defines an automorphism of the quotient $K[X_1, \dots, X_n]/I \cong L$, i.e. an element of $Gal(L|K)$.

If $\sigma \neq \tau$ with $\sigma(I) = \tau(I) = I$, then the induced automorphisms of L/K are distinct, since they induce different permutations on the roots of f.

Conversely, let $\sigma \in Gal(L|K)$, ~~then~~

Note that $I = \{F \in K[X_1, \dots, X_n] \mid 0 = F(\alpha_1, \dots, \alpha_n)\}$.

If $F \in I$, we have $F(\sigma\alpha_1, \dots, \sigma\alpha_n) = 0$.

Let $\tau \in S_n$ be defined by $\sigma\alpha_i = \alpha_{\tau(i)}$

If $F \in K[X_1, \dots, X_n]$, $(\tau F)(\alpha_1, \dots, \alpha_n) = F(\alpha_{\tau(1)}, \dots, \alpha_{\tau(n)}) =$

$= F(\sigma\alpha_1, \dots, \sigma\alpha_n) = \sigma\left(F(\alpha_1, \dots, \alpha_n)\right)$

so $\tau F \in I \iff F \in I$.

Therefore $\tau(I) = I$, and the element of

$Gal(L|K)$ induced by τ is σ.

<u>Next part</u>:

Let $I = Ker\left(\mathbb{Q}[X_1, \dots, X_n] \longrightarrow \mathbb{Q}(\alpha_1, \dots, \alpha_n)\right)$,

$J = Ker\left(\mathbb{Q}_p[X_1, \dots, X_n] \longrightarrow \mathbb{Q}_p(\alpha_1, \dots, \alpha_n)\right)$.

Then $I = J \cap \mathbb{Q}[X_1, \dots, X_n]$.

If $\sigma \in S_n$, it follows that $\sigma(J) = J \Rightarrow$

$\Rightarrow \sigma(I) = \sigma(J) \cap \sigma\left(\mathbb{Q}[X_1, \dots, X_n]\right) =$

$= J \cap \mathbb{Q}[X_1, \dots, X_n] = I$

so $Gal(f|\mathbb{Q}_p) = \{\sigma \in S_n \mid \sigma(J) = J\} \subseteq$

$\subseteq \{\sigma \in S_n \mid \sigma(I) = I\} = Gal(f|\mathbb{Q})$.

Now assume that $f \in \mathbb{Z}[X]$ and that f is monic.

Let $K = \mathbb{Q}_p(\alpha_1, \dots, \alpha_n)$ be the splitting field of $f / \mathbb{Q}_p$. ~~Since~~ By our assumptions on f we have $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$.

If we denote by $x \longmapsto \bar{x}$ the reduction map $\mathcal{O}_K \longrightarrow k_K$, then since $f(X) = \prod_{i=1}^{n} (X - \alpha_i)$ we have

$$\bar{f}(X) = \prod_{i=1}^{n} (X - \bar{\alpha}_i)$$

so $\bar{\alpha}_1, \dots, \bar{\alpha}_n$ are the roots of $\bar{f}$, and $\alpha_i \longmapsto \bar{\alpha}_i$ is the desired natural bijection (when $\bar{f}$ is seperable).

Let $k = \mathbb{F}_p(\bar{\alpha}_1, \dots, \bar{\alpha}_n) \subseteq k_K$.

We have a diagram

$$\begin{tikzcd}
\mathrm{Gal}(f|\mathbb{Q}_p) \arrow[r, equal] & \mathrm{Gal}(K|\mathbb{Q}_p) \arrow[d, equal] \\
& \mathrm{Aut}_{\mathbb{Z}_p}(\mathcal{O}_K) \arrow[d] \arrow[dd, bend left, "{\phi(\sigma) = (\sigma \bmod \mathfrak{m}_K)|_k}"] \\
& \mathrm{Gal}(k_K|\mathbb{F}_p) \arrow[d] \\
\mathrm{Gal}(\bar{f}|\mathbb{F}_p) \arrow[r, equal] & \mathrm{Gal}(k|\mathbb{F}_p)
\end{tikzcd}$$

~~Since~~ An element $\sigma \in \mathrm{Gal}(K|\mathbb{Q}_p)$ is determined by how it permutes the α_i.

If $\sigma_1, \sigma_2 \in \mathrm{Gal}(K|\mathbb{Q}_p)$ with $\phi(\sigma_1) = \phi(\sigma_2)$, then $\overline{\sigma_1(\alpha_i)} = \overline{\sigma_2(\alpha_i)}$ $\forall i \iff \sigma_1(\alpha_i) = \sigma_2(\alpha_i)$ $\forall i \iff \sigma_1 = \sigma_2$, so ϕ is injective.

This gives an isomorphism

$$\mathrm{Gal}(K|\mathbb{Q}_p) \xrightarrow{\sim} \mathrm{Gal}(k|\mathbb{F}_p)$$

~~and~~, shows that $k_K = k$, and identifies $\mathrm{Gal}(f|\mathbb{Q}_p)$ with $\mathrm{Gal}(\bar{f}|\mathbb{F}_p)$ using the bijection

$\alpha_i \longmapsto \overline{\alpha_i}$ (note also that it shows that $K|\mathbb{Q}_p$ is unramified).

We conclude that we have a natural inclusion $\mathrm{Gal}(\bar{f} \mid \mathbb{F}_p) \leq \mathrm{Gal}(f \mid \mathbb{Q})$ as permutation groups.

<u>Last part</u>:

Let $L = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$. Since we have regarded $\alpha_1, \dots, \alpha_n$ as elements of a fixed algebraic closure $\overline{\mathbb{Q}_p} \mid \mathbb{Q}_p$, we have an inclusion $L \subseteq K = \mathbb{Q}_p(\alpha_1, \dots, \alpha_n)$ and this gives a valuation v on L. By Q11, Ex Sheet 2 and its solution, $v = v_{\mathfrak{p}}$ for a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_L$ (at least up to equivalence) and $K = L_{\mathfrak{p}}$.

We then see that the inclusion

$\mathrm{Gal}(f|\mathbb{Q}_p) \subseteq \mathrm{Gal}(f|\mathbb{Q})$ fits into a commutative diagram

$$\begin{tikzcd} \mathrm{Gal}(f|\mathbb{Q}_p) \arrow[d, "\wr"] & \subseteq & \mathrm{Gal}(f|\mathbb{Q}) \arrow[d, "\wr"] \\ \mathrm{Gal}(L_{\mathfrak{p}}|\mathbb{Q}_p) \arrow[rr] & & \mathrm{Gal}(L|\mathbb{Q}) \\ \sigma \arrow[rr, mapsto] & & \sigma|_L \end{tikzcd}$$

where the vertical arrows are the identifications from the first part of this question, and the lower horizontal map is the map studied in Q5.