The Homomorphism Form of Birational Anabelian Geometry

Alberto Corato
Doctor in Philosophy in Mathematics
October 2021

Department of Mathematics
College of Engineering, Mathematics, and Physical Sciences
University of Exeter

Submitted by Alberto Corato to the University of Exeter as a thesis for the Degree of Doctor of Philosophy in Mathematics, October 2021

Signed: .....

Abstract

Let K be a number field, and let $\overline{K}$ be a separable closure of K, which is unique up to isomorphism. One may define the absolute Galois group of K as $G_K = G(\overline{K}/K)$. The cohomology of the absolute Galois group can be studied using class field theory, which Neukirch used to show that some information about the primes of $\overline{K}$ is encoded in G_K, and is preserved by topological isomorphism of absolute Galois groups. Neukirch's construction allowed Uchida to show that a topological isomorphism between absolute Galois groups determines a unique isomorphism of separable closures, a result now known as the birational anabelian Isom-Form. Uchida also obtained some partial results on a variation of the Isom-Form where isomorphisms are replaced with homomorphisms, known as the birational anabelian Hom-Form. More recently, Saïdi and Tamagawa obtained results on the encoding of primes in the maximal m-step solvable quotient G_K^m of G_K, and they used this result on the encoding of primes to obtain an "m-step" version of the Isom-Form.

In this thesis, we build on some ideas used by Uchida to prove his partial results for the birational anabelian Hom-Form, combining them with the work of Saïdi and Tamagawa to determine a condition for which a continuous homomorphism σ_m between m-step solvably closed Galois groups determines some correspondence between primes. We then prove that under some conditions it is possible to recover an injection of fields from σ_m. We also prove that we are able to find conditions for which the injection we recover is uniquely determined, and use this result and the previous one to construct an m-step birational anabelian Hom-Form. Finally, we show that when one of the number fields in our homomorphism is $\mathbb{Q}$, we can define the Hom-Form using our previous result by requiring weaker conditions.

Contents

Notations and Definitions **4**

Introduction **7**

1 Neukirch-Uchida's Theorem **11**

1.1 Preliminary results on Class Field Theory 11

1.2 Local Theory 15

1.3 Neukirch-Uchida's theorem 20

2 The m-step Isom-Form **27**

2.1 The Isom-Form and the Hom-Form 27

2.2 m-step Local Theory 29

3 The m-step birational anabelian Hom-Form **39**

3.1 Local correspondence in the m-step homomorphism of birational anabelian geometry 39

3.2 Conditional Existence in the Hom-Form 51

3.3 Uniqueness 61

4 The m-step Hom-Form over $\mathbb{Q}$ **67**

Notations and Definitions

- For a Galois extension L/K, we will denote by $G(L/K)$ its Galois group.
- For a field k, and a subgroup G of $\mathrm{Aut}(k)$, we will denote by k^G the subfield of k of all the elements fixed under the action of G.
- For a field k, we will denote by $\bar{k}$ a separable closure of k, and by $G_k = G(\bar{k}/k)$ its absolute Galois group.
- For a field k, we will denote its characteristic by $char(k)$.
- We will call a field complete with respect to a discrete valuation with finite residue field a local field. If the valuation is not archimedean we will say the local field is non-archimedean.
- A number field is a finite algebraic field extension of the rational numbers $\mathbb{Q}$.
- We say that a field K is global if it is either a number field or the function field of a curve over a finite field.
- We will say a number field K is totally real if the image of all its embeddings in $\mathbb{C}$ is contained in $\mathbb{R}$. If no embedding $K \hookrightarrow \mathbb{C}$ has image contained in $\mathbb{R}$, we will say K is totally imaginary.
- For an algebraic extension K of $\mathbb{Q}$ (not necessarily finite), we will say that a prime $\mathfrak{p}$ of K is non-archimedean if it induces a non-archimedean valuation. We will denote the set of all non-archimedean primes of K by $\mathfrak{Primes}_K^{\mathrm{na}}$.
- For an extension of number fields K/k we will say that the prime $\mathfrak{P}$ of K is above the prime $\mathfrak{p}$ of k (or, vice versa, that $\mathfrak{p}$ is below $\mathfrak{P}$) if $\mathfrak{P} \cap k = \mathfrak{p}$.
- For a Galois extension K/k and a prime $\mathfrak{P}$ of K, we will denote by $D_{\mathfrak{P}}$ the decomposition group of $\mathfrak{P}$ in $G(K/k)$, we denote the maximal unramified quotient of $D_{\mathfrak{P}}$ by $D_{\mathfrak{P}}^{\mathrm{ur}}$, and the maximal tame quotient by $D_{\mathfrak{P}}^{\mathrm{tame}}$. We also denote by $I_{\mathfrak{P}}$ its inertia subgroup, which corresponds to the kernel of the quotient $D_{\mathfrak{P}} \to D_{\mathfrak{P}}^{\mathrm{ur}}$, and by $I_{\mathfrak{P}}^{\mathrm{tame}}$ the kernel of the quotient $D_{\mathfrak{P}}^{\mathrm{tame}} \to D_{\mathfrak{P}}^{ur}$.

- For a number field K, a prime $\mathfrak{p} \in \mathfrak{Primes}_K^{\mathrm{na}}$ we will denote by $\kappa(\mathfrak{p})$ its residue field, and we will say that $p = char(\kappa(\mathfrak{p}))$ is the residue characteristic of $\mathfrak{p}$.

- For a prime number l, we will denote by $\mathfrak{Primes}_K^{\mathrm{na},(l')}$ the set of all non-archimedean primes of K with residue characteristic different from l.

- For a number field K and a prime $\mathfrak{p}$ of K, we denote by $K_{\mathfrak{p}}$ the localization of K at $\mathfrak{p}$. We will denote by $d_{\mathfrak{p}}$ the degree of the finite extension $[K_{\mathfrak{p}} : \mathbb{Q}_p]$ also known as local degree. We will also denote by $e_{\mathfrak{p}}$ the ramification index of $K_{\mathfrak{p}}/\mathbb{Q}_p$, and by $f_{\mathfrak{p}}$ the inertia degree $[\kappa(\mathfrak{p}) : \mathbb{F}_p]$. We will also denote by $N(\mathfrak{p})$ the norm of the prime $\mathfrak{p}$, given by $N(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$.

- For an abelian profinite group A, we will denote by A_{tor} its torsion subgroup, by $\overline{A_{\mathrm{tor}}}$ the closure of its torsion subgroup and write $A^{/\mathrm{tor}}$ for its torsion-free quotient group. For a profinite group G we will denote by $G^{\mathrm{ab}/\mathrm{tor}}$ the torsion-free quotient of the abelianization of G, that is $(G^{\mathrm{ab}})^{/\mathrm{tor}}$.

- For a global field K, a prime $\mathfrak{P}$ in the separable closure $\bar{k}$, and its decomposition group $D_{\mathfrak{P}}$ in the extension $\overline{K}/K$,

- For a global field K and a subset S of $\mathfrak{Primes}_K^{\mathrm{na}}$ we define the Dirichlet density of the set S as

$$\delta(S) = \lim_{s \to 1^+} \frac{\sum_{p \in S} N(\mathfrak{p})^{-s}}{\sum_{p \in \mathfrak{Primes}_K^{\mathrm{na}}} N(\mathfrak{p})^{-s}}.$$

- For a number field K and a prime number p, consider the splitting

$$p\mathbb{Z} = \prod_{i=1}^{r} \mathfrak{p}_i e^{\mathfrak{p}_i}.$$

  We may then consider the inertia degrees $f_{\mathfrak{p}_i}$ for all $\mathfrak{p}_i$ above p, and order the $\mathfrak{p}_i$ so that for $1 \leq i \leq j \leq r$ we have $f_{\mathfrak{p}_i} \leq f_{\mathfrak{p}_j}$. We define then the splitting type of p in K as the monotone non-decreasing sequence $(f_{\mathfrak{p}_1}, ..., f_{\mathfrak{p}_r})$

- For a profinite group G and a prime number p, we will denote by $\mathrm{cd}_p(G)$ its cohomological p-dimension, and by $\mathrm{cd}(G)$ its cohomological dimension.

- For a profinite group G and a prime number p, we will denote by $G^{(p')}$ its prime-to-p quotient.

- For a profinite group G, we will denote by G^{ab} its maximal abelian quotient $G/\overline{[G,G]}$. If K is a number field and G_K is its absolute Galois group $G(\overline{K}/K)$, the abelianization corresponds to the maximal abelian extension of K contained in $\overline{K}$, which we will denote by K^{ab}.

- For the number field K and for the maximal integer s such that G_K^{ab} has a quotient isomorphic to $\mathbb{Z}_p^s$, we will say that K has $\mathbb{Z}_p$-rank s.

- For a profinite group G and two subgroups H and H' of G we will say that H and H' are commensurable if $H \cap H'$ is open in both H and H'.

- For a profinite group G, a subgroup H of G and a prime number l, we will say H is l-open in G if an l-Sylow subgroup of H is an open subgroup of an l-Sylow subgroup of G.

- For a profinite group G, we will denote by G_l an l-Sylow subgroup of G, which is determined uniquely up to conjugation.

- For a profinite group G, two subgroups H and H' of G, and a prime number l we will say that H and H' are l-commensurable if $H \cap H'$ is l-open in both H and H'.

- For an isomorphism $\sigma : G(K'/K) \xrightarrow{\sim} G(L'/L)$ of Galois groups, and for subextensions K'' of K'/K and L'' of L'/L, we will say K'' and L'' correspond to each other by σ if $\sigma(G(K'/K'')) = G(L'/L'')$.

- For a continuous homomorphism $\sigma : G(K'/K) \to G(L'/L)$ of Galois groups, for a subextension L'' of L'/L, we will say L'' corresponds to K'' by σ if $\sigma^{-1}(G(L'/L'')) = G(K'/K'')$.

- All homomorphism of profinite groups are assumed to be continuous with respect to the profinite topology.

Introduction

For a field K and a separable closure $\overline{K}$ of K we may define the absolute Galois group $G_K = G(\overline{K}/K)$. It is known that any two separable closures of K are isomorphic, and this isomorphism of fields induces an isomorphism between the respective absolute Galois groups. Furthermore, this isomorphism of groups is also continuous with respect to the profinite topology. Naturally, we may then ask if the inverse is also true, explicitly if a topological isomorphism between absolute Galois groups determines an isomorphism between separable closures.
Neukirch showed that starting from a continuous isomorphism σ between two absolute Galois groups $G(\overline{K}/K)$ and $G(\overline{L}/L)$ for two number fields K and L, it is possible to induce a bijection between the sets of primes of K and L by proving that σ must map a decomposition group in K isomorphically to a decomposition group in L. Furthermore, Neukirch also showed this bijection preserves the ramification index and inertia degree of a prime.
These result, known as Neukirch's **Local Theory**, were used by Uchida [Uch2] to obtain what is now known as Neukirch-Uchida's theorem.

Neukirch-Uchida's Theorem. *Let $\sigma : G_K \to G_L$ be an isomorphism of profinite groups. Then, there exists a unique isomorphism of fields $\tau : \overline{K} \to \overline{L}$ such that for all $g \in G_K$,*

$$\sigma(g) = \tau \circ g \circ \tau^{-1}.$$

We may also look at Neukirch-Uchida's theorem as a result that can be placed in the wider picture of **Grothendieck's anabelian conjectures**. In the formulation of these conjectures, Grothendieck ([Gro1] and [Gro2]) claimed that it is possible to recover properties about certain "anabelian" varieties from their fundamental groups. We are interested in looking at two of these conjectures, which in their complete form are stated using finitely generated infinite fields and their absolute Galois groups, the **birational anabelian Isom-Form**, and the **birational anabelian Hom-Form**

Birational Anabelian Isom-Form. *Given two finitely generated infinite fields K and L, and a topological isomorphism between their absolute Galois groups $\sigma : G_K \to G_L$, there exists a unique isomorphism of fields $\tau : \overline{K} \to \overline{L}$ such that*

for all $g \in G_K$,

$$\sigma(g) = \tau \circ g \circ \tau^{-1}.$$

Birational Anabelian Hom-Form. *Given two finitely generated infinite fields* K *and* L*, and a continuous homomorphism between their absolute Galois groups* $\sigma : G_K \to G_L$ *such that* $\sigma(G_K)$ *is open in* G_L*, there exists a unique injection of fields* $\tau : \overline{L} \hookrightarrow \overline{K}$ *such that for all* $g \in G_K$,

$$g \circ \tau = \tau \circ \sigma(g).$$

We may notice that Neukirch-Uchida's theorem is a solution for the Isom-Form in the case where K and L are number fields. Uchida also proved [Uch1] the Isom-Form for function fields of curves over finite fields, and the proof of the Isom-Form was later completed by Pop [Pop].
Whereas the Isom-Form has been proven, there is currently no complete solution for the Hom-Form, however a few partial results have been given. In the case of number fields Uchida [Uch3] proved that the Hom-Form holds unconditionally when $K = \mathbb{Q}$ by showing that in this case the homomorphism of profinite groups is really an isomorphism.
In this paper, he also proved that uniqueness in the Hom-Form also holds unconditionally, and that if we can place certain conditions on a continuous homomorphism of absolute Galois groups σ regarding the image of the decomposition groups of K, we are then able to construct a homomorphism of fields τ as in the statement of the Hom-Form.
More recently, Saïdi and Tamagawa [S-T] proved that replacing G_K and G_L with the **maximal** m**-step solvable quotients** G_K^m and G_L^m, and considering a continuous isomorphism $\sigma_m : G_K^m \to G_L^m$, it is possible to obtain an m-step solvable version of Neukirch's Local Theory. Saïdi and Tamagawa then used this result to show an m-step solvably closed version of Neukirch-Uchida's theorem, where the isomorphism we obtain is between the subfields of $\overline{K}$ and $\overline{L}$ corresponding to these m-step quotients, which are respectively denoted K_m and L_m,.

m-step solvable Isom-Form for Number Fields. *Let* K *and* L *be number fields, let* $m \geq 0$ *be an integer and let* $\sigma_{m+3} : G_K^{m+3} \to G_L^{m+3}$ *be an isomorphism of profinite groups. Consider the isomorphism of profinite groups* $\sigma_m : G_K^m \to G_L^m$ *induced by* σ_{m+3}.
Then, there exists a field isomorphism $\tau_m : K_m \xrightarrow{\sim} L_m$ *such that*

$$\sigma_m(g) = \tau_m g \tau_m^{-1}$$

for every $g \in G_K^m$*, which induces an isomorphism* $\tau : K \xrightarrow{\sim} L$.

An essential part in Saïdi and Tamagawa's work is the investigation of particu-

lar subgroups of the m-step solvably closed Galois group G_K^m, which are identified as the subgroups satisfying a group theoretic property they denote by $(\star_l)$.
Saïdi and Tamagawa show that the subgroups of G_K^m satisfying property $(\star_l)$ are strongly connected to the decomposition groups of the primes of K, and precisely they can be used to recover in a purely group theoretic way the decomposition groups in G_K^m by starting from G_K^{m+2} and "losing" two abelian steps. This connection is then used to formulate their m-step solvable Local Theory, and a τ_m as in the statement is constructed by using a proof similar to Uchida's construction of τ in the Isom-Form.
In this work, we are interested in observing how the Local Theory established by Saïdi and Tamagawa can be applied to a continuous homomorphism of m-step solvable groups with open image, and our goal is to obtain an m-step solvable analogue of Uchida's results on the Hom-Form.
In Chapter 1, we will be giving a brief overview of Neukirch's Local Theory and Uchida's proof of Neukirch-Uchida's theorem, together with a few necessary classical results from Class Field Theory.
Then, in Chapter 2, we will be giving the definition of $(\star_l)$-subgroups, and the statement and proof of a few fundamental results on $(\star_l)$-subgroups obtained by Saïdi and Tamagawa which they used to establish their m-step solvable Local Theory.
In Chapter 3 we will start looking at a homomorphism $\sigma_m : G_K^m \to G_L^m$ with open image, and how we may use $(\star_l)$-subgroups to piece together a mapping between some primes of K and some primes of L, giving an idea for a foundation for a Local Theory. Then, we will show that if we put certain conditions involving $(\star_l)$-subgroups on σ_m, we are then able to construct a mapping between the sets of primes with finite residue field of K and L (denoted respectively $\mathfrak{Primes}_K^{\mathrm{na}}$ and $\mathfrak{Primes}_L^{\mathrm{na}}$) using decomposition groups, and this will allow us to give a Local Theory as desired. We will then use this Local Theory to obtain the following result, which can be found at Theorem 3.2.7 in this thesis:

Theorem A. *Let $m \geq 1$ be a positive integer, and let $\sigma_{m+4} : G_K^{m+4} \to G_L^{m+4}$ be a homomorphism of profinite groups such that the homomorphism of profinite groups $\sigma_{m+3} : G_K^{m+3} \to G_L^{m+3}$ induced naturally from σ_{m+4} restricts to an injection on every subgroups of G_K^{m+3} satisfying condition $(\star_l)$ for some prime number l. Consider the homomorphism of profinite groups $\sigma_m : G_K^m \to G_L^m$ induced by σ_{m+4}. Then, there exists an embedding of fields $\tau_m : L_m \to K_m$ that induces σ_m by*

$$\tau_m \sigma_m(g) = g\tau_m$$

for all $g \in G_K^m$.

We will then prove some results on uniqueness, showing that the homomor-

phism we constructed in Theorem A is unique whenever some conditions on the solvability of K with respect to $\mathbb{Q}$ or, alternatively on the image of σ_m are satisfied. The following will be the main result of this chapter, the proof for which can be found at Theorem 3.3.9 in this thesis.

Theorem B. *Let K and L be number fields, let $m \geq 1$ be an integer and assume K contained in the $m-1$-step solvably closed extension $\mathbb{Q}^{m-1} \subseteq K_m$ of $\mathbb{Q}$. Let $\sigma_{m+4} : G_K^{m+4} \to G_L^{m+4}$ be a homomorphism of profinite groups with open image such that the induced homomorphism of profinite groups $\sigma_{m+3} : G_K^{m+3} \to G_L^{m+3}$ restricts to an injection on every subgroup of G_K^{m+3} satisfying property $(\star_l)$ for some prime number l.*
Then, there exists a unique homomorphism of fields $\tau_m : L_m \to K_m$ such that $\tau_m \sigma_m(g) = g\tau_m$ for all $g \in G_K^m$.

In Chapter 4, we use these result from Chapter 3 to show that we can weaken the conditions we require to construct an m-step Hom-Form in Theorem A are when $K = \mathbb{Q}$, and our criteria for uniqueness is also satisfied. We will in particular be able to obtain the following result, the proof of which can be seen in Theorem 4.5 in this thesis:

Theorem C. *Let $m \geq 0$ and let $\sigma_{m+4} : G_K^{m+4} \to G_L^{m+4}$ be a homomorphism of profinite groups with open image, assume $K = \mathbb{Q}$ and that the image by the homomorphism $\sigma_{m+2} : G_K^{m+2} \to G_L^{m+2}$ induced by σ_{m+4} of any subgroup of G_K^{m+2} satisfying property $(\star_l)$ contains no torsion elements. Then $L = \mathbb{Q}$, and the induced homomorphism $\sigma_{m+1} : G_K^{m+1} \to G_L^{m+1}$ is an isomorphism. Furthermore, if $m \geq 2$ there exists a unique isomorphism of fields $\tau_m : K_m \to L_m$ such that $\sigma_m(g) = \tau_m g \tau_m^{-1}$ for all $g \in G_K^m$.*

Chapter 1

Neukirch-Uchida's Theorem

In this chapter, we introduce a few classical results from class field theory, and their role in determining Neukirch's local theory. Once the local theory has been established, we look at Uchida's proof for the Neukirch-Uchida theorem

1.1 Preliminary results on Class Field Theory

In this section, we will be introducing a few classical results in Class Field Theory and in the cohomology of number fields. All the results will only be given for number fields, but similar results also can be stated for function fields of curves over finite fields. The results in this section, together with their function field counterpart, can be found in [NSW].

Let k be a field, $\bar{k}$ a separable closure of k and G_k the absolute Galois group, which we endow with the profinite topology. We can define the Brauer group of the field k, denoted $\mathrm{Br}(k)$, as the cohomology group $H^2(G_k, \bar{k}^\times)$. If K/k is a Galois extension, we may also define the Brauer group of the extension K/k as $Br(K/k) = H^2(G(K/k), K^\times)$.
If k is a non-archimedean local field, there is a canonical isomorphism between the Brauer group $Br(k)$ and $\mathbb{Q}/\mathbb{Z}$, which is usually denoted

$$inv_k : Br(k) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z} \tag{1.1.1}$$

known as the invariant map.
Let $l \in \mathbb{N}$ be prime to the characteristic of the field k, and denote by μ_l the group of l-th roots of unity. Also, let $\bar{k}^\times$ denote the multiplicative group of $\bar{k}$. If we consider the map $\phi : \bar{k}^\times \to \bar{k}^\times$ given by $\phi(x) = x^l$, we have an exact sequence of group, known as the Kummer exact sequence

$$0 \to \mu_l \to \bar{k}^\times \xrightarrow{\phi} \bar{k}^\times \to 0. \tag{1.1.2}$$

The proofs for the following well known results can be found in [NSW], Propositions 7.1.8

Proposition 1.1.3. *Let k be a non-archimedean local field, and let l be a number prime to $char(k)$. Then, we have $H^2(G_k, \mu_l) \cong \mathbb{Z}/l\mathbb{Z}$.*

Proposition 1.1.4. *Let k be a non-archimedean local field. For a prime number p, we have $\mathrm{cd}_p(G_k) = 1$ when $p = char(k)$, else we have $\mathrm{cd}_p(G_k) = 2$.*

Recall that for a profinite group G, the abelianization G^{ab} is defined as the quotient $G/\overline{[G,G]}$, where $\overline{[G,G]}$ is the closure of the commutator subgroup of G. Studying the cohomology of the local field k, we obtain the following result ([NSW], Theorem 7.2.11)

Proposition 1.1.5. *Let k be a local field. Then there is an exact sequence*

$$0 \to k^\times \to G_k^{\mathrm{ab}} \to \hat{\mathbb{Z}}/\mathbb{Z} \to 0$$

where $\hat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$ and the map $k^\times \to G_k^{\mathrm{ab}}$ is the norm residue symbol $(\cdot, k)$.

These results on the cohomology of a local field can also be used to give a description of the cohomology of a number field. Let us now consider a number field K instead, and for a prime $\mathfrak{p}$ of K, denote by $K_\mathfrak{p}$ its completion with respect to $\mathfrak{p}$. We may define the idèle group of K as the restricted product $I_K = \prod'_\mathfrak{p} K_\mathfrak{p}^\times$ taken over all primes of K (including any archimedean prime).
As we have a natural inclusion $K^\times \hookrightarrow K_\mathfrak{p}^\times$ for all $\mathfrak{p}$, there is a diagonal injection $K^\times \to I_K$. Taking the quotient with respect to this diagonal injection, we may define the idèle class group as $C_K = I_K/K^\times$.
The idèle class group I_K is interesting as studying its cohomology we obtain the following result, known as the Hasse principle for Brauer Groups, which allows us to study the Brauer group of the number field K from the Brauer groups of its localizations.

Theorem 1.1.6 (Hasse principle for Brauer Groups)**.** *Let K be a number field. There is an exact sequence*

$$0 \to \mathrm{Br}(K) \to \oplus_\mathfrak{p} \mathrm{Br}(K_\mathfrak{p}) \overset{inv_K}{\to} \mathbb{Q}/\mathbb{Z} \to 0$$

where the invariant map inv_K is obtained by taking the sum of all the maps $inv_{K_\mathfrak{p}} : K_\mathfrak{p} \to \mathbb{Q}/\mathbb{Z}$ defined as in (1.1.1) *for all non-archimedean primes $\mathfrak{p}$ of K.*

Proposition 1.1.7. *Let S be a finite set of non-archimedean primes of a number field K. Then, there is a natural surjection*

$$Br(K) \to \bigoplus_{\mathfrak{p} \in S} Br(K_\mathfrak{p}).$$

Proof. For every non-archimedean prime $\mathfrak{p}$ we have, as defined in (1.1.1), an isomorphism $inv_{K_\mathfrak{p}} : \mathrm{Br}(K_\mathfrak{p}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$. Then by taking the sum of all the maps $inv_{K_\mathfrak{p}}$, we may define an invariant map $inv_S : \bigoplus_S \mathrm{Br}(K_\mathfrak{p}) \to \mathbb{Q}/\mathbb{Z}$, similarly to the definition of inv_K in Theorem 1.1.6. Let $\mathfrak{p}'$ be a prime not in S. Since $inv_{K_{\mathfrak{p}'}}$ is an isomorphism between $\mathrm{Br}(K_{\mathfrak{p}'}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$, for every element $x \in \bigoplus_S \mathrm{Br}(K_\mathfrak{p})$, we may take an element $y \in \mathrm{Br}(K_{\mathfrak{p}'})$ so that $inv_S(x) + inv_{\mathfrak{p}'}(y) = 0$. However, $x + y \in \oplus_\mathfrak{p} \mathrm{Br}(K_\mathfrak{p})$, and as it is in the kernel of the map inv_K from Theorem 1.1.6 the exactness of the sequence gives us $x + y$ is in the image of $Br(K)$. However, this also means that x is in the image of the natural map $Br(K) \to \bigoplus_{\mathfrak{p} \in S} Br(K_\mathfrak{p})$, and so this map is surjective. □

In the same way we extended the invariant map from a local field to a number field, we may also extend the norm residue symbol. (cf. [NSW], Proposition 8.1.24)

Proposition 1.1.8. *Let K be a number field, and let C_K be its idèle class group. There is a homomorphism*

$$rec : C_K \to G_K^{\mathrm{ab}},$$

called the reciprocity homomorphism, which has dense image and is given by

$$rec(a) = \prod_\mathfrak{p} (a, K_\mathfrak{p}),$$

where the $(\cdot, K_\mathfrak{p})$ are the norm residue symbols for the localizations $K_\mathfrak{p}$.
Furthermore, if we consider the canonical map $I_K \to C_K$, we may also define the map $rec : I_K \to G_K^{\mathrm{ab}}$ by composition.

We will also need the following result ([Ser], Chapter 4.4, Proposition 13)

Proposition 1.1.9. *Let K be a number field. If $p \neq 2$ or if K is totally imaginary,* $\mathrm{cd}_p(G_K) = 2$.

We will now introduce a few classical theorems, which will be used to give a proof of Neukirch-Uchida's theorem.
The first of these result we will need is Krasner's lemma ([NSW], 8.1.6)

Theorem 1.1.10 (Krasner's Lemma)**.** *Let k be a non-archimedean local field, let $\bar{k}$ be a separable closure of k and v the extension of the discrete valuation of k to $\bar{k}$. Let $\alpha_1 \in \bar{k}$ be any element, and let $\alpha_1, \alpha_2, ..., \alpha_n$ be all the conjugates of α_1 in $\bar{k}/k$. If for an element $\beta \in \bar{k}$ and $i = 2, ...n$ we have*

$$v(\alpha_1 - \beta) < v(\alpha_1 - \alpha_i)$$

then $k(\alpha) \subseteq k(\beta)$.

The following theorem can be stated for global fields in general, but we will be only needing it for number fields (cf. [Neu], Theorem 13.4).

Theorem 1.1.11 (Chebotarev's Density Theorem)**.** *Let K be a number field, L/K a finite Galois extension, and let g be an element of $G(L/K)$. Consider the set S of all non-archimedean primes $\mathfrak{p}$ of K unramified in the extension L/K such there exists a prime $\mathfrak{P}$ of L above $\mathfrak{p}$ and g coincides with the Frobenius automorphism of $\mathfrak{P}$ over K.*
Then, the set S has Dirichlet density $\delta(S) = \#\langle\sigma\rangle/\#G(L/K)$

Chebotarev's theorem has the following corollary (cf. [Neu], Corollary 13.6).

Corollary 1.1.12. *Let K be a number field, let L/K be a field extension, and let $S \subseteq \mathfrak{Primes}_K^{\mathrm{na}}$ be the subset of all non-archimedean primes of K that split completely in L/K. Then, $\delta(S) = \frac{1}{[L:K]} \iff L/K$ is a Galois extension.*

We may prove the following theorem by using Chebotarev's theorem (cf. [Neu] Proposition 13.9, [NSW] Theorem 12.2.5).

Theorem 1.1.13 (Bauer's theorem)**.** *Fix a separable closure Ω of $\mathbb{Q}$, let $K/\mathbb{Q}$ be a finite Galois extension, and $L/\mathbb{Q}$ a finite extension, and assume that both K and L are contained in Ω. Then if all but finitely many prime numbers that have a factor of local degree 1 in L split completely in K, $L \supseteq K$.*

Proof. Consider the composite Galois extension LK/L in Ω. Then, all but finitely many primes of L of local degree 1 split completely in LK/L. Then, the set of primes splitting completely in LK/L has Dirichlet density 1 and by Corollary 1.1.12 we get $LK = L$, and so $L \supseteq K$. □

We also need to state the following theorem, as it has an application that will play a key part in the proof of the Neukirch-Uchida theorem (cf. [NSW], Theorem 9.2.7).

Theorem 1.1.14 (Grunwald-Wang)**.** *Let K be a number field, let S be a finite set of non-archimedean primes of K, and $\forall\ \mathfrak{p} \in S$ fix an abelian extension $K'_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$.*
Let A be a finite abelian group such that for all $\mathfrak{p} \in S$ we may define an embedding $G(K'_{\mathfrak{p}}/K_{\mathfrak{p}}) \hookrightarrow A$. Then there exists an abelian extension of number fields K'/K with Galois group A such that the completion of K' with respect to each $\mathfrak{p} \in S$ is isomorphic to the $K'_{\mathfrak{p}}$ that has been fixed.

Before stating an application of this theorem, we need to define what an embedding problem is. Let K'/K be a Galois extension of K, and consider the canonical surjection $\phi : G_K \to G(K'/K)$. An embedding problem for the Galois group G_K is a diagram

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \downarrow \phi & & \\ 1 & \longrightarrow & N & \longrightarrow & E & \xrightarrow{\psi} & G(K'/K) & \longrightarrow & 1 \end{array}$$

where the bottom row is an exact sequence of profinite groups. The embedding problem is said to have a proper solution if there exists a surjective homomorphism $\phi' : G_K \to E$ and such that $\phi = \psi \circ \phi'$. In particular, for some Galois extension L/K, we have that $E \cong G(L/K)$ and so $N \cong G(L/K')$. An application of Grunwald-Wang's theorem then gives us the following result ([NSW], Proposition 9.2.9):

Proposition 1.1.15. *Let K'/K be a finite Galois extension of number fields with Galois group G. Let $n \in \mathbb{N}$ and let p be a prime number. Denote by $\mathbb{F}_p[G]^n$ the additive group given by n copies of $\mathbb{F}_p[G]$ and equipped with the action of G given by left multiplication. Then, the embedding problem*

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \downarrow \phi & & \\ 1 & \longrightarrow & \mathbb{F}_p[G]^n & \longrightarrow & E & \xrightarrow{\psi} & G & \longrightarrow & 1 \end{array}$$

given by the corresponding split exact sequence is properly solvable. That is, there exists a Galois extension L of K' such that $\mathbb{F}_p[G]^n \cong G(L/K')$ and $E = \mathbb{F}_p[G]^n \rtimes G$.

Let us also recall Leopoldt's conjecture (see [NSW], Conjecture 10.3.5), originally formulated by Leopoldt in [Leo], which claims that for every prime number p, the rank of the p-adic regulator of a number field K is equal to $r_1 + r_2 - 1$, where r_1 is the number of real places of K and $2r_2$ is the number of complex places (that is, r_2 is the number of pairs of complex places). If the Leopoldt conjecture holds true in K for p, it has been shown ([Gras], Chapter III, Conjecture 1.6.4), that, if we denote by s the $\mathbb{Z}_p$-rank of K, we have $s = r_2 + 1$. The Leopoldt conjecture has been proven to hold in a few cases by Brumer [Bru]:

Theorem 1.1.16. *Assume K is an abelian extension of $\mathbb{Q}$ or of an imaginary quadratic field. Then, the Leopoldt conjecture holds for K and any prime number p.*

1.2 Local Theory

In this section, the main result is Neukirch's Local Theory, and we will also be giving some results required to establish it. The following result can be found in [NSW], Proposition 12.1.1, where it is proven for the more general case of global fields

Proposition 1.2.1. *Let k be a field, complete with respect to a valuation v, and let $f_1 = \sum_{i=0}^{d} a_i X^i$ and $f_2 = \sum_{i=0}^{d} b_i X^i$ be two separable polynomials in $k[X]$, both of degree d. Then if $v(f_1 - f_2) = \max_i\{v(a_i - b_i)\}$ is smaller than a positive constant determined by the roots of the polynomials, f_2 has the same splitting field as f_1.*

Proof. Assume first that v is an archimedean valuation. By Ostrowski's theorem, either $k \cong \mathbb{R}$ or $k \cong \mathbb{C}$. Let us assume $k = \mathbb{R}$. Then f_1 either has d zeroes in $\mathbb{R}$, and so has splitting field $\mathbb{R}$, or it has a complex zero and splitting field $\mathbb{C}$. All separable polynomials whose coefficients are close enough to f_1 have all their zeroes in $\mathbb{R}$ and or have a complex zero respectively. The case where $k = \mathbb{C}$ is trivial as $\mathbb{C}$ is algebraically closed.
Assume now v is non-archimedean. Let $\alpha_i \in \bar{k}$ for $i = 1, .., d$ be the roots of f_1, and $\beta_j \in \bar{k}$ for $j = 1, .., d$ be the roots of f_2. Then,

$$v(f_2(\alpha_i)) = v((f_1 - f_2)(\alpha_i)) = v(\sum_l (a_l - b_l)\alpha_i^l) \leq \max_l\{v(f_1 - f_2)\alpha_i^l\},$$

which means that if we take a positive $\epsilon > v(f_1 - f_2)$, the value $v(f_2(\alpha_i))$ will be $< c\epsilon$ where c is a multiplicative constant determined as the maximum of $v(\alpha_i^l)$. We may also rewrite $f_2(\alpha_i)$ as a product $b_d \prod_j (\alpha_i - \beta_j)$, and so we get that for at least one j, the value $v(\alpha_i - \beta_j)$ must be smaller than $c\epsilon$ and set $\beta_{j(i)} = \beta_j$.
Assume that ϵ is small enough so that $v(\alpha_i - \beta_{j(i)}) < c\epsilon < v(\alpha_i - \alpha_l)$ whenever $l \neq i$, Krasner's Lemma (see Theorem 1.1.10) gives us $\alpha_i \in k(\beta_j)$, and repeating this argument for all the roots of f_1 we get that the splitting field of f_1 must be contained in the splitting field of f_2.
We may also reverse the argument, and assume we can choose ϵ small enough so that $v(\alpha_i - \beta_{j(i)}) < c'\epsilon < v(\beta_l - \alpha_{j(i)})$ where β_l varies over every root of f_2 distinct from $\beta_{j(i)}$ and c' is a constant determined as the maximum of $v(\beta_{j(i)}^l)$. Then, this gives us the choice of $\beta_{j(i)}$ is unique for every i, and as the α_i are different (as f_1 is separable), it follows that if we can choose an ϵ small enough we obtain a bijection between the sets of roots of f_1 and f_2 by setting $\alpha_i \to \beta_{j(i)}$. We can then apply Krasner's lemma again, and we get the other inclusion.
Let C be the minimum of all the c and c' as determined before. The argument above gives us that if we can choose an ϵ small enough such that for all $1 \leq i \leq d$ we have $v(\alpha_i - \beta_{j(i)}) < C\epsilon$ we can indeed say that f_1 and f_2 have the same splitting field by t. □

The following result is taken from [NSW], Proposition 12.1.2, and like the previous result it is proven for all global fields.

Proposition 1.2.2. *Let k be a number field, $\bar{k}$ a separable closure, and let K be a proper subfield of $\bar{k}$. Then, there is at most a unique prime $\mathfrak{p}$ of K such that $\mathfrak{p}$*

does not decompose in the extension $\bar{k}/K$.

Proof. Let K be a subextension of $\bar{k}/k$, and assume there are two distinct primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of K that do not split in $\bar{k}$. We want to show that necessarily $\bar{k} = K$. Let f_1 and f_2 be two separable non-constant polynomials of the same degree d over K.
By the approximation theorem, for every $\epsilon > 0$, we can say there exists a polynomial $f \in K[X]$ such that $|f - f_1|_{\mathfrak{p}_1} < \epsilon$ and $|f - f_2|_{\mathfrak{p}_2} < \epsilon$.
By the previous result, for an ϵ small enough we have that f and f_1 have the same splitting field over $K_{\mathfrak{p}_1}$. However, since $\mathfrak{p}_1$ does not decompose in the extension $\bar{k}/K$, so f and f_1 have the same splitting field over K. We may repeat the same argument for f and f_2 over $K_{\mathfrak{p}_2}$, and so we get the splitting fields over K of f_1 and f_2 must also coincide.
We may now take $x_1, ..., x_d$ to be distinct elements in K, and take the polynomial $f_1 = \prod_{i=1}^{d}(X - x_i)$ which has splitting field K. We may also take the polynomial f_2 so that it is separable over K and irreducible of degree d. Now, since the splitting field of f_2 must be the same as that of f_1, that is K, and f_2 is irreducible over K it follows that K must in fact be $\bar{k}$. □

If there exists a prime $\mathfrak{p}$ of K that does not decompose in $\bar{k}/K$, which would be unique by the above proposition, we will say that K is $\bar{k}$-Henselian with respect to $\mathfrak{p}$. Proposition 1.2.2 has the following corollary ([NSW], Proposition 12.1.3)

Corollary 1.2.3. *Let k be a number field, and $\bar{k}$ a separable closure of k. If $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are distinct primes of $\bar{k}$, and $D_{\mathfrak{P}_1}$ and $D_{\mathfrak{P}_2}$ are their decomposition groups in G_k respectively. Then, $D_{\mathfrak{P}_1} \cap D_{\mathfrak{P}_2} = 1$*

Proof. Assume that $H = D_{\mathfrak{P}_1} \cap D_{\mathfrak{P}_2}$ is non-trivial. Then, the fixed field $K = \bar{k}^H$ is a proper subfield of $\bar{k}$ and is also extension of the fixed field of both decomposition groups. Thus, we have that both $\mathfrak{P}_1 \cap K$ and $\mathfrak{P}_2 \cap K$ do not split in $\bar{k}$, and by Proposition 1.2.2 we may conclude that $K = \bar{k}$ and get a contradiction. □

An immediate application of this corollary is the following ([NSW], Corollary 12.1.6):

Lemma 1.2.4. *Let k be a number field. Then G_k has trivial center.*

Proof. Let $g \in G_k$ be an element of the center. Then for any prime $\mathfrak{P}$ of $\bar{k}$, we have $D_{g\mathfrak{P}} = gD_{\mathfrak{P}}g^{-1} = D_{\mathfrak{P}}$, and by Corollary 1.2.3 we have that necessarily $g\mathfrak{P} = \mathfrak{P}$, that is $g \in D_{\mathfrak{P}}$. However, if we consider any prime $\mathfrak{P}' \neq \mathfrak{P}$, we have by the same reasoning that $g \in D_{\mathfrak{P}'}$, and so g is in the intersection of the decomposition groups of two different primes, which means that by Corollary 1.2.3 we have $g = 1$. □

We also have the following lemma ([Uch1], Lemma 2):

Lemma 1.2.5. *Let k be an algebraic extension of $\mathbb{Q}$ (not necessarily finite) and let $\bar{k}$ be a separable closure of k. If there exists a prime number l such that $\mathrm{Br}(\bar{k}/K)(l)$ is of rank 1 for every finite subextension K of $\bar{k}/k$, we have that k is $\bar{k}$-Henselian with respect to some prime $\mathfrak{p}$ of K.*

Proof. By Theorem 1.1.6, for all finite subextensions k' of $K/\mathbb{Q}$, we have the map $\mathrm{Br}(k') \to \prod_{\mathfrak{p}'} \mathrm{Br}(k'_{\mathfrak{p}'})$, where $\mathfrak{p}'$ ranges over the primes of k', is injective. As the $\mathrm{Br}(\bar{k}')$ define a projective system, we may pass to the projective limit and get an injective map $\mathrm{Br}(\bar{k}/K) \to \prod_{\mathfrak{P}} \mathrm{Br}(K_{\mathfrak{P}})$ where $\mathfrak{P}$ ranges over the primes of K. It follows then that there exists a unique prime $\mathfrak{P}$ of K such that $\mathrm{Br}(K_{\mathfrak{P}})(l) \neq 0$. Let $\mathfrak{p} = \mathfrak{P} \cap k$. The l-part of the Brauer group of every extension of $\mathfrak{p}$ is non-trivial, and so we have that $\mathfrak{p}$ has a unique extension $\mathfrak{P}$ to K. It follows then k is $\bar{k}$-henselian with respect to $\mathfrak{p}$ as desired, since $\mathfrak{p}$ does not decompose in any finite extension of k. □

Finally, this lemma will allow us to give the proof of Neukirch's Local Theory ([NSW], Lemma 12.1.10)

Lemma 1.2.6. *Let k be a number field, $\bar{k}$ a separable closure of k, $\mathfrak{P}$ a prime of $\bar{k}$ and $D_{\mathfrak{P}} \subset G_k$ its decomposition group. If $H \subseteq G_k$ is an infinite closed subgroup such that H and $D_{\mathfrak{P}}$ are commensurable, then $H \subseteq D_{\mathfrak{P}}$.*

Proof. Let $K = \bar{k}^H$ be the fixed field of H, and let U be any open subgroup of $H \cap D_{\mathfrak{P}}$ such that U is a normal subgroup H, and let $L = \bar{k}^U$.
Since U is open in H, $[L : K]$ is finite, and since $U \subseteq D_{\mathfrak{P}}$, the prime $\mathfrak{p} = L \cap \mathfrak{P}$ does not decompose in the extension $\bar{k}/L$, so we have L is Henselian with respect to $\mathfrak{p}$.
If we consider the prime $\mathfrak{p} \cap K$, we may observe that since all its extensions to L are conjugate to $\mathfrak{p}$, then L is also Henselian with respect to these extensions. However, by Proposition 1.2.2, such a prime must be unique, and so $\mathfrak{p} \cap K$ extends uniquely to $\mathfrak{p}$, which in turn extends uniquely to $\mathfrak{P}$, and so $H \subseteq D_{\mathfrak{P}}$. □

We have now everything we need to present the final result of Neukirch's Local Theory. We will adapt the formulation and the proof used by Uchida in ([Uch1], Lemma 3)

Theorem 1.2.7 (Neukirch)**.** *Let k_1 and k_2 be number fields, and fix $\bar{k}_1$ and $\bar{k}_2$ separable closures of k_1 and k_2 respectively. We may then take the absolute Galois groups G_{k_1} and G_{k_2}, and let $\sigma : G_{k_1} \to G_{k_2}$ be an isomorphism of profinite groups. Let $\mathfrak{p}_1$ be a prime of k_1 and $\mathfrak{P}_1$ be a prime of $\bar{k}_1$ above $\mathfrak{p}_1$. Let D_1 be the decomposition group of $\mathfrak{P}_1$ in G_{k_1}, and let $D_2 = \sigma(D_1)$. Then, there exists a unique prime $\mathfrak{p}_2$ of k_2 and a prime $\mathfrak{P}_2$ of $\bar{k}_2$ above $\mathfrak{p}_2$ such that D_2 is the decomposition group of $\mathfrak{P}_2$ in G_{k_2}.*

Furthermore, we may define a bijective map $\phi : \mathfrak{Primes}_{\bar{k}_1}^{\mathrm{na}} \to \mathfrak{Primes}_{\bar{k}_2}^{\mathrm{na}}$ *by mapping* $\phi(\mathfrak{P}_1) = \mathfrak{P}_2$ *which is Galois equivariant with respect to* σ*.*

Proof. Let E_1 and E_2 be the subfields of $\bar{k}_1$ and $\bar{k}_2$ corresponding to D_1 and D_2 respectively. Since E_1 is the decomposition field of $\mathfrak{P}_1$, we have $[E_{1,\mathfrak{P}_1} : k_{1,\mathfrak{p}_1}] = 1$. Then, for any finite subextension F_1 of $\bar{k}_1/E_1$, it follows the extension $F_{1,\mathfrak{P}_1}/k_{1,\mathfrak{p}_1}$ is also finite. For a fixed extension F_1, denote by F_2 the subfield of $\overline{L}$ corresponding to F_1 by σ.
Let l be a prime number and let μ_l be the group of l-th roots of unity. By Lemma 1.2.6 we may assume that both F_1 and F_2 contain μ_l up to replacing them with open subgroups.
Applying cohomology to the exact sequence $1 \to \mu_l \to \bar{k}_2^\times \to \bar{k}_2^\times \to 1$, we know that by Proposition 1.1.9 we have $\mathrm{cd}_l\, G(\bar{k}_2/F_2) = 2$ and using the Hasse-Brauer exact Sequence (Theorem 1.1.6) we get an exact sequence

$$0 \to H^2(G(\bar{k}_2/F_2), \mu_l) \to \mathrm{Br}(F_2) \xrightarrow{l} \mathrm{Br}(F_2) \to 0$$

where the kernel of the surjective map is the l-torsion of $\mathrm{Br}(F_2)$.
Now, σ induces an isomorphism $H^2(G(\bar{k}_1/F_1), \mu_l) \xrightarrow{\sim} H^2(G(\bar{k}_2/F_2), \mu_l)$, so they have the same order. The exact sequence then gives that $Br(F_2)(l)$ has rank 1, and the same holds true for any extension of F_2, and so by Lemma 1.2.5, we get that F_2 is $\bar{k}_2$-Henselian with respect to some prime $\mathfrak{P}_2$ of $\bar{k}_2$.
Consider the restriction of $\mathfrak{P}_2$ to E_2, which we will denote $\widetilde{\mathfrak{P}}_2$, and let $\mathfrak{q}_1, ..., \mathfrak{q}_n$ be all the extensions of $\widetilde{\mathfrak{P}}_2$ to F_2 (including $\mathfrak{P}_2$). Since the extension F_2/E_2 is finite, it follows that $\mathrm{Br}(F_{2,\mathfrak{q}_i})(l) \neq 0$ for all the $\mathfrak{q}_i$, but by Proposition 1.1.7 we have the map $Br(F_2) \to \prod_i \mathrm{Br}(F_{2,\mathfrak{q}_i})$ is surjective. However, this can only be true if there is only one extension of $\widetilde{\mathfrak{P}}_2$ to F_2. In particular, this means that E_2 is $\bar{k}_2$-Henselian with respect to the prime $\mathfrak{P}_2$. This also means that D_2 is contained in the decomposition group of $\mathfrak{P}_2$.
Repeating the same argument with σ^{-1}, we get that D_2 is actually the entire decomposition group of $\mathfrak{P}_2$. Furthermore, replacing $\mathfrak{P}_1$ with a different prime conjugate to it over $\mathfrak{p}_1$ (and $\mathfrak{P}_2$ with a different prime conjugate to it over $\mathfrak{p}_2$) is equivalent to replacing D_1 (resp. D_2) with a conjugate subgroup in G_K (resp. G_L).
We may conclude then that $\mathfrak{p}_2$ is determined uniquely, and we may define a bijection $\phi : \mathfrak{Primes}_{\bar{k}_1}^{\mathrm{na}} \to \mathfrak{Primes}_{\bar{k}_2}^{\mathrm{na}}$ as desired by $\phi(\mathfrak{P}_1) = \mathfrak{P}_2$. □

The first part of the proof for the following theorem repeats the same argument as the previous proposition. This result is analogous to the previous one ([NSW], Theorem 12.1.9.)

Theorem 1.2.8. *Let k be a number field, κ a non-archimedean local field, and assume that there exists a closed subgroup $H \leq G_k$ such that $H \cong G_\kappa$. Then there exists a unique prime $\mathfrak{p}$ in k, and a unique prime $\mathfrak{q}$ above $\mathfrak{p}$ in $\overline{K}$ such that H is open in $D_\mathfrak{q}$.*

Proof. By Lemma 1.2.6, we may assume that k contains μ_p for some odd prime number p. By Proposition 1.1.3 we have $H^2(U, \mu_p) \cong \mathbb{Z}/p\mathbb{Z}$ for all open subgroups U of H.
Let K be the subfield of $\bar{k}$ corresponding to H. Consider the injective map $H^2(G_K, \mu_p) \to \prod H^2(G_{K_\mathfrak{P}}, \mu_p)$ from Theorem 1.1.6. The injectivity of this map implies that one of the $H^2(G_{K_\mathfrak{P}}, \mu_p)$ must be non-trivial, and so fix a prime $\mathfrak{P}$ such that $H^2(G_{K_\mathfrak{P}}, \mu_p)$ is non-trivial. Since we chose p odd, $\mathfrak{P}$ is non-archimedean.
Let L be an arbitrary separable extension of K, corresponding to an open subgroup U of H. By Proposition 1.1.7 there is a surjection $H^2(G_L, \mu_p) \to \prod_\mathfrak{P} H^2(G_{L_\mathfrak{P}}, \mu_p)$, where the product is indexed over all primes of L above $\mathfrak{P}$. Let $\mathfrak{P}'$ be a prime of L above $\mathfrak{P}$. We have that $G_{L'_\mathfrak{P}}$ is an open subgroup of $G_{K_\mathfrak{P}}$, and so we have an isomorphism $H^2(G_{L_\mathfrak{P}}, \mu_p) \cong Z/p\mathbb{Z}$. The surjectivity of the map then implies by a counting argument that there can only be one such $\mathfrak{P}'$, and since L was chosen arbitrarily then $\mathfrak{P}$ does not decompose in any extension of K, and so it does not decompose in $\bar{k}/K$. The unique prime above $\mathfrak{P}$ in $\bar{k}$ is then the $\mathfrak{q}$ we were looking for. Such a $\mathfrak{q}$ is unique as by Corollary 1.2.3 for all other primes $\mathfrak{q}'$ of $\overline{K}$, $H \cap G_{\mathfrak{q}'} = 1$. □

1.3 Neukirch-Uchida's theorem

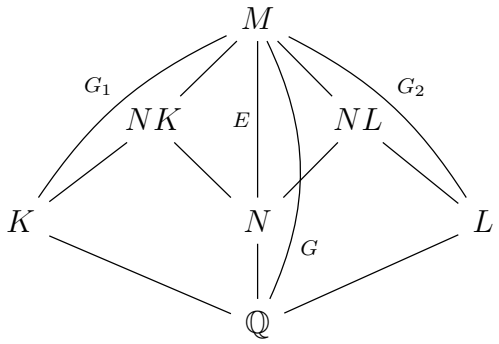
Now that the local theory has been stated and proven, we can proceed to state and prove Neukirch-Uchida's theorem, which is going to be the main theorem in this section. The results here are taken from [Uch2], where Uchida proves the same results in the slightly more general case of solvably closed Galois extensions.

Let K and L be number fields, and let $\overline{K}$ and $\overline{L}$ be respectively a separable closure for K and for L. The fields K and L are said to be arithmetically equivalent if they have the same Dedekind ζ function. A result by Perlis [Per] gives us that K and L are arithmetically equivalent if and only if every prime number l has the same splitting type in K and L. Arithmetic equivalence was shown by Gassmann [Gas] to be equivalent to the following: let us consider the Galois extension $M/\mathbb{Q}$ given by the composite of the normal closures of K and L, the Galois group $G(M/K)$ and $G(M/L)$ have the same number of elements in every conjugacy class of $G(M/\mathbb{Q})$. This condition is also known as Gassmann equivalence.
Theorem 1.2.7, together with Local Class Field Theory, shows that if we have an isomorphism of profinite groups $\sigma : G_K \to G_L$, then corresponding primes of K

and L have the same residue characteristic, inertia degree and ramification index as we can recover them from their decomposition group. In particular, K and L are arithmetically equivalent, and this statement also holds when replacing K and L with finite separable extensions K' and L'. The following result is taken from ([Uch2], Lemma 1).

Lemma 1.3.1. *Let K, L be number fields, and let $N/\mathbb{Q}$ be a Galois extension. Then, if K and L are arithmetically equivalent, the composites NK and NL are also arithmetically equivalent.*

Proof. Let $M/\mathbb{Q}$ be a Galois extension containing K, L and N. Let $E = G(M/N)$ be the corresponding Galois group, which is a normal subgroup of $G = G(M/\mathbb{Q})$, and let $G_1 = G(M/K)$ and $G_2 = G(M/L)$.



As K and L are arithmetically equivalent, two conjugacy classes of G_1 and G_2 in G have the same size. Furthermore, since E is normal in G, the subgroups $G_1 \cap E$ and $G_2 \cap E$, which correspond to the composites KN and LN respectively, will also have the same number of elements in every conjugate class of G. It now follows by the discussion above that KN and LN are arithmetically equivalent. □

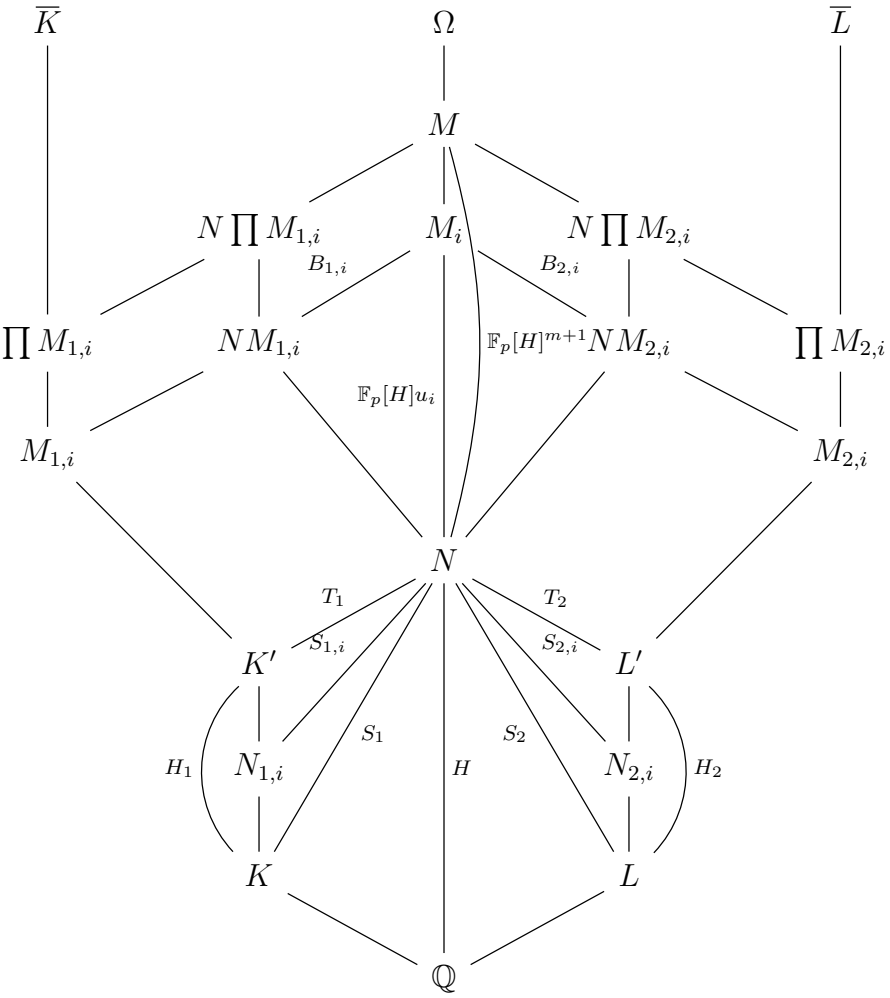
We may now state and prove the celebrated Neukirch-Uchida Theorem. We will be adapting the proof given by Uchida in [Uch2].

Theorem 1.3.2 (Neukirch-Uchida's theorem)**.** *Let $\sigma : G_K \to G_L$ be an isomorphism of profinite groups. Then, there exists a unique isomorphism of fields $\tau : \overline{K} \to \overline{L}$ such that for all $g \in G_K$*

$$\sigma(g) = \tau \circ g \circ \tau^{-1}.$$

Proof. Let K'/K be a finite Galois extension of K contained in $\overline{K}$, let U_1 be the open normal subgroup of G_K corresponding to K', and let L' be the subfield of $\overline{L}$ corresponding to $U_2 = \sigma(U_1)$. Since the isomorphism gives that U_2 is an open normal subgroup of G_L, we also have that L'/L is a Galois extension. Let us denote by $H_1 = G(K'/K)$ and $H_2 = G(L'/L)$ the respective Galois groups. Then, the isomorphism σ induces an isomorphism of finite groups $H_1 \to H_2$ by quotients which, by abuse of notation, we will also denote σ.

Let $\mathfrak{A}_{K'}$ be the set of isomorphisms $\tau : K' \to L'$ such that $\sigma(g) = \tau \circ g \circ \tau^{-1}$ for all $g \in H_1$. The collection of sets $\mathfrak{A}_{K'}$ indexed over all the finite Galois extension K'/K contained in $\overline{K}$ defines a projective system. Furthermore, since all the $\mathfrak{A}_{K'}$ are finite (compact) and non-empty, their inverse limit over K' is non-empty as well ([RZ], Proposition 1.1.4), and it corresponds to the set of isomorphisms $\tau : \overline{K} \to \overline{L}$ satisfying the conditions of the theorem's statement. Thus, if we can show that for an arbitrary choice of an extension K' finite and Galois over K, the set $\mathfrak{A}_{K'}$ is non-empty and finite, the existence of τ in the statement is proven.
The diagram below is a visualization of the constructions in the following part of the proof.



Fix then a Galois extension K'/K and let L' be the Galois extension of L contained in $\overline{L}$ corresponding to K' by σ. For a fixed separable closure Ω of $\mathbb{Q}$, we have embeddings of K' and L' in Ω. Let us fix two such embeddings, and let us also denote the images of these embeddings in Ω by K' and L'. Then, let N be a finite Galois subextension of $\Omega/\mathbb{Q}$ containing K' and L'. Let $H = G(N/\mathbb{Q})$, $S_1 = G(N/K)$, $S_2 = G(N/L)$, $T_1 = G(N/K')$ and $T_2 = G(N/L')$. Since H_1 is finite, we may take a set $\{h_{1,1}, ..., h_{1,m}\}$ of generators for H_1, and for $i = 1, .., m$, we set $h_{2,i} = \sigma(h_{1,i})$.

Furthermore, since $S_1/T_1 \cong H_1$ and $S_2/T_2 \cong H_2$, for all $1 \leq i \leq m$ we define $s_{1,i} \in S_1$ and $s_{2,i} \in S_2$ to be elements mapped to $h_{1,i}$ and $h_{2,i}$ by the quotients respectively. We may take a prime number p such that $p \equiv 1 \pmod{|H|}$ and we may also take $p > |H|^2$, and applying Proposition 1.1.15 we get a split exact sequence

$$1 \to \mathbb{F}_p[H]^{m+1} \to E \to H \to 1$$

where, for some Galois extension $M/\mathbb{Q}$ containing N, we have $E = G(M/\mathbb{Q})$ and $\mathbb{F}_p[H]^{m+1} \cong G(M/N)$. Since p does not divide $|H|$, we can find elements $u_0, ..., u_m$ in the group $\mathbb{F}_p[H]^{m+1}$ so that we may write $\mathbb{F}_p[H]^{m+1} = \oplus_{i=0}^{m} \mathbb{F}_p[H]u_i$. Denote by M_i be the subfield of M fixed by the subgroup of $\mathbb{F}_p[H]^{m+1}$ generated by $u_0, .., \widehat{u_i}, .., u_m$. This gives us that the Galois group $G(M_i/\mathbb{Q})$ is a split extension of H by $\mathbb{F}_p[H]u_i$.

For $1 \leq i \leq m$, let $S_{1,i}$ be the subgroup of S_1 generated by $s_{1,i}$ and T_1, and similarly let $S_{2,i}$ be the subgroup of S_2 generated by $s_{2,i}$ and T_2. Let $N_{1,i}$ be the subfield of N contained in K' corresponding to $S_{1,i}$ and $N_{2,i}$ be the subfield of N contained in L' corresponding to $S_{2,i}$ respectively. By construction, we have that $\sigma(S_{1,i}) = S_{2,i}$ and so $N_{1,i}$ corresponds to $N_{2,i}$ by σ. Let us also define $S_{1,0} = T_1$ and $S_{2,0} = T_2$.

Let χ_i be a character $S_{1,i}/T_1 \to \mathbb{F}_p$ of order $|S_{1,i}/T_1|$ (observe that if $i = 0$, this quotient is trivial and so is the character). We may take a field $M_{1,i}$ so that $M_{1,i}/K'$ is the maximal abelian p-extension of K' contained in M_i where the operation of $S_{1,i}/T_1$ on the Galois group $G(M_{1,i}/K')$ is given by scalar multiplication by the values of χ_i. Observe also that since T_1 contains no elements of order p (as we have chosen $p \equiv 1 \pmod{|H|}$ and T_1 is a subgroup of H), $M_{1,i}$ and N are disjoint as extensions of K'.

Since $M_{1,i}$ is an abelian extension of K', it can be identified with a subextension of $\overline{K}$, and so for each $M_{1,i}$ there exists a field $M_{2,i}$ contained in $\overline{L}$, which we can identify with a subfield of Ω, corresponding to it by σ. Since $M_{2,i}$ corresponds to $M_{1,i}$ by σ, they are arithmetically equivalent. Since by definition of arithmetical equivalence they have the same Galois closure, and M_i is a Galois extension of $M_{1,i}$, it follows that $M_i/M_{2,i}$ is a Galois extension as well and in particular $M_{2,i}$ is contained in M_i.

We have that χ_i also induces a character $\chi_i\sigma^{-1}$ of $S_{2,i}/T_2$, which we can by abuse of notation also denote χ_i. Since $N_{1,i}$ corresponds to $N_{2,i}$ by σ, it follows σ induces an isomorphism between $G(M_{1,i}/N_{1,i})$ and $G(M_{2,i}/N_{2,i})$, and it follows by construction that $M_{2,i}$ is also the maximal abelian p-extension of L' contained in M_i so that the operation of $S_{2,i}/T_2$ on the Galois group $G(M_{2,i}/L')$ is given by scalar multiplication by the values of χ_i, and $M_{2,i}$ and N are disjoint.

From the construction it also follows that the field $\prod_i M_{1,i}$ can also be identified

with an extension of K' contained in $\overline{K}$, and this extensions corresponds by σ to an extension of L' contained in $\overline{L}$ which can be identified with $\prod_i M_{2,i}$, which also means $\prod_i M_{1,i}$ and $\prod_i M_{2,i}$ are arithmetically equivalent. Furthermore as N, $M_{1,i}$ and $M_{2,i}$ are all subfields of M, by Lemma 1.3.1 we also have $N\prod_i M_{1,i}$ is arithmetically equivalent to $N\prod_i M_{2,i}$.
Let $B_{1,i}$ be the subgroup of $G(M/\mathbb{Q})$ corresponding to $NM_{1,i}$. Since $B_{1,i} \subseteq M_i$, we may also see it as a subgroup of $\mathbb{F}_p[H]u_i$.
Since

$$G(M_{1,i}/K') \cong G(NM_{1,i}/N) \cong G(M_i/N)/G(M_i/NM_{1,i}) \cong \mathbb{F}_p[H]u_i/B_{1,i},$$

they are isomorphic as $S_{1,i}/T_1$-modules, then for any element $s \in S_{1,i}$, we have that $(s-\chi_i(s))\mathbb{F}_p[H]u_i$ is contained in $B_{1,i}$, which means the subgroup

$$C_{1,i} = \sum_{s\in S_{1,i}} (s-\chi_i(s))\mathbb{F}_p[H]u_i$$

is also contained in $B_{1,i}$ as the classes of $s-\chi_i(s)$ are trivial in $G(M_{1,i}/K')$ as by definition the action of $S_{1,i}/T_{1,i}$ on $G(M_{1,i}/K')$ coincides with multiplication by the values of χ_i.
We may also consider the quotient $\mathbb{F}_p[H]u_i/C_{1,i}$, and observe that by construction T_1 acts trivially on it. Thus, the extension of K' corresponding to $C_{1,i}$ corresponds to an abelian p-extension of K' on which $S_{1,i}/T_1$ acts via χ_i, but by maximality this means that this is a subextension of $M_{1,i}/K'$, that is $C_{1,i} \supseteq B_{1,i}$. Since by construction $C_{1,i} \subseteq B_{1,i}$ we have $C_{1,i} = B_{1,i}$. We obtain then that $N\prod_i M_{1,i}$ corresponds to the subgroup generated by all the $(s-\chi_i(s))\mathbb{F}_p[H]u_i$ as s varies in $S_{1,i}$ which we will denote A_1. Notice that

$$A_1 = \sum_{i=1}^{m} B_{1,i}.$$

We may repeat this procedure replacing $M_{1,i}$ with $M_{2,i}$, K' with L', construct groups $B_{2,i}$ for all i analogous to $B_{1,i}$, and we may finally obtain a subgroup $A_2 = \sum_i B_{2,i}$ corresponding to $N\prod_i M_{2,i}$, and analogous to A_1.
We have shown above that $N\prod M_{1,i}$ and $N\prod M_{2,i}$ are arithmetically equivalent, so by the definition it follows that every element of A_1 is conjugate to an element of A_2 by some element of E, and by the split exact sequence the action by conjugation of E of $\mathbb{F}_p[H]$ corresponds to the action by left multiplication of some element $h \in H$ on $\mathbb{F}_p[H]$. That is, $\forall\ a \in A_1$, there exists an element $h \in H$ (depending on a) such that $ha \in A_2$.

Fix now the element

$$a = \sum_{t_1 \in T_1} (t_1 - 1)u_0 + \sum_{i=1}^{m} s_{1,i} - \chi_i(s_{1,i})u_i$$

in A_1. Then, there exists $h \in H$ such that $ha \in A_2$ and in particular it follows that $h\sum_{t_1 \in T_1}(t_1 - 1)u_0$ is an element of $B_{2,0}$, and for all $1 \leq i \leq m$ we also have $h(s_{1,i} - \chi_i(s_{1,i}))u_i$ is an element of $B_{2,i}$. Expanding the first we get

$$h \sum_{t_1 \in T_1} (t_1 - 1) \in \sum_{t_2 \in T_2} (t_2 - 1)\mathbb{F}_p[H]u_0$$

which, using the fact that

$$\sum_{t_2 \in T_2} t_2 \sum_{t_2 \in T_2} (t_2 - 1) = 0 \in \mathbb{F}_p[H]$$

we can rewrite as

$$\sum_{t_2 \in T_2} t_2 h \sum_{t_1 \in T_1} (t_1 - 1) = 0 \in \mathbb{F}_p[H]u_0.$$

Fix an element $t_1' \in T_1$. The coefficient of $ht_1' \in H$ in the sum must be a multiple of p to have zero in $\mathbb{F}_p[H]$. Observe that the number of elements in the sum of the form $t_2''ht_1''$ (also elements of H) is $|H|^2$ which is less than p, and therefore the number of elements $t_2''ht_1'' = ht_1'$ is also less than p. We then get that ht_1' must cancel out with a term of the form $-t_2'h$ for some $t_2' \in T_2$, that is $t_2'h = ht_1'$, and so we get $h^{-1}T_2h \subseteq T_1$, but since T_1 and T_2 have the same order this is really an equality $hT_1h^{-1} = T_2$, therefore h induces an isomorphism between K' and L'. Now, we can expand $h(s_{1,i} - \chi_i(s_{1,i}))u_i \in B_{2,i}$ and for each $i = 1, .., m$ we get

$$h(s_{1,i} - \chi_i(s_{1,i})) \in \sum_{s \in S_{2,i}} (s - \chi_i(s))\mathbb{F}_p[H]u_i$$

which can be rewritten as

$$\sum_{s \in S_{2,i}} s\chi_i(s)^{-1}h(s_{1,i} - \chi_i(s_{1,i})) = 0 \in \mathbb{F}_p[H].$$

By a similar idea to the one used above for ht_1, the coefficient of $hs_{1,i}$ must be 0 and we must have that for some $s' \in S_{2,i}$ we have $hs_{1,i} = s'\chi_i(s'^{-1})h\chi_i(s_{1,i})$, and so $hs_{1,i} = s'h$ and $\chi_i(s') = \chi_i(s_{1,i})$. By the definition of χ_i, it follows $h_{2,i} = s'T_2 = s_{2,i}T_2$. Since $s' = hs_{1,i}h^{-1}$, and we then get $h_{2,i}$ and $hh_{1,i}h^{-1}$ define the same action on L'. In particular, repeating this for all $1 \leq i \leq m$, we get that the action of $h_{1,i}$ conjugated by h coincides with the action of $h_{2,i}$ for all the generators $h_{1,i}$ of H_1. Together with the fact h induces an isomorphism $K' \xrightarrow{\sim} L'$

we obtained above, this gives h is an element of $\mathfrak{A}_{K'}$. Observe that since with this construction h must be an element of H and H is finite, we only have $\mathfrak{A}_{K'}$ is finite. Taking the projective limit of these sets $\mathfrak{A}_{K'}$ as intended, we get that as all of them are non-empty and compact, the projective limit is non-empty ([RZ], Proposition 1.1.4) and the isomorphism τ from the statement does indeed exist. It remains now to prove that τ is unique. Assume there is another isomorphism ρ. Then, the composition $\tau \circ \rho^{-1}$ is an automorphism of $\overline{K}$ which by the construction seen in this proof must map any extension of K to itself, and so must be in the center of G_K. However, by Lemma 1.2.4 the center of G_K is trivial, and so we have that $\tau \circ \rho^{-1}$ is the identity, that is $\tau = \rho$. □

As a closing remark to this chapter, while this was not initially set as a condition of the theorem, the isomorphism τ we obtain automatically restricts to an isomorphism between K and L, as by the condition $\sigma(g) = \tau g \tau^{-1}$ the subfield of $\overline{K}$ fixed by all elements of G_K (that is, K) is mapped by τ to the subfield of $\overline{L}$ fixed by all elements of G_L (that is, L).

Chapter 2

The m-step Isom-Form

In this chapter, we will be looking at Grothendieck's birational anabelian conjectures, and we will also look at a result by Saïdi and Tamagawa [S-T] that proves an m-step formulation of the Isom-Form for number fields. We will then follow this by looking at the characterization given by Saïdi and Tamagawa of particular subgroups of the maximal m-step solvably closed quotient G_K^m of G_K that has been used to obtain this m-step Isom-Form.

2.1 The Isom-Form and the Hom-Form

Neukirch-Uchida's theorem inserts in the greater field of Grothendieck's birational anabelian conjectures. These conjectures follow roughly the idea that a finitely generated infinite field K can be recovered group theoretically from its absolute Galois G_K. We are interested in looking at two of them, the Isom-Form and the Hom-Form.

Theorem 2.1.1 (Birational Anabelian Isom-Form)**.** *Let K and L be two finitely generated infinite fields, and let G_K and G_L be their absolute Galois groups. If one has a continuous isomorphism $\sigma : G_K \to G_L$, there is a unique field isomorphism $\tau : \overline{K} \to \overline{L}$ such that*

$$\tau g \tau^{-1} = \sigma(g)$$

for all $g \in G_K$, and we have the following commutative diagram

$$\begin{array}{ccc} \overline{K} & \xrightarrow[\tau]{\sim} & \overline{L} \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle \sigma(g)} \\ \overline{K} & \xrightarrow[\tau]{\sim} & \overline{L} \end{array}$$

Neukirch-Uchida's theorem proves that this statement holds in the case where K and L are number fields. Further results by Uchida [Uch1] for function fields of curves over finite fields and Pop [Pop] for finitely generated fields of higher transcendence degree complete the proof of the Isom-Form.

The second conjecture, the Hom-Form, is closely related to the first one. In the Hom-Form, the isomorphism of the absolute Galois groups is replaced with an open continuous homomorphism, and the isomorphism of fields is replaced with an embedding $\overline{L} \hookrightarrow \overline{K}$. In the case of number fields the Hom-Form conjecture reads as follows:

Conjecture 2.1.2 (Hom-Form for Number fields)**.** *Let K and L be number fields, and let $\sigma : G_K \to G_L$ be a continuous homomorphism of profinite groups such that $\sigma(G_K)$ is open in G_L. Then, there exists a unique homomorphism of fields $\tau : \overline{L} \to \overline{K}$ such that $\forall g \in G_K$ we have*

$$g\tau = \tau\sigma(g)$$

that is, the following diagram is commutative

$$\begin{array}{ccc} \overline{L} & \xrightarrow{\tau} & \overline{K} \\ \downarrow{\scriptstyle \sigma(g)} & & \downarrow{\scriptstyle g} \\ \overline{L} & \xrightarrow{\tau} & \overline{K} \end{array}$$

Unlike the Isom-Form, this is currently still an open conjecture. There are, however, some partial results. In particular there are a few results by Uchida ([Uch3]):

Theorem 2.1.3 (Uchida, Uniqueness in the Hom-Form)**.** *If there exists a τ as in 2.1.2, then it is unique.*

Theorem 2.1.4 (Uchida's Theorem 1)**.** *Assume that in the statement of Conjecture 2.1.2 $K = \mathbb{Q}$. Then, the conjecture holds true. Furthermore, we have that $L = \mathbb{Q}$, and σ is an isomorphism.*

The following theorem proves a conditional version of the Hom-Form

Theorem 2.1.5 (Uchida's Theorem 2)**.** *Let $\sigma : G_K \to G_L$ be a continuous homomorphism of profinite groups such that for every prime $\mathfrak{p} \in \mathfrak{Primes}_K^{\mathrm{na}}$ there exists a prime $\mathfrak{q} \in \mathfrak{Primes}_L^{\mathrm{na}}$ such that $\sigma(D_\mathfrak{p}) \subseteq D_\mathfrak{q}$, and $\sigma(D_\mathfrak{p})$ is open in $D_\mathfrak{q}$. Then, $\sigma(G_K)$ is open in G_L and there exists a unique homomorphism of fields $\tau : \overline{L} \to \overline{K}$ such that*

$$\tau\sigma(g) = g\tau$$

for all $g \in G_K$.

To prove Theorem 2.1.5 (see [Uch3]), Uchida first puts the local conditions on decomposition groups, and after proving that the conditions he's asking for are enough to establish a local correspondence between the primes of K and the primes of L, he proceeds to construct the homomorphism following roughly the

same idea as the proof of Theorem 1.3.2, showing successfully that τ exists.
It is also interesting to observe that in Neukirch-Uchida's theorem, an analogous result can be obtained by replacing the absolute Galois groups G_K and G_L with their maximal pro-solvable quotients without altering the proof given in Theorem 1.3.2 (see [Uch2]).
In a recent article, Saïdi and Tamagawa [S-T] looked at replacing the full absolute Galois groups G_K and G_L with their maximal m-step solvable quotients G_K^m and G_L^m (see Section 2.2 for notation), and consequently replacing the separable closures $\overline{K}$ and $\overline{L}$ with the maximal m-step abelian extensions K_m and L_m, they obtain a result analogous to Neukirch-Uchida for maximal m-step solvable quotients:

Theorem 2.1.6 (Saïdi-Tamagawa)**.** *Let K and L be number fields, let $m \geq 0$ be an integer and let $\sigma_{m+3} : G_K^{m+3} \to G_L^{m+3}$ be an isomorphism of profinite groups. Consider the induced isomorphism of profinite groups $\sigma_m : G_K^m \to G_L^m$.*
Then, there exists a field isomorphism $\tau_m : K_m \to L_m$ such that

$$\sigma_m(g) = \tau_m g \tau_m^{-1}$$

for all $g \in G_K^m$. That is, $\forall g \in G$ we have a commutative diagram

$$\begin{array}{ccc} \overline{K}_m & \xrightarrow{\sim}_{\tau} & L_m \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle \sigma_m(g)} \\ \overline{K}_m & \xrightarrow{\sim}_{\tau} & L_m \end{array}$$

Furthermore if $m \geq 2$ (resp. $m = 1$), the above isomorphism $\tau_m : K_m \to L_m$ (resp. $\tau : K \to L$ induced by $\tau_1 : K_1 \to L_1$) is uniquely determined by the condition $\sigma_m(g) = \tau_m g \tau_m^{-1}$.
In particular, $\tau_m : K_m \to L_m$ always restricts to a unique isomorphism $K \xrightarrow{\sim} L$.

The proof by Saïdi and Tamagawa works by establishing a local theory for m-step solvable quotients, showing that this local theory induces a correspondence between primes. Then, once the Local Theory has been established, they show the isomorphism $\tau_m; K_m \to L_m$ can be constructed following a similar idea to the one used by Uchida in the proof of Neukirch-Uchida's theorem given in Theorem 1.3.2.

2.2 m-step Local Theory

In this section, we aim to give a few results by Saïdi and Tamagawa on the nature of special subgroups of the maximal m-step solvable quotient of an absolute Galois group necessary to construct a local theory. We will also include some of the

proofs given by Saïdi and Tamagawa for these results, as they are helpful in understanding the structure of decomposition groups in G_K^m and how the main object introduced in this section, $(\star_l)$-subgroups, work.

Let G be a profinite group and let $G[1] = \overline{[G,G]}$ be the closed subgroup of G generated by the commutator subgroup. We may define the derived series

$$G = G[0] \supseteq G[1] \supseteq G[2] \supseteq G[3] \supseteq ...$$

by setting $G[i+1] = \overline{[G[i], G[i]]}$, and we may also define the maximal i-step solvable quotient of G as $G^i = G/G[i]$. We can then define the canonical quotients $G \twoheadrightarrow G^i$, whose kernel is $G[i]$. We may also observe that if $j \geq i \geq 0$, we have $G[j] = (G[i])[j-i]$ and so we also have canonical quotients $G^j \twoheadrightarrow G^i$ with kernel $G[i]^{j-i} = G^j[i]$

If G is the absolute Galois group $G_K = G(\overline{K}/K)$ of a number field K, then, the maximal abelian quotient G_K^{ab} is the Galois group of the maximal abelian extension K^{ab}/K contained in $\overline{K}$, and similarly we define the maximal m-step abelian extension K_m/K as the subextension of $\overline{K}$ determined by the subgroup $G_K[m]$ of G_K, and the quotient G_K^m is the Galois group $G(K_m/K)$.

If we let $\bar{\mathfrak{p}}$ be a prime of K, and $\mathfrak{P}$ be a prime of $\overline{K}$ above it, we can then find the unique prime $\mathfrak{p}$ in K_m below $\mathfrak{P}$. Let $D_{\mathfrak{P}} \subset G_K$ be the decomposition group of $\mathfrak{P}$, and let $D_{\mathfrak{p}} \subseteq G_K^m$ be the decomposition group of $\mathfrak{p}$. Then, the quotient $G_K \twoheadrightarrow G_K^m$ induces a natural surjective homomorphism $D_{\mathfrak{P}} \to D_{\mathfrak{p}}$.

We know that $D_{\mathfrak{p}}$ is m-step solvable as it is a subgroup of G_K^m which is m-step solvable itself, then it follows immediately that this surjective homomorphism must factor through $D_{\mathfrak{P}}^m$, the maximal m-step solvable quotient of $D_{\mathfrak{P}}$. The first result by Saïdi and Tamagawa (see [S-T], Proposition 1.1 for the proof) gives us a few results on the structure of $D_{\mathfrak{p}}$ in relation to $D_{\mathfrak{P}}^m$.

Proposition 2.2.1. *Let $m \geq 0$ be an integer, let $\mathfrak{P}$ be a prime of $\overline{K}$, let $\mathfrak{p}$ be the prime of K_m below it and let $\bar{\mathfrak{p}}$ be their image in K. Let p be their common residue characteristic. Then:*

(i) The natural surjective map $D_{\mathfrak{P}}^m \to D_{\mathfrak{p}}$ is an isomorphism.

(ii) If $m \geq 1$, then $\log_p |D_{\mathfrak{p}}^{\mathrm{ab\,/\,tor}}/pD_{\mathfrak{p}}^{ab/tor}| \geq 2$, p is the unique prime number for which this is true, and $d_{\mathfrak{p}} = \log_p |D_{\mathfrak{p}}^{\mathrm{ab\,/\,tor}}/pD_{\mathfrak{p}}^{\mathrm{ab\,/\,tor}}| - 1$.

(iii) If $m \geq 1$, then $f_{\bar{\mathfrak{p}}} = \log_p(1 + |(D_{\mathfrak{p}}^{\mathrm{ab}})_{\mathrm{tor}}^{(p')}|)$ and $N(\bar{\mathfrak{p}}) = p^{f_{\bar{\mathfrak{p}}}}$

(iv) If $m \geq 1$ the map $D_{\mathfrak{P}} \to D_{\mathfrak{P}}^{\mathrm{ur}}$ factors through $D_{\mathfrak{p}}$.

(v) If $m \geq 2$ the map $D_{\mathfrak{P}} \to D_{\mathfrak{P}}^{\mathrm{tame}}$ factors through $D_{\mathfrak{p}}$ and $\ker(D_{\mathfrak{p}} \twoheadrightarrow D_{\mathfrak{P}}^{\mathrm{tame}})$ is the maximal pro-p subgroup of $D_{\mathfrak{p}}$

(vi) For all integers i such that $m \geq i \geq 2$ the kernel of $D_{\mathfrak{p}} \to D_{\mathfrak{p}}^i$ is pro-p

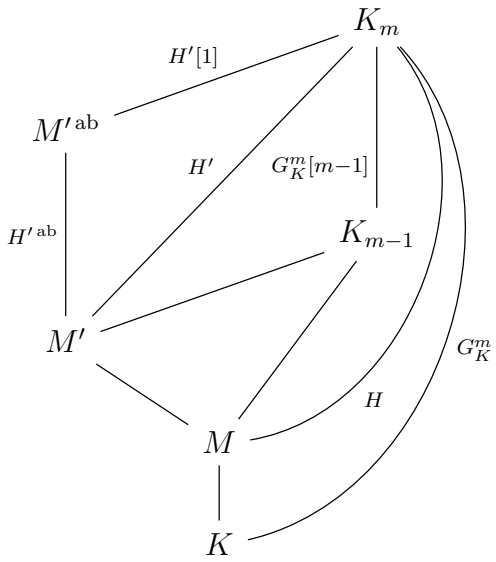
(vii) For all integers i such that $m-1 \geq i \geq 0$ the kernel of $D_{\mathfrak{p}} \to D_{\mathfrak{p}}^i$ is infinite

(viii) If $m \geq 2$, $D_{\mathfrak{p}}$ is centre free and torsion free

We have seen in Neukirch's local theory (Corollary 1.2.3) that two distinct decomposition group in G_K have trivial intersection, that is in a way they are completely separated from each other. In G_K^m, this separatedness property is not true in general, however we have the following result ([S-T], Proposition 1.3).

Proposition 2.2.2. *Let $m \geq 1$ be an integer, and let $\mathfrak{p}, \mathfrak{p}' \in \mathfrak{Primes}_{K_m}^{\mathrm{na}}$, and consider the decomposition groups $D_{\mathfrak{p}}, D_{\mathfrak{p}}' \subset G_K^m$. Furthermore, let $\bar{\mathfrak{p}}, \bar{\mathfrak{p}'}$ be their images in K_{m-1}. Then, $D_{\mathfrak{p}} \cap D_{\mathfrak{p}'} \neq 1 \iff \bar{\mathfrak{p}} = \bar{\mathfrak{p}'}$*

Proof. Assume first $\bar{\mathfrak{p}} = \bar{\mathfrak{p}'}$. Then, $\mathfrak{p}$ and $\mathfrak{p}'$ are conjugate primes above $\bar{\mathfrak{p}}$ and it follows that their decomposition groups are also conjugate in the Galois group of the extension K_m/K_{m-1}. However, $G(K_m/K_{m-1}) = G_K^m[m-1] = G_K[m-1]^{\mathrm{ab}}$ is abelian, therefore it follows $D_{\mathfrak{p}} \cap G_K^m[m-1] = D_{\mathfrak{p}'} \cap G_K^m[m-1]$. Furthermore, by Proposition 2.2.1.(vii), the kernels of the projections $D_{\mathfrak{p}} \to D_{\bar{\mathfrak{p}}}$ and $D_{\mathfrak{p}'} \to D_{\bar{\mathfrak{p}}}$ are infinite, and since these kernels are subgroups of $G_K^m[m-1]$ it follows that the intersections $D_{\mathfrak{p}} \cap G_K^m[m-1] = D_{\mathfrak{p}'} \cap G_K^m[m-1]$ are non-trivial and so $D_{\mathfrak{p}} \cap D_{\mathfrak{p}'} \neq 1$. We now need to show that the converse is also true. First, let us assume $m = 1$. In this case, an application of ([Gras], Corollary 4.16.7, Chapter III) gives us that since $D_{\mathfrak{p}} \cap D_{\mathfrak{p}'}$ is non-trivial, $\mathfrak{p}$ and $\mathfrak{p}'$ are conjugate in the extension K^{ab}/K, that is they are above the same prime $\bar{\mathfrak{p}}$ of K.
Let us now assume $m \geq 2$, and let $F = D_{\mathfrak{p}} \cap D_{\mathfrak{p}'}$. Observe that $D_{\mathfrak{p}}$ and $D_{\mathfrak{p}'}$ are torsion-free by Proposition 2.2.1.(viii) and so F is also torsion-free, and since it is non-trivial by assumption it is infinite. Let M be a finite subextension of K_{m-1}/K, which corresponds to an open subgroup H of G_K^m containing $G_K^m[m-1]$,. By ([S-T], Lemma 1.2) we may take an open subgroup H' of H such that $H' \supseteq G_K^m[m-1]$ and $F \cap H'$ has a non-trivial image in H'^{ab}. We may then take an subextension M' of K_m/K corresponding to H', which must be contained in K_{m-1}, and the subextension M_1' of K_m/K corresponding to $H'[1]$, the kernel of $H' \to H'^{\mathrm{ab}}$. Since $M' \subset K_{m-1}$, the field M_1' is in fact the maximal abelian extension M'^{ab} of M', contained in K_m. The following diagram shows graphically the construction in this proof:



Let $\mathfrak{q}$ and $\mathfrak{q}'$ be the images of $\mathfrak{p}$ and $\mathfrak{p}'$ respectively in M'^{ab}, and consider their decomposition groups $D_{\mathfrak{q}}, D_{\mathfrak{q}'} \subset H'^{\mathrm{ab}}$. We now have $D_{\mathfrak{q}} \cap D_{\mathfrak{q}'}$ contains the image of $F \cap H'$ in H'^{ab}, which is non-trivial, and applying this same proposition for $m = 1$, which was proven earlier, we get the images of $\mathfrak{q}$ and $\mathfrak{q}'$ in M' are the same prime $\bar{\mathfrak{q}}$ of M', and so their images in M must also coincide. Since M was chosen as an arbitrary finite subextension of K_{m-1}/K, it now follows immediately that this also holds for K_{m-1}, otherwise we would have a finite subextension of K_{m-1}/K where this does not hold, and so $\bar{\mathfrak{p}} = \bar{\mathfrak{p}}'$. □

Another consequence of Corollary 1.2.3 is that the naturally defined map associating to a prime of $\overline{K}$ its decomposition group in G_K is invertible, that is we have a bijection $\mathfrak{Primes}_{\overline{K}}^{\mathrm{na}} \xrightarrow{\sim} Dec(\overline{K}/K)$. A result analogous to this for the m-step case was also given by Saïdi and Tamagawa ([S-T], Proposition 1.9). This result is given without proof in the following proposition.

Proposition 2.2.3. *Let K be a number field, $\widetilde{K}$ an infinite extension of K such that $\widetilde{K} \supseteq \mathbb{Q}^{\mathrm{ab}}$ and consider its maximal abelian extension $\widetilde{K}^{\mathrm{ab}}/\widetilde{K}$. Let $\mathfrak{p}, \mathfrak{p} \in \mathfrak{Primes}_{\widetilde{K}^{\mathrm{ab}}}^{\mathrm{na}}$ and consider the decomposition groups $D_{\mathfrak{p}}$ and $D_{\mathfrak{p}'} \subset G(\widetilde{K}^{\mathrm{ab}}/K)$. Then, $D_{\mathfrak{p}} = D_{\mathfrak{p}'} \iff \mathfrak{p} = \mathfrak{p}'$, and the natural map $\mathfrak{Primes}_{\widetilde{K}^{\mathrm{ab}}}^{\mathrm{na}} \to \mathrm{Dec}(\widetilde{K}^{\mathrm{ab}}/K)$ is bijective.*

This result has the following corollaries, which expand the description of the separatedness of decomposition groups in G_K^m given by Proposition 2.2.2

Corollary 2.2.4. *Let $m \geq 2$ and let $\mathfrak{p}, \mathfrak{p}'$ be primes of K_m, and consider the decomposition groups $D_{\mathfrak{p}}, D_{\mathfrak{p}'} \subset G_K^m$. Then, $D_{\mathfrak{p}} = D_{\mathfrak{p}'} \iff \mathfrak{p} = \mathfrak{p}'$.*

Proof. This follows immediately by taking $\widetilde{K} = K_{m-1}$ in the statement of 2.2.3. □

Corollary 2.2.5. *Let $\widetilde{K}$ be an infinite Galois extension of K such that $\widetilde{K}$ contains $\mathbb{Q}^{\mathrm{ab}}$. Then, the centraliser of $G(\widetilde{K}^{\mathrm{ab}}/K)$ in $\mathrm{Aut}(\widetilde{K}^{\mathrm{ab}})$ is trivial, and $G(\widetilde{K}^{\mathrm{ab}}/K)$ is centre free. In particular, for $m \geq 2$, the centraliser of G_K^m in $\mathrm{Aut}(K^m)$ is trivial, and G_K^m is centre free.*

Proof. By definition, the centraliser of $G(\widetilde{K}^{\mathrm{ab}}/K)$ in $\mathrm{Aut}(\tilde{K}^{\mathrm{ab}})$ must act trivially on every decomposition group in $G(\widetilde{K}^{\mathrm{ab}}/K)$. Then, the bijection in Proposition 2.2.3 gives us that the action of the centraliser on the primes of $\widetilde{K}^{\mathrm{ab}}$ is trivial. As there is a natural injective map $\mathrm{Aut}(\widetilde{K}^{\mathrm{ab}}) \to \mathrm{Aut}(\mathfrak{Primes}^{\mathrm{na}}_{\widetilde{K}^{\mathrm{ab}}})$ (cf. [S-T], Lemma 1.8), it follows that since its action is trivial, the centraliser it must be trivial itself, and the first part of the statement follows.
The second part also follows immediately by taking $\widetilde{K} = K_{m-1}$. □

Now that we have an idea for the separatedness of primes in maximal m-step solvable extensions, we require the following definitions, which are fundamental in Saïdi and Tamagawa's construction of a local theory for the m-step case.

Definition 2.2.6. *Let $m \geq 2$ be an integer, $F \subseteq G_K^m$ a closed subgroup, l a prime number and let $\widetilde{F}$ be the inverse image of F in G_K^{m+1}. Then, we say that F has property $(\star_l)$ if it satisfies the following:*

- *There exists an exact sequence $1 \to \mathbb{Z}_l \to F \to \mathbb{Z}_l \to 1$.*
- *The inflation map $\inf_{F,l} : H^2(F, \mathbb{F}_l) \to H^2(\widetilde{F}, \mathbb{F}_l)$ has non-trivial image.*

We will denote the image of the map $\inf_{F,l}$ by $\mathcal{H}^2(F, \mathbb{F}_l)$. We also denote the set of all subgroups of G_K^m satisfying property $(\star_l)$ by $\widetilde{\mathcal{D}}_{m,l,K}$ (or just $\widetilde{\mathcal{D}}_{m,l}$ if there is no need to distinguish between two different fields).

Observe that if $\mathfrak{p}$ is a prime of K_m, and we consider its decomposition group $D_{\mathfrak{p}}$ in G_K^m, we may take an l-Sylow subgroup $D_{\mathfrak{p},l}$. We may also consider the inertia subgroup $I_{\mathfrak{p}} \subseteq D_{\mathfrak{p}}$, and the group $I_{\mathfrak{p},l} = I_{\mathfrak{p}} \cap D_{\mathfrak{p},l}$, which isomorphic to $\mathbb{Z}_l$. We then have a natural exact sequence

$$1 \to I_{p,l} \to D_{\mathfrak{p},l} \to \mathbb{Z}_l \to 1.$$

Definition 2.2.7. *Let F, F' be subgroups of G_K^m satisfying condition $(\star_l)$. We define an equivalence relation $\approx$ on $\widetilde{\mathcal{D}}_{m,l,K}$ by setting that $F \approx F'$ if and only if for any open subgroup $H \subseteq G_K^m$ such that $H \supseteq G_K^m[m-1]$ we have that the images of $F \cap H$ and $F' \cap H$ in H^{ab} are commensurable. We will denote the set of equivalence classes for this relation by $\mathcal{D}_{m,l,K}$ (or $\mathcal{D}_{m,l}$ if there is no need to distinguish between two different fields).*

These definitions are purely group-theoretic, and allow us to recover the set $\mathcal{D}_{m,l,K}$ of all subgroups of G_K^m satisfying property $(\star_l)$ starting from G_K^{m+1}. Furthermore, the following propositions (Proposition 1.22 and Proposition 1.23 in [S-T]) give us a strong connection between $(\star_l)$-subgroups and the decomposition groups in G_K^m.

Proposition 2.2.8. *Let $m \geq 2$, $F \subseteq G_K^m$ a closed subgroup and let l be a prime number. Let $\mathfrak{p}$ be a non-archimedean prime of K_m with residue characteristic $p \neq l$, and let $D_\mathfrak{p} \subseteq G_K^m$ be its decomposition group. Consider an l-Sylow subgroup $D_{\mathfrak{p},l}$ of $D_\mathfrak{p}$. Then, if F is an open subgroup of $D_{\mathfrak{p},l}$, we have F satisfies condition $(\star_l)$.*
Vice versa, if F satisfies condition $(\star_l)$ there exists a (not necessarily unique) non-archimedean prime $\mathfrak{p}$ (with the same properties as above) such that F is an open subgroup of $D_{\mathfrak{p},l}$. Furthermore, the prime $\bar{\mathfrak{p}}$ of K_{m-1} below $\mathfrak{p}$, is uniquely determined by F.

Proof. Let $\mathfrak{p}$ be a prime of K_m, let $D_\mathfrak{p}$ its decomposition group in K_m/K, and let l be a prime number different from the residue characteristic of $\mathfrak{p}$. Let us take an open subgroup F of $D_{\mathfrak{p},l}$. By Proposition 2.2.1.(v), for any $\mathfrak{P}$ in $\overline{K}$ above $\mathfrak{p}$, F is mapped isomorphically to its image F' in $D_\mathfrak{P}^{\text{tame}}$ as the kernel of $D_\mathfrak{p} \to D_\mathfrak{P}^{\text{tame}}$ is pro-p. It also follows that the l-group F' is open in some l-Sylow of $D_\mathfrak{P}^{\text{tame}}$, as by definition of $I_\mathfrak{P}^{\text{tame}}$ there is an exact sequence

$$0 \to I_\mathfrak{P}^{\text{tame}} \to D_\mathfrak{P}^{\text{tame}} \to D_\mathfrak{P}^{\text{ur}} \to 0$$

with $I_\mathfrak{P}^{\text{tame}} \cong \widehat{\mathbb{Z}}^{(p')}$ and $D_\mathfrak{P}^{\text{ur}} \cong \widehat{\mathbb{Z}}$. As F' is open in $D_\mathfrak{P}^{\text{tame}}$, and the open subgroups of $\mathbb{Z}_l$ are isomorphic to $\mathbb{Z}_l$ itself, F' fits in an exact sequence

$$0 \to \mathbb{Z}_l \to F' \to \mathbb{Z}_l \to 0$$

given by the exact sequence above, which means F also does as $F \cong F'$.
Let then F_0 be a closed subgroup of $D_\mathfrak{P}$ mapped isomorphically to F by the surjection $D_\mathfrak{P} \to D_\mathfrak{p}$, which exists by 2.2.1.(v), and let $\widehat{F}$ be the inverse of F with respect to the surjection $G_K \twoheadrightarrow G_K^m$.
The isomorphism $F_0 \xrightarrow{\sim} F$ naturally induces an isomorphism between cohomology groups $H^2(F, \mathbb{F}_l) \xrightarrow{\sim} H^2(F_0, \mathbb{F}_l)$. Furthermore, since we have a natural injection $F_0 \hookrightarrow \widehat{F}$, we can factor this isomorphism between the cohomology groups through the inflation map $H^2(F, \mathbb{F}_l) \to H^2(\widehat{F}, \mathbb{F}_l)$, and the restriction map $H^2(\widehat{F}, \mathbb{F}_l) \to H^2(F_0, \mathbb{F}_l)$. As $H^2(F, \mathbb{F}_l)$ is non-trivial, then the isomorphism $H^2(F, \mathbb{F}_l) \xrightarrow{\sim} H^2(F_0, \mathbb{F}_l)$ has non-trivial image. Then, it follows the inflation map $H^2(F, \mathbb{F}_l) \to H^2(\widehat{F}, \mathbb{F}_l)$ must also have non-trivial image.
Furthermore, this inflation map must factor through $H^2(\widetilde{F}, \mathbb{F}_l)$ where $\widetilde{F}$ is the

inverse image of F by the quotient $G_K^{m+1} \twoheadrightarrow G_K^m$. It then follows that the inflation map $\inf_{F,l} : H^2(F, \mathbb{F}_l) \to H^2(\widetilde{F}, \mathbb{F}_l)$ has non-trivial image, as desired, and F satisfies property $(\star_l)$.

We now want to prove the converse statement, so assume F satisfies condition $(\star_l)$, and let K' be the subextension of K_m/K corresponding to F, and let $\widehat{F}$ be defined as above. First, we can show K' is totally imaginary. Assume by contradiction there exists a real embedding $K' \hookrightarrow \mathbb{R}$, which must extend to an embedding $K_m \to \mathbb{C}$. These embeddings determine a homomorphism $G(\mathbb{C}/\mathbb{R}) \to G_K^m$, which is injective as $K(\sqrt{-1})/K$ is an abelian extension of K (possibly trivial), and so $K_m \supseteq \mathbb{Q}(\sqrt{-1})$. However, this implies F contains torsion elements, which contradicts the definition of property $(\star_l)$ (Definition 2.2.6).

It now follows by ([S-T], Proposition 1.17) that

$$\mathcal{H}^2(F, \mathbb{F}_l) \hookrightarrow \prod_{\tilde{\mathfrak{p}}} H^2(\widehat{F}_{\tilde{\mathfrak{p}}}, \mathbb{F}_l),$$

where $\tilde{\mathfrak{p}}$ ranges over all non-archimedean primes of K', is injective (see Definition 2.2.6 for the definition of $\mathcal{H}^2(F, \mathbb{F}_l)$). Since by definition of property $(\star_l)$, the group $\mathcal{H}^2(F, \mathbb{F}_l)$ is non-trivial and the map is injective, at least one of the $H^2(\widehat{F}_{\tilde{\mathfrak{p}}}, \mathbb{F}_l)$ will also be non-trivial. Fix then $\tilde{\mathfrak{p}}$ for which $H^2(\widehat{F}_{\tilde{\mathfrak{p}}}, \mathbb{F}_l)$ is non-trivial.

Now, the image $F_{\tilde{\mathfrak{p}}}$ of $\widehat{F}_{\tilde{\mathfrak{p}}}$ in G_K^m is the closed subgroup of F corresponding to the decomposition group of $\tilde{\mathfrak{p}}$ in $G(K_m/K')$, and the image of the restriction map $H^2(F, \mathbb{F}_l) \to H^2(F_{\tilde{\mathfrak{p}}}, \mathbb{F}_l)$ is non-trivial. We may use ([S-T], Lemma 1.19) to show that $F_{\tilde{\mathfrak{p}}} = F$.

Furthermore, since $H^2(\widehat{F}_{\tilde{\mathfrak{p}}}, \mathbb{F}_l)$ is non-trivial, by ([S-T], Corollary 1.15) $\widehat{F}_{\tilde{p}}$ is l-open in the decomposition group of $p = char(\tilde{\mathfrak{p}})$ in $G_{\mathbb{Q}}$. Let $\mathfrak{p}$ be the prime of K below $\tilde{\mathfrak{p}}$. It now follows that the image of $\widehat{F}_{\tilde{\mathfrak{p}}}$ in G_K^m is l-open in $D_{\mathfrak{p}} \subset G_K^m$. However we know this image is $F_{\tilde{\mathfrak{p}}} = F$.

Assume now F is contained in more than a decomposition group in G_K^m. By Proposition 2.2.2, the intersection of these decomposition groups is non-trivial, as it contains F, and so there is a unique prime $\bar{\mathfrak{p}}$ in K_{m-1} below all the primes of K_m whose decomposition group contains F. This shows F determines the prime $\bar{\mathfrak{p}}$ uniquely.

It only remains to show $l \neq char(\mathfrak{p})$. Let H' be an open subgroup of $D_{\mathfrak{p}}$ containing $D_{\mathfrak{p}}[1]$. Then, H' corresponds to a finite abelian extension L of $K_{\mathfrak{p}}$ such that the extension $L/\mathbb{Q}_{\mathfrak{p}}$ is non-trivial, and $F \cap H'$ is l-open in H'. The natural map

$$F \cap H'^{\mathrm{ab}} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \to H'^{\mathrm{ab}} \otimes_{\hat{\mathbb{Z}}} \mathbb{Q}_l$$

then needs to be surjective, and using again ([S-T], Lemma 1.19) there is an exact sequence $1 \to \mathbb{Z}_l \to F \cap H' \to \mathbb{Z}_l \to 1$, which means $F \cap H'^{\mathrm{ab}} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$.

By local class field theory, $\mathrm{cd}(H'^{\mathrm{ab}} \otimes_{\hat{\mathbb{Z}}} \mathbb{Q}_l) = 1$ when $l \neq p$, and since $[L : \mathbb{Q}_p] > 1$, we get a contradiction when $l = p$ as $[L : \mathbb{Q}_p] + 1 > 2 \geq F \cap H'^{\mathrm{ab}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, and so may conclude $l \neq char(\mathfrak{p})$. □

In particular, the above result gives us that l-Sylow subgroups of decomposition groups satisfy property $(\star_l)$.

Proposition 2.2.9. *Let K be a number field, and G_K^{m+1} its maximal $(m+1)$-step solvable Galois group. Then, starting from G_K^{m+1} we can recover the following:*

(i) There is a natural injective map $\phi_{m,l} : \mathcal{D}_{m,l} \hookrightarrow \mathfrak{Primes}^{\mathrm{na}}_{K_{m-1}}$

(ii) $\phi_{m,l}$ restricts to a bijective map $\mathcal{D}_{m,l} \xrightarrow{\sim} \mathfrak{Primes}^{\mathrm{na},(l')}_{K_{m-1}}$

(iii) The map $\phi_{m,l}$ is G_K^m-equivariant with respect to the actions of G_K^m on $\mathcal{D}_{m,l}$ and $\mathfrak{Primes}^{\mathrm{na}}_{K_{m-1}}$. In particular, the action of G_K^m on $\mathcal{D}_{m,l}$ factors through G_K^{m-1}. Furthermore, if we let $a \in D_{m,l}$ and $\bar{\mathfrak{p}} = \phi_{m,l}(a)$, the stabiliser of a in G_K^{m-1} is the decomposition group $D_{\bar{\mathfrak{p}}}$.

Proof. By 2.2.8, we can construct a surjective map $\tilde{\phi}_{m,l} : \widetilde{\mathcal{D}}_{m,l} \twoheadrightarrow \mathfrak{Primes}^{\mathrm{na},(l')}_{K_{m-1}}$ by mapping a subgroup $F \subset G_K^m$ satisfying property $(\star_l)$ to the unique prime $\bar{\mathfrak{p}}$ it determines in K_{m-1}. The first thing we want to show is that this map is compatible with the equivalence relation $\approx$, and so we may factor the map through $\mathcal{D}_{m,l}$.
Let F and F' be subgroups of G_K^m satisfying property $(\star_l)$, and let $\mathfrak{p}$ and $\mathfrak{p}'$ be primes of K_m such that F is an open subgroup of $D_{\mathfrak{p},l}$ and F' is an open subgroup of $D_{\mathfrak{p}',l}$. Also, let H be an open subgroup of G_K^m that contains $G_K^m[m-1]$. Let then K' be the subextension of K_m/K corresponding to H and finally let let $\bar{\mathfrak{p}}$ and $\bar{\mathfrak{p}}'$ be the primes of K_{m-1} below $\mathfrak{p}$ and $\mathfrak{p}'$ respectively. Observe that since by definition H contains $G_K^m[m-1]$, K' is a subfield of K_{m-1}, and therefore the maximal abelian extension K'^{ab} of K' in $\overline{K}$ is contained in K_m.
First, we want to show that if F' also satisfies $(\star_l)$ and $F \approx F'$ as in Definition 2.2.7, then the image of F' by $\tilde{\phi}_{m,l}$ is $\bar{\mathfrak{p}}$. By definition of $\approx$, the images of $F \cap H$ and $F' \cap H$ in H^{ab} are commensurable. Furthermore, since K' is contained in K_{m-1}, its maximal abelian extension K'^{ab} is contained in K_m and so we have $H^{\mathrm{ab}} \cong G^{\mathrm{ab}}_{K'}$.
In particular if we let $\tilde{\mathfrak{p}}$ and $\tilde{\mathfrak{p}}'$ be the primes of K' below $\mathfrak{p}$ and $\mathfrak{p}'$, and consider the decomposition groups $D_{\tilde{\mathfrak{p}}}$ and $D_{\tilde{\mathfrak{p}}'}$ in $G^{\mathrm{ab}}_{K'}$, they are l-commensurable, and therefore their intersection is infinite. It now follows by Corollary 2.2.4 that $\tilde{\mathfrak{p}} = \tilde{\mathfrak{p}}'$, and since K' was an arbitrary finite subextension of K_{m-1}/K, we may extend this to K_{m-1} and get $\bar{\mathfrak{p}} = \bar{\mathfrak{p}}'$. It then follows that $\tilde{\phi}_{m,l}$ factors through $\mathcal{D}_{m,l}$.
Now, we want to show injectivity. With the same notation as before, assume that $\tilde{\phi}_{m,l}(F) = \tilde{\phi}_{m,l}(F')$, and denote by $\bar{\mathfrak{p}} \in \mathfrak{Primes}^{\mathrm{na}}_{K_{m-1}}$ their image by $\tilde{\phi}_{m,l}$. We then want to show $F \approx F'$.

Let $\tilde{p}$ be the image of $\bar{p}$ in K'. The images of $F \cap H$ and $F' \cap H$ in $H^{\mathrm{ab}} = G_{K'}^{\mathrm{ab}}$ are both open subgroups of the l-Sylow subgroup $D_{\tilde{\mathfrak{p}},l}$ of the decomposition group $D_{\tilde{\mathfrak{p}}} \subset G_{K'}^{\mathrm{ab}}$, and so their intersection must be open in both of them, that is they are commensurable and $F \approx F'$, and this proves the first assertion.
We may now take for any prime $\bar{\mathfrak{q}}$ of K_{m-1} with residue characteristic different from l, a prime $\mathfrak{q}$ of K_m above it, its decomposition group $D_{\mathfrak{q}} \subset G_K^m$, and an l-Sylow of $D_{\mathfrak{q}}$, which satisfies property $(\star_l)$. Then, by definition, the image of the l-Sylow subgroup by $\tilde{\phi}$ must be $\bar{\mathfrak{q}}$, and ,together with the injectivity that follows from the first assertion, we obtain the second assertion.
Furthermore, we have that G_K^m acts by conjugation on $\widetilde{\mathcal{D}}_{m,l}$, and the map $\tilde{\phi}_{m,l}$ is G_K^m-equivariant, and since the action of G_K^m on $\mathfrak{Primes}_{K_{m-1}}^{\mathrm{na}}$ factors through G_K^{m-1}, the action on $\widetilde{\mathcal{D}}_{m,l}$, so the action on $\mathcal{D}_{m,l}$ also does, and the last assertion in the proposition follows immediately. □

We are now able to give a characterisation for the decomposition groups in G_K^m by "losing" 2 abelian steps of information as follows:

Corollary 2.2.10. *Let $m \geq 2$. For each prime $\mathfrak{p}$ of K_m, starting from G_K^{m+2} we can recover $D_{\mathfrak{p}} \subset G_K^m$ group theoretically. In particular, we can recover from G_K^{m+2} the set $\mathrm{Dec}(K_m/K)$ of all decomposition groups in the extension K_m/K.*

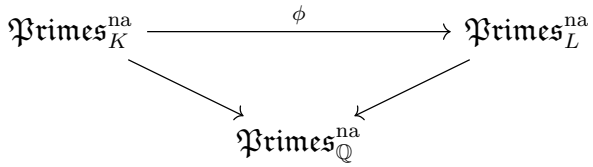
Proof. By Definition 2.2.6, starting from G_K^{m+2}, we can recover the $(\star_l)$ groups in G_K^{m+1}. Then, combining Proposition 2.2.8 and Proposition 2.2.9 we can recover the set $\mathrm{Dec}(K_m/K)$ of all decomposition group in G_K^m. □

Finally, Saïdi and Tamagawa obtain the following local correspondence ([S-T], Corollary 1.27)

Proposition 2.2.11. *Let $m \geq 2$ be an integer, let K and L be number fields and let $\sigma_{m+2} : G_K^{m+2} \xrightarrow{\sim} G_L^{m+2}$ be an isomorphism of profinite groups. Consider the induced isomorphism of profinite groups $\sigma_m : G_K^m \xrightarrow{\sim} G_L^m$. Then, there exists a unique bijection $\phi_m : \mathfrak{Primes}_{K_m}^{\mathrm{na}} \to \mathfrak{Primes}_{L_m}^{\mathrm{na}}$ such that the following diagram, where the vertical arrows are the natural bijections given by Corollary 2.2.4 and for any decomposition group $D \subseteq G_K^m$, $\bar{\sigma}_m(D) = \sigma_m(D)$, is commutative and is Galois equivariant.*

$$\begin{array}{ccc} \mathrm{Dec}(K_m/K) & \xrightarrow{\bar{\sigma}_m} & \mathrm{Dec}(L_m/L) \\ \uparrow & & \uparrow \\ \mathfrak{Primes}_{K_m}^{\mathrm{na}} & \xrightarrow{\phi_m} & \mathfrak{Primes}_{L_m}^{\mathrm{na}} \end{array}$$

Furthermore, ϕ_m induces a bijection $\phi : \mathfrak{Primes}_K^{\mathrm{na}} \to \mathfrak{Primes}_L^{\mathrm{na}}$ fitting in a commutative diagram



where the maps from $\mathfrak{Primes}_K^{\mathrm{na}}$ *and* $\mathfrak{Primes}_L^{\mathrm{na}}$ *to* $\mathfrak{Primes}_{\mathbb{Q}}^{\mathrm{na}}$ *are given by taking the residue characteristic of a prime.*

With this last result, the proof of Theorem 2.1.6 can be obtained by following the same idea of proof as in Theorem 1.3.2, where the field isomorphism is constructed at K_m starting from G_K^{m+3} as losing an extra step is required to define the extensions $M_{1,i}$ and $M_{2,i}$ as in the proof presented in Theorem 1.3.2.

Chapter 3

The m-step birational anabelian Hom-Form

In this chapter, we will be proving conditional result for the Hom-Form in the m-step solvable case. First, we aim to establish a local correspondence, then we will be showing that under some conditions, we have existence and uniqueness in an m-step solvably closed variation of the Grothendieck anabelian Hom-Form conjecture for number fields.

3.1 Local correspondence in the m-step homomorphism of birational anabelian geometry

In the previous chapter we have given the method determined by Saïdi and Tamagawa to recover decomposition groups in m-step solvable extension, and observed how they were able to use it to establish a local theory and a local correspondence in the m-step version of the Isom-Form. In this section we will observe how we can define a partial local correspondence between the primes of two number fields K and L starting from a homomorphism of profinite groups $\sigma_m : G_K^m \to G_L^m$ such that the image of $\sigma_m(G_K^m)$ is an open subgroup of G_L^m.

Let us first fix some notation. For a homomorphism $\sigma_m : G_K^m \to G_L^m$ (not necessarily with open image) we will denote the extension of L corresponding to $\sigma_m(G_K^m)$ by $\widetilde{L}$, and the subfield of K_m corresponding to $\ker(\sigma_m)$ by Λ. We can immediately observe that σ_m induces an isomorphism $G(\Lambda/K) \cong G(L_m/\widetilde{L})$. We then have the following factorization for σ_m.

$$\begin{array}{ccc} G_K^m & \xrightarrow{\sigma_m} & G_L^m \\ \downarrow & & \uparrow \\ G(\Lambda/K) & \xrightarrow{\sim} & G(L_m/\tilde{L}) \end{array}$$

The following proposition gives us that the homomorphism σ_m naturally induces a homomorphism $\sigma_{m-1} : G_K^{m-1} \to G_L^{m-1}$.

Proposition 3.1.1. *Let $m, n \geq 1$ be integers such that $m > n$, and let $\sigma : G_K^m \to G_L^n$ be a homomorphism of profinite groups Then, there is a naturally induced homomorphism $\sigma_n : G_K^n \to G_L^n$ such that σ factors through σ_n, as in the following diagram, where the vertical arrows is the canonical quotient*

$$\begin{array}{ccc} G_K^m & & \\ \downarrow & \searrow^{\sigma} & \\ G_K^n & \xrightarrow{\sigma_n} & G_L^n \end{array}$$

In particular, if we have $n = m - 1$, a homomorphism of profinite groups $\sigma_m : G_K^m \to G_L^m$ and consider its composition with the canonical quotient $G_L^m \to G_L^{m-1}$, we have there exists a naturally induced homomorphism $\sigma_{m-1} : G_K^{m-1} \to G_L^{m-1}$ such that the following diagram commutes

$$\begin{array}{ccc} G_K^m & \xrightarrow{\sigma_m} & G_L^m \\ \downarrow & & \downarrow \\ G_K^{m-1} & \xrightarrow{\sigma_{m-1}} & G_L^{m-1} \end{array}$$

Furthermore, if $\sigma(G_K^m)$ is open in G_L^m, $\sigma_{m-1}(G_K^{m-1})$ is also open in G_L^{m-1}.

Proof. The kernel of the projection $G_K^m \twoheadrightarrow G_K^n$ is by definition the subgroup $G_K^m[n] \subseteq G_K^m$. It follows naturally that $\sigma(G_K^m[n]) \subseteq G_L^n[n]$, which is trivial. This gives us the kernel of the quotient $G_K^m \twoheadrightarrow G_K^n$ is contained in the kernel of σ. We are then able to induce the map σ_n canonically as desired.
The second assertion follows from the first, together with the observation that $\sigma_m(G_K^m[m-1]) \subseteq G_L^m[m-1]$ and so the kernel of the left vertical arrow is mapped to the kernel of the right vertical arrow.
The last assertion in the statement follows as the projection $G_L^m \twoheadrightarrow G_L^{m-1}$ maps the subgroup $G(L_m/\widetilde{L})$ of G_L^m to the subgroup $G(L_{m-1}/(L_{m-1} \cap \widetilde{L})$ of G_L^{m-1}, and $L_{m-1} \cap \widetilde{L}$ is necessarily a finite degree extension of L. Therefore by commutativity of the diagram if the image of σ_m is open in G_L^m the image of σ_{m-1} is also open in G_L^{m-1}. □

If we start with $m < n$, and a map $\sigma : G_K^m \to G_L^n$, we can take the composition of σ with the canonical projection $G_L^n \to G_L^m$ to obtain a map $\sigma_m : G_K^m \to G_L^m$. It also follows like in the proof of Proposition 3.1.1 that $G_K^m[m-1]$ is mapped into $G_L^n[m-1]$ and we can induce starting from σ a homomorphism $\sigma_{m-1} : G_K^{m-1} \to G_L^{m-1}$.

Proposition 3.1.2. *Let $n > 1$ be an integer. Then, there is no homomorphism of profinite groups $\sigma : G_K^{\mathrm{ab}} \to G_L^n$ with open image.*

Proof. Assume such a σ exists. Then, a composition of σ with the canonical quotient $G_L^n \to G_L^2$, gives us a homomorphism of profinite groups $G_K^{\mathrm{ab}} \to G_L^2$, which has open image as the quotient map is an open map. We may then restrict ourselves to studying the case where $n = 2$.
The subgroup of G_L^2 corresponding to the image of σ is also given as the Galois group $G' = G(L_2/\widetilde{L})$, which must be abelian as G_K^{ab} is. Up to replacing it with its normal closure, we may assume G' is a normal subgroup of G_L^2. We may then take the quotient $H = G(\widetilde{L}/L) = G_L^m/G'$, and consider its maximal abelian quotient H^{ab}. Since the kernel of $G_L^2 \twoheadrightarrow H$ is the abelian group $G(L_2/\widetilde{L})$, and the kernel $H[1]$ of $H \twoheadrightarrow H^{\mathrm{ab}}$ is finite as H is finite, the kernel of the composite $G_L^2 \twoheadrightarrow H^{\mathrm{ab}}$ will be an extension of $H[1]$ by a finite group F_0, and we will denote this kernel by F. Furthermore, since H^{ab} is the maximal abelian quotient, $G_L^2 \twoheadrightarrow H^{\mathrm{ab}}$ must factor through G_L^{ab}. As we can obtain G_L^2 an extension of G_L^{ab} by $G_L^2[1]$. We then get a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G_L^2[1] & \longrightarrow & G_L^2 & \longrightarrow & G_L^{\mathrm{ab}} & \longrightarrow & 0 \\ & & \downarrow & & \| & & \downarrow & & \\ 0 & \longrightarrow & F & \longrightarrow & G_L^2 & \longrightarrow & H^{\mathrm{ab}} & \longrightarrow & 0 \end{array}$$

where the rows are short exact sequences, and $G_L^2[1]$ must map injectively to F.
Let l be a prime number. Since $\widetilde{L}$ is a finite extension of $\mathbb{Q}$, its maximal abelian extension has finite $\mathbb{Z}_l$-rank (cf. [NSW], Proposition 10.3.20), and since F is abelian, it corresponds to a quotient of $G_{\widetilde{L}}^{\mathrm{ab}}$. It follows then F also has finite $\mathbb{Z}_l$-rank.
However, for every finite subextension L' of L^{ab}/L, the maximal abelian extension of L' in $\overline{L}$ is a subextension of L_2/L^{ab}. Let us observe that the $\mathbb{Z}_l$-rank s of ${L'}^{\mathrm{ab}}/L'$ increases with the degree of L', and in particular s increases with the degree $[L' : \mathbb{Q}]$.
We may then see the group $G_L^2[1] = G(L_2/L^{\mathrm{ab}})$ as the inverse limit of all the $G({L'}^{\mathrm{ab}}/L')$, and by the above argument $G_L^2[1]$ has infinite $\mathbb{Z}_l$-rank. Since $H[1]$ is finite and F has finite $\mathbb{Z}_l$-rank, we get a contradiction as we can not have the required injective map $G_L^2[1] \hookrightarrow F$.
We may then conclude as desired that there is no homomorphism of profinite groups $G_K^{\mathrm{ab}} \to G_L^2$ with open image. □

Corollary 3.1.3. *A homomorphism of profinite groups $\sigma : G_K^2 \to G_L^2$ with open image does not factor through G_K^{ab}.*

Proof. The statement follows immediately from the statement of Proposition 3.1.2 □

Corollary 3.1.4. *Let m and n be positive integers, and let $\sigma : G_K^m \to G_L^n$ be a homomorphism of profinite groups with open image. Then, there exists a positive integer $m' \leq min(m,n)$ such that a homomorphism $\sigma_{m'} : G_K^{m'} \to G_L^{m'}$ can be induced from σ, and $\sigma_{m'}$ does not factor through $G_K^{m'-1}$.*

Proof. If $m = 1$, then necessarily $\sigma : G_K^{\mathrm{ab}} \to G_L^n$ can not factor through the trivial group as it has open image, and composing with the quotient $G_L^n \twoheadrightarrow G_L^{\mathrm{ab}}$ we get a homomorphism $\sigma_1 : G_K^{\mathrm{ab}} \to G_L^{\mathrm{ab}}$. In this case, $m' = 1$.
If $n = 1$, we can induce a homomorphism $\sigma_1 : G_K^{\mathrm{ab}} \to G_L^{\mathrm{ab}}$ from σ which like in the previous case does not factor through the trivial group.In this case, $m' = 1$
If $m, n \geq 2$, then we can take the induced morphism $\sigma_2 : G_K^2 \to G_L^2$ and by Corollary 3.1.3 this will not factor through G_K^{ab}. In this case, $m' = 2$ (it is possible that for some $m' > 2$ the statement also holds). □

We are now interested in constructing a map between sets of primes starting from $\sigma_m : G_K^m \to G_L^m$ (not necessarily open) as Saïdi and Tamagawa do in Proposition 2.2.11. Our goal is to define a map θ_m from a subset of $\mathfrak{Primes}_{K_m}^{\mathrm{na}}$ to a subset of $\mathfrak{Primes}_{L_m}^{\mathrm{na}}$ starting from σ_m and $(\star_l)$-subgroups at some level m. A priori, we do not know if this map will be defined for every prime $\mathfrak{p}$ of K_m, so we will denote by P_m the subset of $\mathfrak{Primes}_{K_m}^{\mathrm{na}}$ of all the primes for which θ_m is defined, and we get

$$\theta_m : P_m \to \mathfrak{Primes}_{L_m}^{\mathrm{na}}$$

. It is useful to recall the possible continuous images of subgroups satisfying property $(\star_l)$, which we use as following:

Proposition 3.1.5. *Let $m \geq 2$ be an integer. Consider the profinite group G_K^m, let G be a profinite group, and let $\sigma : G_K^m \to G$ be a homomorphism of profinite groups. Let F be a subgroup of G_K^m satisfying property $(\star_l)$. Recall that we have an exact sequence*

$$1 \to \mathbb{Z}_l \to F \to \mathbb{Z}_l \to 1,$$

and let us denote by $U_1 \cong \mathbb{Z}_l$ the subgroup of F appearing on the left in the exact sequence, and by U_2 the quotient F/U_1.
Then, exactly one of the following is true:

(i) $\mathrm{cd}(\sigma(F) = 2$, *and σ restricts to an injection on F.*

(ii) $cd(\sigma(F)) \leq 1$. *In this case either*

- *(a)* $F \subseteq \ker(\sigma)$ *and $\sigma(F)$ is trivial*
- *(b)* $\sigma(F) \cong \mathbb{Z}_l$ *and* $F \cap \ker(\sigma) = U_l$.

(iii) $\sigma(F)$ *contains an l-torsion element. In this case either:*

(a) $\sigma(F)$ *is a finite non-trivial quotient of* $\mathbb{Z}_l$.

(b) $\sigma(F)$ *fits in an exact sequence* $1 \to F_1 \to \sigma(F) \to \mathbb{Z}_l \to 1$, *where* F_1 *is a finite non-trivial quotient of* $\mathbb{Z}_l$ *given by the image of* U_1.

(c) $\sigma(F)$ *fits in an exact sequence* $1 \to F_1 \to \sigma(F) \to F_2 \to 1$ *where* F_1 *and* F_2 *are finite (non-trivial) quotients of* $\mathbb{Z}_l$. *In particular* $\sigma(F)$ *is metabelian.*

Proof. Let us denote by V the normal closed subgroup of F which is the kernel of the map $F \to \sigma(F)$. Observe that by ([S-T], Lemma 1.19, (iv) $\iff$ (viii)) any non-trivial closed subgroup of F is either open in F (and of cohomological dimension 2) or of cohomological dimension 1. Furthermore, all normal subgroups of F which are isomorphic to $\mathbb{Z}_l$ are open subgroups of U_1, and it then follows that if V is non-trivial, then $V' = V \cap U_1$ must also be non-trivial and must contain an open subgroup of U_1. Observe that, furthermore, this gives that U_2 is the maximal abelian quotient of F.
From the above discussion, it also follows that if V' is trivial, then V is trivial and σ restricts to an injection on F, and so we get case (i).
If $V = F$, we naturally have $\sigma(F)$ is trivial, and so we are in case (ii)a.
Assume now V is proper and non-trivial. Then, by the above discussion, it follows that V' is also non-trivial. Let us assume first that $V' = U_1$. Then, the restriction of σ to F factors through the quotient $F \twoheadrightarrow U_2$, that is $\sigma(F)$ is a quotient of $\mathbb{Z}_l$, which must be either $\mathbb{Z}_l$ itself, and we are in case (ii)b, or a finite non-trivial quotient of $\mathbb{Z}_l$, and so we are in case (iii)a.
It remains to study what happens when V' is proper and open in U_1. Trivially, $\sigma(F)$ contains $\sigma(U_1) \cong \mathbb{Z}_l/V'$, which is a torsion group and so we are in case (iii). Observe now that if $cd(V) = 1$, then $V' = V$, which gives us (iii)b as $\sigma(F)$ fits in the exact sequence $1 \to \mathbb{Z}_l/V' \to \sigma(F) \to \mathbb{Z}_l \to 1$. If, instead, $\mathrm{cd}(V) = 2$ and so V is open in F. Then, the quotient F/V is finite, and $\sigma(F)$ contains the finite group $\sigma(U_1)$. In particular, we have an exact sequence $1 \to \sigma(U_1) \to F \to F_2$, which we obtain pushing $1 \to U_1 \to F \to U_2 \to 1$ by σ. Observe that F_2 can not be trivial, otherwise $\sigma(F)$ would be abelian, that is $\sigma_{|F}$ factors through $F \twoheadrightarrow U_2$, and $V' = U_1$, which is a contradiction. This finally gives us we get case (iii)c. □

Corollary 3.1.6. *Let* $m \geq 2$, *and consider the canonical quotient* $G_K^{m+1} \twoheadrightarrow G_K^m$. *Consider a subgroup* $F \subset G_K^{m+1}$ *satisfying property* $(\star_l)$, *and its image* $\overline{F}$ *in* G_K^m. *Then,* $\overline{F}$ *also satisfies property* $(\star_l)$ *and the quotient induces an isomorphism between* F *and* $\overline{F}$.

Proof. By Proposition 2.2.8, there exists a prime $\mathfrak{p}$ in K_{m+1} with decomposition group $D_\mathfrak{p} \subseteq G_K^{m+1}$ (such a prime $\mathfrak{p}$ is not necessarily unique) such that F is an open subgroup of an l-Sylow subgroup $D_{\mathfrak{p},l}$ of $D_\mathfrak{p}$. Let $\bar{\mathfrak{p}}$ be the unique prime of

K_m below $\mathfrak{p}$, with decomposition group $D_{\mathfrak{p}} \subset G_K^m$, and observe that the quotient $G_K^{m+1} \twoheadrightarrow G_K^m$ naturally induces a surjective map $D_{\mathfrak{p}} \twoheadrightarrow D_{\bar{\mathfrak{p}}}$. Then, the l-Sylow subgroup $D_{\mathfrak{p},l}$ is mapped surjectively onto an l-Sylow subgroup of $D_{\bar{\mathfrak{p}}}$, which we will denote $D_{\bar{\mathfrak{p}},l}$.
Since $D_{\mathfrak{p},l}$ and $D_{\bar{\mathfrak{p}},l}$ both satisfy property $(\star_l)$, it follows the quotient induces an isomorphism $D_{\mathfrak{p},l} \xrightarrow{\sim} D_{\bar{\mathfrak{p}},l}$. It then follows that $F \subset D_{\mathfrak{p},l}$ the image of F by the quotient $G_K^{m+1} \to G_K^m$, which we will denote $\overline{F}$ as in the statement, will then be an open subgroup of $D_{\bar{\mathfrak{p}},l}$. It then follows that $\overline{F}$ also satisfies property $(\star_l)$ by Proposition 2.2.8, and the quotient $G_K^{m+1} \twoheadrightarrow G_K^m$ restricts to an isomorphism on F. □

We are interested in looking further at what happens in the first case in Proposition 3.1.5.

Lemma 3.1.7. *Let $m > 2$ be an integer, and let $\sigma_{m+1} : G_K^{m+1} \to G_L^{m+1}$ be a homomorphism of profinite groups, let l be a prime number and let F be a subgroup of G_K^m satisfying property $(\star_l)$. Assume that the induced morphism $\sigma_m : G_K^m \to G_L^m$ restricts to an injection on F. Then, $\sigma_m(F) \subset G_L^m$ also satisfies property $(\star_l)$.*

Proof. Let us denote $\sigma_m(F)$ by F'. As σ_m is injective on F, then it restricts to an isomorphism between F and F', therefore we know that we can fit F' in an exact sequence

$$1 \to \mathbb{Z}_l \to F' \to \mathbb{Z}_l \to 1.$$

Denote by $\widetilde{F}$ the inverse image of F in G_K^{m+1} with respect to the canonical quotient and, similarly, let $\widetilde{F}'$ be the inverse of image of F' in G_L^{m+1}. By commutativity of the diagram in Proposition 3.1.1, it follows that $\widetilde{F}' = \sigma_{m+1}(\widetilde{F})$. Then, we can induce a commutative diagram of cohomology groups

$$\begin{array}{ccc} H^2(\widetilde{F}', \mathbb{F}_l) & \longrightarrow & H^2(\widetilde{F}, \mathbb{F}_l) \\ {\scriptstyle \inf_{F'}}\uparrow & & {\scriptstyle \inf_F}\uparrow \\ H^2(F', \mathbb{F}_l) & \xrightarrow{\sim} & H^2(F, \mathbb{F}_l) \end{array}$$

where the vertical arrows are the inflation maps and the horizontal arrows are induced by σ_{m+1} and σ_m. Since σ_m is an isomorphism between F and F', the induced arrow $H^2(F', \mathbb{F}_l) \to H^2(F, \mathbb{F}_l)$ is also an isomorphism.
Since F satisfies property $(\star_l)$ the inflation map $\inf_F : H^2(F, \mathbb{F}_l) \to H^2(\widetilde{F}, \mathbb{F}_l)$ has non-trivial image, and it follows the composition $H^2(F', \mathbb{F}_l) \to H^2(\widetilde{F}, \mathbb{F}_l)$ will also have non-trivial image. By commutativity of the diagram we then conclude that the inflation map $\inf_{F'} : H^2(F', \mathbb{F}_l) \to H^2(\widetilde{F}', \mathbb{F}_l)$ also needs to have non-trivial image, and so the subgroup F' of G_L^m also satisfies property $(\star_l)$. □

Definition 3.1.8. *Let l be a prime number and $m \geq 2$ be a positive integer. Let $\sigma_m : G_K^m \to G_L^m$ be a homomorphism of profinite groups. We will say that a sub-*

group F of G_K^m satisfies condition $(\dagger_l)$ if F satisfies condition $(\star_l)$ and σ_m restricts to an injection on F.
We will denote by $\widetilde{\mathcal{C}}_{\sigma_m,l}$ the subset of $\widetilde{\mathcal{D}}_{m,l,K}$ (see Definition 2.2.6) of all the subgroups of G_K^m satisfying property $(\dagger_l)$.

The following result is just a statement of Lemma 3.1.7 using the notation introduced above.

Corollary 3.1.9. *In the same setting as Lemma 3.1.7, a map*

$$\tilde{\psi}_{m,l} : \widetilde{\mathcal{C}}_{\sigma_m,l} \to \widetilde{\mathcal{D}}_{m,l,L}$$

is naturally induced from σ_m.

The equivalence relation $\approx$ on $\widetilde{\mathcal{D}}_{m,l,K}$ in Definition 2.2.7 induces naturally an equivalence relation on the subset $\widetilde{\mathcal{C}}_{\sigma_m,l}$. We may define the set of equivalence classes $\mathcal{C}_{\sigma_m,l} = \widetilde{\mathcal{C}}_{\sigma_m,l}/\approx$. Since the equivalence relation on $\widetilde{\mathcal{C}}_{\sigma_m,l}$ is a restriction of the one on $\widetilde{\mathcal{D}}_{m,l,K}$, there is a natural injective map $\mathcal{C}_{\sigma_m,l} \hookrightarrow \mathcal{D}_{m,l,K}$. We will show in Proposition 3.1.13 that $\tilde{\psi}_{m,l}$ also factors through $\mathcal{C}_{\sigma_m,l}$. Finally, let $P_{m-1}^{(l')}$ denote the image of $\mathcal{C}_{\sigma_m,l}$ by the map $\phi_{m,l,K}$ defined as in 2.2.9. Observe that by construction every prime in $P_{m-1}^{(l')}$ has residue characteristic different from l. Finally let

$$P_{m-1} = \bigcup_l P_{m-1}^{(l')}.$$

We have then the following natural diagram:

$$\begin{array}{ccc}
\widetilde{\mathcal{C}}_{\sigma_m,l} & \hookrightarrow & \widetilde{\mathcal{D}}_{m,l,K} \\
\downarrow & & \downarrow \\
\mathcal{C}_{\sigma_m,l} & \hookrightarrow & \mathcal{D}_{m,l,K} \\
\wr\downarrow \phi_{m,l,K} & & \wr\downarrow \phi_{m,l,K} \\
P_{m-1}^{(l')} & \hookrightarrow & \mathfrak{Primes}_{K_{m-1}}^{\mathrm{na},(l')} \\
\downarrow & & \downarrow \\
P_{m-1} & \hookrightarrow & \mathfrak{Primes}_{K_{m-1}}^{\mathrm{na}}
\end{array}$$

Observe that an equivalence class of elements $\widetilde{\mathcal{C}}_{\sigma_m,l}$ does not necessarily contain by construction all the elements of an equivalence class in $\widetilde{\mathcal{D}}_{m,l,K}$. However, the following result gives us this statement is true.

Proposition 3.1.10. *Let $m \geq 2$ be an integer, and let $\sigma_{m+1} : G_K^{m+1} \to G_L^{m+1}$ be a homomorphism of profinite groups, and let F be a subgroup of G_K^m satisfying property $(\dagger_l)$. Let $\mathfrak{p}$ be a prime of K_m such that F is l-open in the decomposition group $D_\mathfrak{p} \subset G_K^m$ (see Proposition 2.2.8). Then, for any prime $\mathfrak{p}'$ conjugate to $\mathfrak{p}$ in*

K_m/K, any subgroup F' which is l-open in $D_{\mathfrak{p}'}$ also satisfies property $(\dagger_l)$.
In particular, if F'' is a subgroup of G_K^m satisfying property $(\star_l)$ such that $F \approx F''$, F'' also satisfies property $(\dagger_l)$.

Proof. Let F and F' be as in the statement. By Proposition 2.2.8, we know that for some prime $\mathfrak{p}$ of K_m with decomposition group $D_{\mathfrak{p}} \subseteq G_K^m$, F is contained in an l-Sylow subgroup $D_{\mathfrak{p},l}$ of $D_{\mathfrak{p}}$.
First, we want to show σ_m restricts to an injection on $D_{\mathfrak{p},l}$. By assumption, σ_m restricts to an injection on F and, if we consider the inertia part $I_{\mathfrak{p},l} = I_{\mathfrak{p}} \cap D_{\mathfrak{p},l}$, we know that the kernel of σ_m must contain either an open subgroup of $I_{\mathfrak{p},l}$, or be trivial (cf. Proposition 3.1.5). Then, it must contain the image of the intersection $I_{\mathfrak{p},l} \cap F$, which is a non-trivial open subgroup of $I_{\mathfrak{p},l}$ (which must be isomorphic to $\mathbb{Z}_l$), where σ restricts to an injection.
It follows that the image of $I_{\mathfrak{p},l}$ contains a subgroup isomorphic to $\mathbb{Z}_l$, but since $I_{\mathfrak{p},l} \cong \mathbb{Z}_l$, this implies that σ_m restricts to an injection on $I_{\mathfrak{p},l}$ and by Proposition 3.1.5 it also follows σ_m also restricts to an injection on $D_{\mathfrak{p},l}$. It then immediately also follows that σ_m restricts to an injection on any open subgroup of $D_{\mathfrak{p},l}$. Furthermore, since any other l-Sylow of $D_{\mathfrak{p}}$ is conjugate to $D_{\mathfrak{p},l}$, their images by σ_m are also conjugate, and so they also have cohomological dimension 2.
Let now $\mathfrak{p}'$ be any prime conjugate to $\mathfrak{p}$ in K_m/K. Then, there exists $h \in G_K^m$ such that $h\mathfrak{p} = \mathfrak{p}'$ and $hD_{\mathfrak{p}}h^{-1} = D_{\mathfrak{p}'}$, and their images by σ_m will also be conjugate and, in particular, isomorphic. It then follows σ_m also restricts to an isomorphism on the l-Sylows of $D_{\mathfrak{p}'}$.
Since conjugation necessarily maps any l-Sylow of $D_{\mathfrak{p}}$ to an l-Sylow of $D_{\mathfrak{p}'}$, it follows that for any subgroup F' which is l-open in $D_{\mathfrak{p}'}$, we obtain $\mathrm{cd}(\sigma(F')) = 2$, and so F' satisfies property $(\dagger_l)$.
Let us now take a subgroup F'' of G_K^m satisfying property $(\star_l)$ such that $F \approx F''$. By Proposition 2.2.9 F'' is an open subgroup of the decomposition group $D_{\mathfrak{p}''} \subset G_K^m$ of a prime $\mathfrak{p}''$ of K_m such that $\mathfrak{p}$ and $\mathfrak{p}''$ have the same restriction in K_{m-1}. It follows that $\mathfrak{p}$ and $\mathfrak{p}''$ are conjugate in K_m/K and by the above argument we obtain that σ_m restricts to an injection on F'', and so F'' satisfies property $(\dagger_l)$. □

The above result also shows that, for a prime $\bar{\mathfrak{p}}$ of K, it is sufficient to check if a single prime $\mathfrak{p}$ of K_{m-1} satisfies condition $(\dagger_l)$ to find if all the primes of K_{m-1} above $\mathfrak{p}$ satisfy condition $(\dagger_l)$ or not.

Proposition 3.1.11. *Let $m \geq 2$ be an integer, and let $\sigma_{m+1} : G_K^{m+1} \to G_L^{m+1}$ be a homomorphism of profinite groups. Consider the induced homomorphism of profinite groups $\sigma : G_K^m \to G_L^m$, consider the map $\tilde{\psi}_{m,l}$ induced by σ_m (as in Corollary 3.1.9) and let $F_1, F_2 \in \widetilde{\mathcal{C}}_{\sigma_m,l}$ such that $F_1 \approx F_2$ under the equivalence relation $\approx$ of Definition 2.2.7. Let $F_1' = \tilde{\psi}_{m,l}(F_1)$ and $F_2' = \tilde{\psi}_{m,l}(F_2)$ be their*

images in $\widetilde{\mathcal{D}}_{m,l,L}$. *Then,* $F_1' \approx F_2'$.
In particular, the map $\tilde{\psi}_{m,l}$ *induces a map* $\psi_{m,l} : \mathcal{C}_{\sigma_m,l} \to \mathcal{D}_{m,l,L}$.

Proof. Let H' be an open subgroup of G_L^m containing $G_L[m, m-1]$, and let H be its inverse image by σ_m. Since $\sigma_m(G_K[m, m-1])$ is contained in $G_L[m, m-1]$ then $H \supseteq G_K[m, m-1]$ and is open, since H' is. Let $\widetilde{F}_1$ and $\widetilde{F}_2$ be the images of $F_1 \cap H$ and $F_2 \cap H$ in H^{ab}. By definition of $\approx$, we have $\widetilde{F}_1 \cap \widetilde{F}_2$ is open in both $\widetilde{F}_1$ and $\widetilde{F}_2$, that is $\widetilde{F}_1$ and $\widetilde{F}_2$ are commensurable.
Let $\widetilde{F}_1'$ and $\widetilde{F}_2'$ be the images of $F_1' \cap H'$ and $F_2' \cap H'$ in ${H'}^{\mathrm{ab}}$. Since $F_1' = \sigma_m(F_1)$ and $H' \supseteq \sigma_m(H)$, we can see that $F_1' \cap H' \supseteq \sigma_m(F_1 \cap H)$ and similarly we can also get $F_2' \cap H' \supseteq \sigma_m(F_2 \cap H)$. Furthermore, since σ_m restricts to an isomorphism between F_1 and F_1' (resp. F_2 and F_2'), we can also see that $F_1 \cap H$ is isomorphic to its image by σ_m (resp. the image of $F_2 \cap H$ is isomorphic to its image by σ_m). However, since $\sigma_m(H) \subseteq H'$ and σ_m is an isomorphism between F_1 and F_1' and between F_2 and F_2', it now follows that $F_1 \cap H \cong F_1' \cap H'$ and $F_2 \cap H \cong F_2' \cap H'$, and the isomorphisms are given by σ_m.
From this, we get that the induced homomorphism σ_1 also induces an isomorphism between $\widetilde{F}_1$ and $\widetilde{F}_1'$ and, likewise, between $\widetilde{F}_2$ and $\widetilde{F}_2'$. However, this also means that $\widetilde{F}_1' \cap \widetilde{F}_2' \cong \widetilde{F}_1 \cap \widetilde{F}_2$. Thus, we get that $\widetilde{F}_1' \cap \widetilde{F}_2'$ is an open subgroup of both $\widetilde{F}_1'$ and $\widetilde{F}_2'$, which are then commensurable. Since this does not depend on the choice of H', we have proven $F_1' \approx F_2'$.
We can now conclude by defining a map $\mathcal{C}_{\sigma_m,l} \to \mathcal{D}_{m,l,L}$ by mapping the class in $\mathcal{D}_{m,l,K}$ of an element F of $\widetilde{\mathcal{C}}_{\sigma_m,l}$ to the congruence class of $\sigma_m(F)$ in $\mathcal{D}_{m,l,L}$, and the above argument gives us this map is well-defined with respect to equivalence classes. □

After this proposition we may construct the following diagram:

$$\begin{array}{ccc}
\widetilde{\mathcal{C}}_{\sigma_m,l} & \xrightarrow{\tilde{\psi}_{m,l}} & \widetilde{\mathcal{D}}_{m,l,L} \\
\big\downarrow & & \big\downarrow \\
\mathcal{C}_{\sigma_m,l} & \xrightarrow{\psi_{m,l}} & \mathcal{D}_{m,l,L} \\
\wr\big\downarrow \phi_{m,l,K} & & \wr\big\downarrow \phi_{m,l,L} \\
P_{m-1}^{(l')} & & \mathfrak{Primes}_{K_{m-1}}^{\mathrm{na},(l')}
\end{array}$$

Since the bottom vertical arrows are bijections, we can construct naturally a map $P_{m-1}^{(l')} \to \mathfrak{Primes}_{K_{m-1}}^{\mathrm{na},(l')}$ and get the following corollary:

Corollary 3.1.12. $\psi_{m,l}$ *induces a map* $\theta_{m-1,l} : P_{m-1}^{(l')} \to \mathfrak{Primes}_{L_{m-1}}^{\mathrm{na},(l')}$

We now have maps $\theta_{m-1,l}$ for all the prime numbers l, and we want to see if they are compatible and in which way, so that they can be glued together to obtain a map $\theta_{m'} : P_{m'} \to \mathfrak{Primes}_{L_{m'}}^{\mathrm{na}}$ for some integer $m' \leq m$.

Proposition 3.1.13. *Let $m \geq 3$ be an integer, and let $\sigma_{m+1} : G_K^{m+1} \to G_L^{m+1}$ be a homomorphism of profinite groups. Consider the homomorphism $\sigma_m : G_K^m \to G_L^m$ induced by σ_{m+1}.*
Let $\mathfrak{p}$ be a prime of K_m, l_1, l_2 two distinct prime numbers, and let F_1 and F_2 be subgroups of the decomposition group $D_\mathfrak{p} \subset G_K^m$ satisfying conditions $(\dagger_{l_1})$ and $(\dagger_{l_2})$ respectively. Then, $\sigma_m(F_1)$ and $\sigma_m(F_2)$ are contained in decomposition groups in G_L^m that define the same prime in L_{m-2}.
In particular, a mapping $\theta_{m-2} : P_{m-2} \to \mathfrak{Primes}^{\mathrm{na}}_{L_{m-2}}$ is defined by taking the prime $\bar{\bar{\mathfrak{p}}}$ of K_{m-2} below $\mathfrak{p}$ and mapping it to the unique prime $\bar{\bar{\mathfrak{q}}}$ of L_{m-2} such that $\sigma_{m-2}(D_{\bar{\bar{\mathfrak{p}}}}) \subseteq D_{\bar{\bar{\mathfrak{q}}}}$.

Proof. First, observe that the stabilisers of the equivalence classes of F_1 and F_2 in $\mathcal{D}_{m,l,K}$ with respect to the action of G_K^{m+1} (see Proposition 2.2.9) coincide, and correspond to the decomposition group $D_{\bar{\mathfrak{p}}} \subset G_K^{m-1}$ where $\bar{\mathfrak{p}}$ is the prime of K_{m-1} below $\mathfrak{p}$ by Proposition 2.2.9
Also, by Proposition 2.2.8 we have that F_1' and F_2' are open subgroups of Sylows subgroups for some primes, so let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be primes (not necessarily uniquely determined) of L_m such that F_1' is l_1-open in $D_{\mathfrak{q}_1}$ and F_2' is l_2-open in $D_{\mathfrak{q}_2}$. Then, the stabilisers of the classes of F_1' and F_2' are the decomposition groups in G_L^{m-1} of the primes $\bar{\mathfrak{q}_1}$ and $\bar{\mathfrak{q}_2}$ of L_{m-1}, below $\mathfrak{q}_1$ and $\mathfrak{q}_2$ respectively.
We then get that both $D_{\bar{\mathfrak{q}_1}}$ and $D_{\bar{\mathfrak{q}_2}}$ need to contain $\sigma_{m-1}(D_{\bar{\mathfrak{p}}})$. Observe that the image $\overline{F}_1$ of F_1 by the quotient $G_K^m \twoheadrightarrow G_K^{m-1}$ satisfies property $(\star_l)$ by Proposition 3.1.6 and similarly the image $\overline{F}_1'$ in G_L^{m-1} of F_1' also satisfies property $(\star_l)$. By commutativity in Proposition 3.1.1 $\overline{F}_1$ is mapped surjectively by σ_{m-1} to $\overline{F}_1'$ and this map must be an isomorphism by Proposition 3.1.5. However, since $F_1 \subset D_\mathfrak{p}$, we obtain $\overline{F}_1 \subset D_{\bar{\mathfrak{p}}}$, which means $\sigma_{m-1}(D_{\bar{\mathfrak{p}}})$ is non-trivial and in particular $D_{\bar{\mathfrak{q}}_1} \cap D_{\bar{\mathfrak{q}}_2} \neq 1$.
It then follows $\bar{\mathfrak{q}}_1$ and $\bar{\mathfrak{q}}_2$ must be above the same prime $\bar{\bar{\mathfrak{q}}}$ of L_{m-2} by Proposition 2.2.2, and the images of $D_{\bar{\mathfrak{q}}_1}$ and $D_{\bar{\mathfrak{q}}_2}$ in G_K^{m-2} by the canonical quotient coincide with $D_{\bar{\bar{\mathfrak{q}}}}$.
If we denote by $\bar{\bar{\mathfrak{p}}}$ the prime of K_{m-2} below $\bar{\mathfrak{p}}$ we may now able to say that the decomposition group $D_{\bar{\bar{\mathfrak{p}}}} \subset G_K^{m-2}$ is mapped to a non-trivial subgroup of the decomposition group $D_{\bar{\bar{\mathfrak{q}}}} \subseteq G_L^{m-2}$, and the prime $\bar{\bar{\mathfrak{q}}}$ is uniquely determined. We are then able to define the mapping $\theta_{m-2} : P_{m-2} \to \mathfrak{Primes}^{\mathrm{na}}_{L_{m-2}}$ by setting $\theta_{m-2}(\bar{\bar{\mathfrak{p}}}) = \bar{\bar{\mathfrak{q}}}$. □

With this result, we have now obtained that starting from $(\star_l)$-subgroups that are mapped injectively gives us a map between sets of primes as desired. Specifically, we have the following diagram:

$$\begin{array}{ccccc}
\widetilde{\mathcal{D}}_{m,l,K} \supseteq & \widetilde{\mathcal{C}}_{\sigma_m,l} & \xrightarrow{\tilde{\psi}_{m,l}} & \widetilde{\mathcal{D}}_{m,l,L} & \\
& \downarrow & & \downarrow & \\
\mathcal{D}_{m,l,K} \supseteq & \mathcal{C}_{\sigma_m,l} & \xrightarrow{\psi_{m,l}} & \mathcal{D}_{m,l,L} & \\
& \downarrow{\scriptstyle \phi_{m,l,K}} & & \downarrow{\scriptstyle \phi_{m,l,L}} & \\
\mathfrak{Primes}^{\mathrm{na}}_{K_{m-1}} \supseteq & P_{m-1} & & \mathfrak{Primes}^{\mathrm{na}}_{L_{m-1}} & \\
& \downarrow & & \downarrow & \\
\mathfrak{Primes}^{\mathrm{na}}_{K_{m-2}} \supseteq & P_{m-2} & \xrightarrow{\theta_{m-2}} & \mathfrak{Primes}^{\mathrm{na}}_{L_{m-2}} &
\end{array}$$

In this situation, we will say that the homomorphism of profinite groups $\sigma_{m-2} : G_K^{m-2} \to G_L^{m-2}$ induces the map $\theta_{m-2} : P_{m-2} \to \mathfrak{Primes}^{\mathrm{na}}_{L_{m-2}}$.
The two following results show us that subgroups satisfying property $(\dagger_l)$ in G_K^{m-1} can in some way be lifted to G_K^m.

Proposition 3.1.14. *Let $m \geq 3$ be an integer, let $\sigma_{m+1} : G_K^{m+1} \to G_L^{m+1}$ be a homomorphism of profinite groups, let l be a prime number and consider the induced homomorphism of profinite groups $\sigma_{m-1} : G_K^{m-1} \to G_L^{m-1}$. Then, let $\bar{F}$ be a subgroup of G_K^{m-1} satisfying property $(\dagger_l)$.*
Then, for any subgroup F of G_K^m satisfying property $(\star_l)$ such that F is mapped surjectively onto $\bar{F}$ by the canonical quotient we have F satisfies condition $(\dagger_l)$.

Proof. As $\sigma_{m-1}(\bar{F})$ is the image of $\bar{F}$ by σ_{m-1} by the commutativity in Proposition 3.1.1, then $\sigma_m(F)$ must map surjectively onto $\sigma_{m-1}(\bar{F})$, which has cohomological l-dimension ≥ 2. However, by Proposition 3.1.5, this means that the composition of σ_m and the canonical quotient $G_L^m \twoheadrightarrow G_L^{m-1}$ restricts to an injective map on F, which also implies σ_m restricts to an injection on F, and so F satisfies condition $(\dagger_l)$. □

Corollary 3.1.15. *Let $m \geq 3$ be a positive integer and let $\sigma_{m+1} : G_K^{m+1} \to G_L^{m+1}$ be a homomorphism of profinite groups with open image, and consider the induced homomorphisms $\sigma_m : G_K^m \to G_L^m$ and $\sigma_{m-1} : G_K^{m-1} \to G_L^{m-1}$.*
Let $\bar{\mathfrak{p}}$ be a prime of K_{m-1} and consider the decomposition group $D_{\bar{\mathfrak{p}}} \subset G_K^{m-1}$, and let $l \neq char(\mathfrak{p})$ be a prime number. Assume that there exists a prime $\bar{\mathfrak{q}} \in \mathfrak{Primes}^{\mathrm{na}}_{L_{m-1}}$ with decomposition group $D_{\bar{\mathfrak{q}}} \subseteq G_L^{m-1}$ (not necessarily uniquely determined) such that $\sigma_{m-1}(D_{\bar{\mathfrak{p}}})$ is l-open in $D_{\bar{\mathfrak{q}}}$. Then, there exists a subgroup F of G_K^m satisfying condition $(\dagger_l)$ such that the image of F by the canonical map $\widetilde{\mathcal{D}}_{m,l,K} \to \mathfrak{Primes}^{\mathrm{na}}_{K_{m-1}}$ is $\bar{\mathfrak{p}}$.

Proof. Since $\sigma_{m-1}(D_{\bar{\mathfrak{p}}})$ is l-open in $D_{\bar{\mathfrak{q}}}$, by definition of l-open the image of an l-Sylow subgroup $D_{\bar{\mathfrak{p}},l}$ of $D_{\bar{\mathfrak{p}}}$ by σ_{m-1} is open in an l-Sylow $D_{\bar{\mathfrak{q}},l}$ of $D_{\bar{\mathfrak{q}}}$, and so satisfies condition $(\star_l)$, which implies by Proposition 3.1.5 that $D_{\bar{\mathfrak{p}},l}$ is isomorphic to its image, and it satisfies condition $(\dagger_l)$. It follows immediately that any open

subgroup of $D_{\bar{\mathfrak{p}},l}$ also satisfies $(\dagger_l)$.
Let $\mathfrak{p}$ be any prime of K_m above $\bar{\mathfrak{p}}$, and let F be an open subgroup of an l-Sylow subgroup $D_{\mathfrak{p},l}$ of $D_{\mathfrak{p}} \subset G_K^m$. Then, the image of F in G_K^{m-1} by the canonical quotient is an open subgroup of an l-Sylow subgroup $D_{\bar{\mathfrak{p}},l}$ satisfying $(\star_l)$ which we will denote $\bar{F}$, which we have shown needs then to satisfy $(\dagger_l)$. It now follows by Proposition 3.1.14 that F also satisfies $(\dagger_l)$. □

The following proposition is the last result for this section, and shows that the definition of the map θ_{m-2} in Proposition 3.1.13 induces a mapping between the primes of the base fields K and L.

Proposition 3.1.16. *Let $m \geq 1$ be a positive integer, $\sigma_{m+3} : G_K^{m+3} \to G_L^{m+3}$ a homomorphism of profinite groups, and consider the map $\theta_m : P_m \to \mathfrak{Primes}_{L_m}^{\mathrm{na}}$ induced from $\sigma_m : G_K^m \to G_L^m$ as in Proposition 3.1.13.*
Then, considering the natural actions of G_K^m on P_m and of G_L^m on $\mathfrak{Primes}_{L_m}^{\mathrm{na}}$, we have $\theta_m(g\mathfrak{p}) = \sigma_m(g)\theta_m(\mathfrak{p})$ for all in $g \in G_K^m$ and $\mathfrak{p} \in P_m$ (i.e. the map θ_m is equivariant with respect to the natural actions of G_K^m on P_m and $\sigma_m(G_K^m) \subseteq G_L^m$ on $\mathfrak{Primes}_{L_m}^{\mathrm{na}}$).
It follows that for all $0 \leq i \leq m-1$, if we let P_i be the subset of all primes of K_i which are below some prime of P_m, there is a map $\theta_i : P_i \to \mathfrak{Primes}_{L_i}^{\mathrm{na}}$ naturally induced from θ_m.
In particular, we may induce a well-defined map $\theta : P \to \mathfrak{Primes}_L^{\mathrm{na}}$, where P is the set of all primes of K below a prime of P_m. We will then say that σ_m induces θ.

Proof. Let $\mathfrak{p} \in P_m$, and let $D_{\mathfrak{p}} \subset G_K^m$ be its decomposition group. By definition, for all $g \in G_K^m$, we have $gD_{\mathfrak{p}}g^{-1} = D_{g\mathfrak{p}}$ (observe that by Proposition 3.1.10 $g\mathfrak{p} \in P_m$), and let $\mathfrak{q} = \theta_m(\mathfrak{p})$.
Let $\tilde{\mathfrak{p}}$ be a prime of K_{m+1} above $\mathfrak{p}$. Recall that, by the definition of θ_m in Proposition 3.1.13 for some prime number l, the $(\star_l)$-subgroups contained in the decomposition group $D_{\tilde{\mathfrak{p}}} \subseteq G_K^{m+1}$ are mapped by σ_m to a subgroup of a decomposition group $D_{\tilde{\mathfrak{q}}}$ for some (not necessarily unique) prime $\tilde{\mathfrak{q}}$ of L_{m+1} above $\mathfrak{q}$. Then, for any lift $\tilde{g} \in G_K^{m+1}$ of g, the $(\star_l)$-subgroups contained in the decomposition group $D_{\tilde{g}\mathfrak{p}}$ are mapped by σ_{m+1} (injectively, by Proposition 3.1.14) to subgroups of $\sigma_{m+1}(\tilde{g})D_{\tilde{\mathfrak{q}}}\sigma_{m+1}(\tilde{g})^{-1}$, which coincides with $D_{\sigma_{m+1}(\tilde{g})\mathfrak{q}}$.
As $\sigma_{m+1}(\tilde{g})D_{\tilde{\mathfrak{q}}}\sigma_{m+1}(\tilde{g})^{-1}$ is mapped by the natural quotient $G_L^{m+1} \twoheadrightarrow G_L^m$ surjectively to $\sigma_m(g)D_{\mathfrak{q}}\sigma_m(g)^{-1} = D_{\sigma_m(g)\mathfrak{q}}$, it then follows that indeed $\theta_m(g\mathfrak{p}) = \sigma_m(g)\theta_m(\mathfrak{p})$, as desired.
For $0 \leq i \leq m-1$, we may now take primes $\mathfrak{p}_1, \mathfrak{p}_2 \in P_m$ conjugate in the extension K_m/K_i. Then, there exists $g' \in G_K^m[i]$ such that $g'\mathfrak{p}_1 = \mathfrak{p}_2$. Then, if we let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be primes of L_m such that $\mathfrak{q}_1 = \theta_m(\mathfrak{p}_1)$ and $\mathfrak{q}_2 = \theta_m(\mathfrak{p}_2)$, it follows that $\sigma_m(g')\mathfrak{q}_1 = \mathfrak{q}_2$. However (cf. the proof of Proposition 3.1.1) $\sigma_m(g') \in G_L^m[i]$, and

so $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are conjugate in the extension L_m/L_i. It then follows we have a map $\theta_i : \mathfrak{P}_i \to \mathfrak{Primes}_{L_i}^{\mathrm{na}}$ induced naturally from θ_m.
The last assertion also follows from the above argument, as it gives us that if $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are conjugate in K_m/K, then $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are conjugate in L_m/L, and so we also have the map $\theta : P \to \mathfrak{Primes}_L^{\mathrm{na}}$ as desired. □

3.2 Conditional Existence in the Hom-Form

In this section we are interested in showing that, if some particular conditions on $(\star_l)$-subgroups and the mapping of primes θ_m we defined in the previous section hold, we can construct an injection of fields inducing our homomorphism of profinite groups as in the Hom-Form, which will be our main result for this section.

We have seen in Proposition 3.1.13 that if a subgroup satisfying property $(\star_l)$ in G_K^m is mapped injectively to a subgroup satisfying property $(\star_l)$ in G_L^m, then the prime it determines in K_{m-2} is mapped to a unique prime of L_{m-2}.

Proposition 3.2.1. *Let $m \geq 2$ be an integer, and let $\sigma_m : G_K^m \to G_L^m$ be a homomorphism of profinite groups induced by a homomorphism of profinite groups $\sigma_{m+1} : G_K^{m+1} \to G_L^{m+1}$.*
Assume that for every prime number l, σ_m restricts to an injection on every closed subgroup F of G_K^m satisfying property $(\star_l)$ (that is for every $F \subset G_K^m$, F satisfies $(\star_l)$ if and only if F satisfies $(\dagger_l)$).
Then the mapping of primes $\theta_{m-2} : P_{m-2} \to \mathfrak{Primes}_{L_{m-2}}^{\mathrm{na}}$ (obtained as in Proposition 3.1.13) is defined for every finite prime of K_{m-2}, that is $P_{m-2} = \mathfrak{Primes}_{K_{m-2}}^{\mathrm{na}}$.

Proof. This follows immediately from as starting with G_K^{m+1} by Proposition 2.2.10 we can recover all the decomposition groups in G_K^{m-2} from the subgroups satisfying $(\star_l)$ in G_K^m, and by 3.1.13 since all the $(\star_l)$-subgroups in G_K^m satisfy condition $(\dagger_l)$, the prime they determine in K^{m-2} is mapped to a unique prime in L^{m-2}. □

In the above proposition, we are not requiring a priori that σ_m has open image, however we will show that if the condition of Proposition 3.2.1 is satisfied, the image will automatically be an open subgroup of G_K^m.

Definition 3.2.2. *Let $m \geq 1$, and $\sigma_{m+3} : G_K^{m+3} \to G_L^{m+3}$ be a homomorphism of profinite groups such that the homomorphism $\sigma_{m+2} : G_K^m \to G_L^m$ induced by σ_{m+3} restricts to an injection on every element of $\widetilde{\mathcal{D}}_{m+2,l,K}$, so that the homomorphism of profinite groups $\sigma_m : G_K^m \to G_L^m$ induced by σ_{m+3} induces a mapping between primes $\theta_m : \mathfrak{Primes}_{K_m}^{\mathrm{na}} \to \mathfrak{Primes}_{L_m}^{\mathrm{na}}$ according to Propositions 3.1.13 and 3.2.1.*
We will say that σ_{m+3} satisfies condition $(\dagger)$.

An immediate consequence of θ_m being defined at every prime of K_m (that is $P_m = \mathfrak{Primes}^{\mathrm{na}}_{K_m}$) gives us (cf. Proposition 3.1.16) $P_{m-1} = \mathfrak{Primes}^{\mathrm{na}}_{K_{m-1}}$ and $P = \mathfrak{Primes}^{\mathrm{na}}_{K}$. In particular, the induced maps θ_{m-1} and θ are also defined at every prime of K_m and K respectively.
We now want to study the induced mapping $\theta : \mathfrak{Primes}^{\mathrm{na}}_K \to \mathfrak{Primes}^{\mathrm{na}}_L$ between the primes of the number fields.

Proposition 3.2.3. *Let $m \geq 1$ be an integer and $\sigma_{m+3} : G_K^{m+3} \to G_L^{m+3}$ be a homomorphism of profinite groups satisfying condition (†). Let $\sigma_m : G_K^m \to G_L^m$ be the homomorphism of profinite groups induced by σ_{m+3}*
Let $\theta : \mathfrak{Primes}^{\mathrm{na}}_K \to \mathfrak{Primes}^{\mathrm{na}}_L$ be the map of primes induced by σ_m (see Proposition 3.1.16). Let $\bar{\mathfrak{p}}$ be a prime of K, and let $\bar{\mathfrak{q}} = \theta(\bar{\mathfrak{p}})$. Then, $\bar{\mathfrak{p}}$ and $\bar{\mathfrak{q}}$ have the same residue characteristic p, $f_{\bar{\mathfrak{p}}} \geq f_{\bar{\mathfrak{q}}}$ and $N\bar{\mathfrak{p}} \geq N\bar{\mathfrak{q}}$.
Furthermore, the same inequalities replacing $\bar{\mathfrak{q}}$ with a prime $\tilde{\mathfrak{q}}$ above it in a finite subextension L' of $\widetilde{L}/L$, where $\widetilde{L}$ denotes the subfield of L_m corresponding to the image of σ_m.

Proof. By the definition of θ (Proposition 3.1.16) we have that there exists a prime $\mathfrak{p}$ of K_m above $\bar{\mathfrak{p}}$ which is mapped by θ_m to a prime $\mathfrak{q}$ of L_m above $\bar{\mathfrak{q}}$.
We then get that for every prime number l different from $p = char(\mathfrak{p})$, σ_m maps an l-Sylow subgroup of $D_{\mathfrak{p}}$ isomorphically to a subgroup of $D_{\mathfrak{q}}$ satisfying condition $(\star_l)$. It follows that l is different from $char(\mathfrak{q})$, and repeating this argument for all prime numbers $l \neq char(\mathfrak{p}) = p$, we get that $\mathfrak{q}$ and $\bar{\mathfrak{q}}$ must also necessarily have residue characteristic p.
Consider the decomposition group $D_{\mathfrak{p}} \subseteq G_K^m$, and recall that by proposition 2.2.1.(iii), we can recover the inertia degree $f_{\bar{p}}$ and the norm $N\bar{\mathfrak{p}}$ from the prime-to-p torsion of $D_{\mathfrak{p}}^{\mathrm{ab}}$.
Furthermore, since $\sigma_m(D_{\mathfrak{p}})$ is contained in $D_{\mathfrak{q}} \subset G_L^m$, it is an m-step solvable group, but this does not necessarily mean $\sigma_m(D_{\mathfrak{p}}) = D_{\mathfrak{q}}$. However, we may consider an extension $\mathfrak{q}'$ of $\mathfrak{q}$ in some separable closure $\bar{L}$ of L containing L_m such that $\sigma_m(D_{\mathfrak{p}})$ is a quotient of the m-step solvably closed quotient $D^m_{\mathfrak{q}'}$ of the decomposition group $D_{\mathfrak{q}'} \subset G_L$ of $\mathfrak{q}'$.
Let l be a prime number different from p, and consider the l-Sylow subgroup $D^m_{\mathfrak{q}',l}$ of $D^m_{\mathfrak{q}'}$, which has cohomological l-dimension 2. The image of $D_{\mathfrak{q}',l}$ in H with respect to the quotient must then be an l-Sylow subgroup H_l of H, which by Proposition 3.1.5 has cohomological dimension ≤ 2.
However, since σ_m maps $D_{\mathfrak{p}}$ surjectively to H, every l-Sylow of $D_{\mathfrak{p}}$ is mapped surjectively to an l-Sylow subgroup of H. Furthermore, since every l-Sylow subgroup of $D_{\mathfrak{p}}$ satisfies condition $(\dagger_l)$, it maps isomorphically to its image in H, and so it follows $\mathrm{cd}_l(H) = 2$.
By 3.1.5 it now follows that there is an isomorphism $D^m_{\mathfrak{q}',l} \xrightarrow{\sim} H_l$. It now follows

the l-part of the kernel of the quotient $D^m_{\mathfrak{q}'} \twoheadrightarrow H$ is trivial. We may repeat this for all the primes $l \neq p$, so we get that the kernel of this quotient is a pro-p subgroup V of $D^m_{\mathfrak{q}'}$. We then get the following diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & V & \longrightarrow & D^m_{\mathfrak{q}'} & \longrightarrow & H & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & V^{\mathrm{ab}} & \longrightarrow & D^{\mathrm{ab}}_{\mathfrak{q}'} & \longrightarrow & H^{\mathrm{ab}} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & \longrightarrow & D^{\mathrm{ab},(p')}_{\mathfrak{q}'} & \longrightarrow & H^{\mathrm{ab},(p')} & \longrightarrow & 1
\end{array}$$

where the vertical arrows are given by passing to the abelianization and to the prime-to-p quotient respectively. In particular, we get the prime-to-p torsion of H is isomorphic to the prime-to-p torsion of $D^{\mathrm{ab}}_{\mathfrak{q}'}$. However, we also know that since $D^{\mathrm{ab}}_{\mathfrak{p}} \twoheadrightarrow H^{\mathrm{ab}}$, the prime-to-$p$ torsion of H^{ab} is determined by the image of the prime-to-p torsion of $D^{\mathrm{ab}}_{\mathfrak{p}}$.
If we denote by $\bar{\mathfrak{q}}'$ the restriction of $\mathfrak{q}'$ to L, from the above argument we then get $f_{\bar{\mathfrak{p}}} \geq f_{\bar{\mathfrak{q}}'}$ and $N\bar{\mathfrak{p}} \geq N\bar{\mathfrak{q}}'$. However, since $\mathfrak{q}'$ was an extension of $\mathfrak{q}$, it follows $\bar{\mathfrak{q}}' = \bar{\mathfrak{q}}$, and this also gives us $f_{\bar{\mathfrak{p}}} \geq f_{\bar{\mathfrak{q}}}$ and $N\bar{\mathfrak{p}} \geq N\bar{\mathfrak{q}}$ as desired.
Let L' be as in the statement, and let $\tilde{\mathfrak{q}}$ be a prime in L' above $\bar{\mathfrak{q}}$, which we may assume below the prime $\mathfrak{q}$ of L_m as defined above without loss of generality. Then, we may observe that $\tilde{\mathfrak{q}}$ and $\bar{q}$ have the same residue characteristic. Since $H \subseteq G(L_m/L')$ and the decomposition group of $\mathfrak{q}$ (over $\tilde{\mathfrak{q}}$) in $G(L_m/L')$ is the quotient of the decomposition group $D_{\tilde{\mathfrak{q}}'} \subset G_L$ of an extension $\tilde{\mathfrak{q}}'$ of $\tilde{\mathfrak{q}}$ in $\bar{L}$, and we may repeat the same argument above and obtain the inequalities $f_{\bar{\mathfrak{p}}} \geq f_{\tilde{\mathfrak{q}}}$ and $N\bar{\mathfrak{p}} \geq N\tilde{\mathfrak{q}}$ as desired. □

Let us recall that for a homomorphism of profinite groups $\sigma_m : G^m_K \to G^m_L$, we say that a subextension L' of L_m/L corresponds to a subextension K' of K_m/K if $\sigma_m^{-1}(G(L_m/L')) = G(K_m/K')$. Observe that $\ker(\sigma_m)$ is contained in $G(K_m/K')$, and if L'/L is Galois, then K'/K also is. Furthermore, if we let $\widetilde{L}$ be the subfield of L_m corresponding to the image of σ_m and consider the composite $\widetilde{L}L'$ we have the following diagram:

$$\begin{array}{ccc}
G(K_m/K') & \xrightarrow{\sigma_m} & G(L_m/\widetilde{L}L') \\
\downarrow & & \downarrow \\
G^m_K & \xrightarrow{\sigma_m} & G^m_L \\
\downarrow & & \downarrow \\
G(K'/K) & \hookrightarrow & G(\widetilde{L}L'/L)
\end{array}$$

and we will say that the injective map $G(K'/K) \hookrightarrow G(\widetilde{L}L'/L)$ is induced by σ_m by quotients. We may also observe that since the image of G^m_K by σ_m is

$G(L/\widetilde{L})$, then the image of the injective map in the diagram is the subgroup corresponding to $G(\widetilde{L}L'/\widetilde{L})$ of $G(\widetilde{L}L'/L)$. Then, we will say that an isomorphism $G(K'/K) \xrightarrow{\sim} G(\widetilde{L}L'/\widetilde{L})$ is also induced by σ_m by taking quotients.

Proposition 3.2.4. *Let $m \geq 1$ be a positive integer, and $\sigma_{m+3} : G_K^{m+3} \to G_L^{m+3}$ be a homomorphism of profinite groups satisfying condition (†), consider the induced homomorphism of profinite groups $\sigma_m : G_K^m \to G_L^m$ and let $\theta : \mathfrak{Primes}_K^{\mathrm{na}} \to \mathfrak{Primes}_L^{\mathrm{na}}$ be the map of primes induced by σ_m. Then, there are only finitely many primes of L that are not image of a prime of K by θ.*
Furthermore, if $\widetilde{L}$ is the subextension of L_m/L corresponding to $\sigma_m(G_K^m)$, we have $\tilde{L}/L$ is finite, and $[K : \mathbb{Q}] \geq [\widetilde{L} : \mathbb{Q}] \geq [L : \mathbb{Q}]$. In particular, σ_m has open image.

Proof. Assume by contradiction there are infinitely many primes of L that are not in the image of θ. Since L has a finite number of ideal classes, there must be an ideal class of L containing infinitely many of these primes, so let us denote them by $\mathfrak{q}_0, \mathfrak{q}_1, \mathfrak{q}_2, ...$ Furthermore, for all $i \geq 1$ the ideal $\mathfrak{q}_0/\mathfrak{q}_i$ is principal, and so is generated by some element α_i.
Consider the infinite extension $L' = L(\sqrt{\alpha_1}, \sqrt{\alpha_2}, ...)$ of L contained in L^{ab} (and so also contained in L_m). Also, consider the extension K' of K corresponding to L' by σ_m.
The only primes of L that may ramify in L'/L are primes with residue characteristic 2 or the $\mathfrak{q}_i$, and since all primes of K have an image in L, a prime of K can only be ramified in K'/K if its image in L ramifies in L'/L. Furthermore, by Proposition 3.2.3 every prime of K has the same residue characteristic as its image in L, and as we know that the $\mathfrak{q}_i$ are not in the image of θ, the only primes that may ramify in K'/K are primes with residue characteristic 2.
It follows that since by construction $G(K'/K) \xrightarrow{\sim} G(L'\widetilde{L}/\widetilde{L})$, K'/K is abelian, and by Class Field Theory as the abelian extension K'/K is only ramified over the prime number 2 it must be finite. This then gives us that the composite extension $L'\widetilde{L}/\widetilde{L}$ is finite as well. However, since $L'\widetilde{L}$ is an infinite extensions of L this implies $\widetilde{L}$ is also an infinite extension of L. Furthermore, since $G(L'\widetilde{L}/\widetilde{L}) \cong G(L'/\widetilde{L} \cap L')$ we get $L'' = L' \cap \widetilde{L}$ corresponds to a finite subgroup of $G(L'/L)$, and we may then consider the abelian extension L''/L, which will then also be infinite over L.
Let $\mathfrak{p}$ be a prime of K with odd residue characteristic and of degree 1. Then, its image $\mathfrak{q} = \theta(\mathfrak{p})$ must be unramified in L'/L, and by Proposition 3.2.3 it follows $p = N\mathfrak{p} = N\mathfrak{q}$. Furthermore, by Proposition 3.2.3 we may also replace L with a finite abelian extension L_0/L contained in $L'' \subseteq \widetilde{L}$, and for any extension $\mathfrak{q}'$ of $\mathfrak{q}$ to L_0 we get $N\mathfrak{p} = N\mathfrak{q}'$, and as $\mathfrak{q}$ does not ramify in L_0/L, this gives us $\mathfrak{q}'$ is of degree 1 over L, that is it splits completely in L_0. As this holds for any finite extension of L contained in L'', we get that $\mathfrak{q}$ splits completely in L''/L.
Now, the set A of the primes of K of degree 1 and of odd residue characteristic

has positive Dirichlet density which is given by

$$\delta_K(A) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in A} N\mathfrak{p}^{-s}}{\log(1/(s-1))} \geq \frac{1}{[K:\mathbb{Q}]}.$$

Consider now the image $\theta(A)$ of A in L, and recall again that $p = N\mathfrak{p} = N\mathfrak{q}$ when $\mathfrak{q} = \theta(\mathfrak{p})$. Observe that there are only up to $[K:\mathbb{Q}]$ primes of K with residue characteristic p, and as only primes with the same residue characteristic may map to the same prime $\mathfrak{q}$ of L, we get that

$$\delta_L(\theta(A)) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{q}\in\theta(A)} N\mathfrak{q}^{-s}}{\log(1/(s-1))} \geq \frac{\delta_K(A)}{[K:\mathbb{Q}]}.$$

By the above argument all the primes of L contained in $\theta(A)$ split completely in the infinite extension L''/L. If we take a finite Galois subextension L_1 of L''/L, the primes of $\theta(A)$ will also split completely in L_1/L. Let us take then an L_1 such that $[L_1:L]^{-1} < \delta_L(\theta(A))$. Then, we obtain a contradiction of Chebotarev's density theorem (Corollary 1.1.12) as the set of primes of L that splits completely in L_1 has density $\geq \delta_L(\theta(A)) > [L_1:L]^{-1}$. It then follows that L'' may not be an infinite extension of L, which gives us our initial assumption that infinitely many primes are not in the image of θ is a contradiction.
We want now to show $\widetilde{L}/L$ is finite. Since only finitely many primes of θ are not in the image, we may take a prime number p unramified in $L/\mathbb{Q}$ so that all primes $\mathfrak{q}_1, ..., \mathfrak{q}_n$ of L above p are in the image of θ. Then, we may take some primes $\mathfrak{p}_1, ..., \mathfrak{p}_n$ of K such that $\mathfrak{q}_i = \theta(\mathfrak{p}_i)$. Then, by Proposition 3.2.3 all the $\mathfrak{p}_i$ are also above p, and it follows $f_{p_i} \geq f_{\mathfrak{q}_i}$, for all $i = 1, ..., n$ and since by construction $e_{q_i} = 1$ we get

$$[L:\mathbb{Q}] = \sum_{i=1}^{n} f_{\mathfrak{q}_i} e_{\mathfrak{q}_i} \leq \sum_{i=1}^{n} f_{\mathfrak{p}_i} e_{\mathfrak{p}_i} \leq [K:\mathbb{Q}].$$

Observe that if we replace L with a finite extension $\widehat{L}$ contained in $\widetilde{L}$, the above inequality still holds by Proposition 3.2.3 and it follows that $[\widetilde{L}:\mathbb{Q}] \leq [K:\mathbb{Q}]$. □

With this result, if a homomorphism of profinite groups $\sigma_{m+3} : G_K^{m+3} \to G_L^{m+3}$ satisfying condition (†) gives us a correspondence between inertia degrees of primes of L and K, and we may now start working towards the construction of the injective homomorphism of fields τ.

Proposition 3.2.5. *Let $m \geq 1$ be a positive integer, and $\sigma_{m+3} : G_K^{m+3} \to G_L^{m+3}$ be a homomorphism of profinite groups satisfying condition (†), consider the homomorphism of profinite groups $\sigma_m : G_K^m \to G_L^m$ induced by σ_{m+3} and let $\theta : \mathfrak{Primes}_K^{\mathrm{na}} \to \mathfrak{Primes}_L^{\mathrm{na}}$ be the map of primes induced by σ_m.*
Let M be a Galois extension of $\mathbb{Q}$ containing both K and L. Let $H = G(M/Q)$,

and consider the subgroups $H_1 = G(M/K)$ and $H_2 = G(M/L)$ of H. Then, every element of H_1 is conjugate to an element of H_2 in H.

Proof. An element $h \in H_1$ defines a Frobenius automorphism for a prime $\mathfrak{P}$ in M above a prime number p unramified in $K/\mathbb{Q}$. It then follows that the prime $\mathfrak{p}$ below $\mathfrak{P}$ in K is of degree 1, and its image $\mathfrak{q} = \theta(\mathfrak{p})$ in L is also of degree 1 by 3.2.3. We may then take a prime $\mathfrak{Q}$ above $\mathfrak{q}$ in M. Since $\mathfrak{Q}$ must also have residue characteristic p, it follows that $\mathfrak{P}$ and $\mathfrak{Q}$ are conjugate primes, so let t be an element of H such that $\mathfrak{Q} = t\mathfrak{P}t^{-1}$. It follows then that $tht^{-1} \in H_2$, and so every element of H_1 is conjugate to an element of H_2 as desired. □

Proposition 3.2.6. *Assume that the number fields L and K are contained in the same separable closure Ω of $\mathbb{Q}$, and consider their m-step solvably closed Galois extension L_{m+3}/L and K_{m+3}/K contained in Ω.*
Let $m \geq 1$ be a positive integer, and let $\sigma_{m+3} : G_K^{m+3} \to G_L^{m+3}$ be a homomorphism of profinite groups satisfying condition (†), consider the induced homomorphism of profinite groups $\sigma_m : G_K^m \to G_L^m$.
Let L' be a finite Galois extension of L contained in L_m and let K' be the finite Galois extension of K contained in K_m corresponding to L' by σ_m. Let $M \subseteq \Omega$ be a finite Galois extension of $\mathbb{Q}$ containing L' and K. Then M also contains K'.

Proof. By Proposition 3.1.16, we have a map $\theta : \mathfrak{Primes}_K^{\mathrm{na}} \to \mathfrak{Primes}_L^{\mathrm{na}}$ induced by σ_m. Let p be a prime number that splits completely in M, Then, the primes of L' above p are of degree 1 over $\mathbb{Q}$, and are in particular of degree 1 over L.
Assume then that the map θ restricts to a surjection over the primes of L of residue characteristic p, and observe that by Proposition 3.2.4 this condition is satisfied by all but finitely many prime numbers p as only finitely many primes of L are not in the image of θ.
Then, since every prime of L above p is in the image of θ, we can take the inverse with respect to θ and σ_m and get that any prime of K' above p has degree 1 over K. However since p splits completely in M, any prime above p in K has degree 1 over $\mathbb{Q}$, and taking the composite of the degrees this shows that the primes above p in K' have degree 1.
Now, since p splits completely in M, every prime of K above p also splits completely in M. Since, we know that every prime of K that splits completely in M also splits completely in K', except for the finite number of prime number where θ does not induce a surjection, it follows that by Bauer's Theorem (see Theorem 1.1.13) $M \supseteq K'$. □

We are now able to apply Uchida's method for the proof of Neukirch-Uchida's Theorem (see 1.3.2) to our situation, and obtain an injective homomorphism of fields. This is the main result in this section.

Theorem 3.2.7. *Let $m \geq 1$ be a positive integer, and let $\sigma_{m+4} : G_K^{m+4} \to G_L^{m+4}$ be a homomorphism of profinite groups satisfying condition (†), consider the homomorphism of profinite groups $\sigma_m : G_K^m \to G_L^m$ induced by σ_{m+4}.*
Then, there exists an injection of fields $\tau_m : L_m \to K_m$ that induces σ_m by

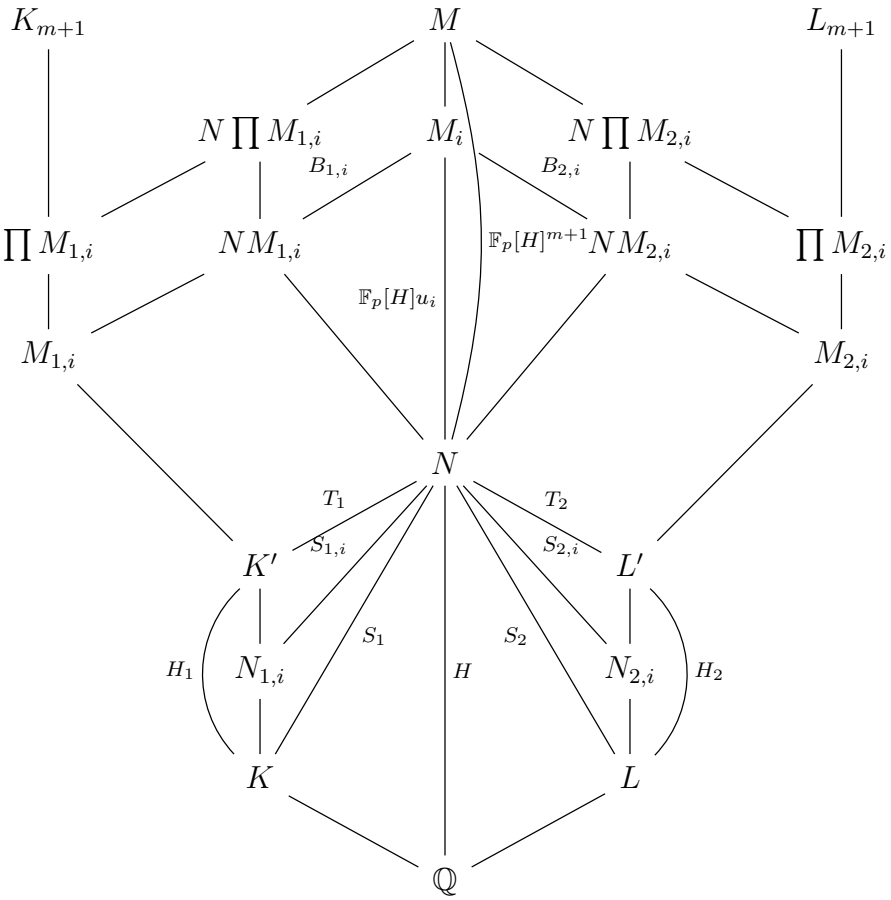
$$\tau_m \sigma_m(g) = g\tau_m$$

for all $g \in G_K^m$.
Furthermore, if $m \geq 1$ the restriction of τ_m to L_{m-1} gives an injective homomorphism $\tau_{m-1} : L_{m-1} \hookrightarrow K_{m-1}$ inducing the homomorphism $\sigma_{m-1} : G_K^{m-1} \to G_L^{m-1}$ induced by σ_{m+3} by

$$\tau_{m-1}\sigma_{m-1}(g') = g'\tau_{m-1}$$

for all $g' \in G_K^{m-1}$.
In particular, an injective homomorphism $\tau : L \hookrightarrow K$ is defined.

Proof. The below diagram gives a visualization of the construction in the following part of the proof. This can be compared with the diagram in the proof of Theorem 1.3.2



Consider a finite Galois subextension L'/L of L_m, and let K' be the finite Galois extension of K corresponding to it by σ_m. Let $H_1 = G(K'/K)$ and $H_2 = G(L'/L)$. Since by definition $G(K_m/K') = \sigma_m^{-1}[G(L_m/L')]$, the kernel of σ_m is contained in

$G(K_m/K')$, and so the map $\sigma : H_1 \hookrightarrow H_2$ induced from σ_m by quotients is injective.

Let N be a finite Galois extension of $\mathbb{Q}$ contained in some separable closure Ω of $\mathbb{Q}$ such that we have embeddings $K' \hookrightarrow N$ and $L' \hookrightarrow N$, and let us consider the images of these embeddings canonically identified with K' and L'.

Let us then define the Galois groups $H = G(N/\mathbb{Q})$, $S_1 = G(N/K)$, $S_2 = G(N/L)$, $T_1 = G(N/K')$ and $T_2 = G(N/L')$. Consider a set of generators $h_{1,1}, ..., h_{1,n}$ for H_1, and set $h_{2,i} = \sigma(h_{1,i})$. Since $H_1 = S_1/T_1$, for all $i = 1, ..., n$ we may define an element $s_{1,i} \in S_1$ such that $s_{1,i}T_1 = h_{1,i}$, and similarly we may define an element $s_{2,i} \in S_2$ such that $s_{2,i}T_2 = h_{2,i}$. For each $s_{1,i}$ we also define a subgroup $S_{1,i}$ generated by $s_{1,i}$ and T_1, and similarly we define $S_{2,i}$ as the subgroup generated by $s_{2,i}$ and T_2. Let us also set $S_{1,0} = T_1$ and $S_{2,0} = T_2$.

We may take a subfield $N_{1,i}$ of N corresponding to $S_{1,i}$ and a subfield $N_{2,i}$ of N corresponding to $S_{2,i}$. By these definitions, $S_{1,i}/T_1 \cong G(K'/N_{1,i})$ is a cyclic subgroup of H_1 generated by $h_{1,i}$, and $S_{2,i}/T_2$ is a cyclic subgroup of H_2 generated by $h_{2,i} = \sigma(h_{1,i})$. Then, we have that σ restricts to a surjective homomorphism $S_{1,i}/T_1 \twoheadrightarrow S_{2,i}/T_2$. However, since σ is injective, this is an isomorphism, and furthermore $N_{2,i}$ must correspond to $N_{1,i}$ by σ_m.

We may now take a prime number p such that $p \equiv 1 \pmod{|H|}$ and $p > |H|^2$, and consider the split group extension

$$1 \to \mathbb{F}_p[H]^{n+1} \to E \to H \to 1.$$

Then, by Proposition 1.1.15 there exists a Galois extension M of $\mathbb{Q}$ containing N such that $G(M/N) = \mathbb{F}_p[H]^{n+1}$ and $G(M/\mathbb{Q}) = E$. We may also take a set of elements $u_0, ..., u_n$ of $\mathbb{F}_p[H]^{n+1}$ so that we may write

$$\mathbb{F}_p[H]^{n+1} = \bigoplus_{i=0}^{n} \mathbb{F}_p[H]u_i$$

and for every $i = 0, ..., n$, we may consider the subfield M_i of M determined by the subgroup $\oplus_{j \neq i}\mathbb{F}_p[H]u_j$ of $\mathbb{F}_p[H]^{n+1}$. Then, taking the quotient of $\mathbb{F}_p[H]^{n+1}$ with respect to this subgroup (which is a normal subgroup as $\mathbb{F}_p[H]^{n+1}$ is abelian) we get that M_i is a Galois extension of $\mathbb{Q}$ and $G(M_i/\mathbb{Q})$ is determined by the split group extension

$$1 \to \mathbb{F}_p[H]u_i \to G(M_i/\mathbb{Q}) \to H \to 1.$$

Let χ_i be a character of $S_{1,i}/T_i$ of order $|S_{1,i}/T_i|$ (observe that when $i = 0$, $S_{1,0}/T_1$ is trivial and so is χ_0), which we may consider as valued in $\mathbb{F}_p$. Since σ induces an isomorphism $S_{1,i}/T_1 \cong S_{2,i}/T_2$, we may induce by $\chi_i\sigma^{-1}$ a character of $S_{2,i}/T_2$, which we will denote χ_i'.

We may then consider a p-extension $M_{2,i}/L'$, which is the maximal subfield of M_i where the operation of $S_{2,i}/T_2$ on $G(M_{2,i}/L')$ coincides with the scalar multiplication of the values of χ_i'.
Observe that since this is an abelian extension of $L' \subset L_m$, this may be identified with a subfield of L_{m+1}. Thus, we may consider it as a subfield of L_{m+1}, and consider the subextension of K_{m+1}/K corresponding to $M_{2,i}$ by σ_{m+1}, which we will denote by $M_{1,i}$. Since $M_{2,i}$ is an extension of L', it follows that $M_{1,i}$ is an extension of K'. We are then able to obtain by Proposition 3.2.6 that as M_i contains $M_{2,i}$ and K', it also contains $M_{1,i}$.
Furthermore, the map σ induced by σ_{m+1} by quotients on the Galois group $G(M_{1,i}/N_{1,i})$ is injective by definition, and we also have $\sigma(G(M_{1,i}/N_{1,i}))$ is contained in $G(M_{2,i}/N_{2,i})$. But since $N_{2,i}$ corresponds to $N_{1,i}$ by σ_m, this is an isomorphism. Then the operation of $S_{1,i}/T_1$ on $G(M_{1,i}/N_{1,i})$ must coincide with scalar multiplication by the values of χ_i.
We may then consider the composite $NM_{1,i}$, contained in M_i and corresponding to a subgroup $B_{1,i}$ of $F_p[H]u_i = G(M_i/N)$. Similarly, we define the subgroup $B_{2,i}$ corresponding to $NM_{2,i}$.
By the construction, we get $G(M_{1,i}/K')$ and $G(NM_{1,i}/N) = \mathbb{F}_p[H]u_i/B_{1,i}$ are isomorphic as $S_{1,i}/T_1$-modules and therefore if we take an element $b_{1,i} \in B_{1,i}$, we can construct a subgroup $(b_{1,i} - \chi_i(b_{1,i}))\mathbb{F}_p[H]u_i$ contained in $B_{1,i}$. We are then able to construct a subgroup $C_{1,i}$ generated by all the $(b_{1,i} - \chi_i(b_{1,i}))\mathbb{F}_p[H]u_i$ as $b_{1,i}$ varies in $B_{1,i}$. Furthermore, we may repeat the same construction over L' to construct a subgroup $C_{2,i}$.
The action of T_2 on $\mathbb{F}_p[H]u_i/C_{2,i}$ is trivial, so $C_{2,i}$ must correspond to a subfield of M_i containing $NM_{2,i}$, which must be also an abelian p-extension of L' where the operation of $S_{2,i}/T_2$ coincides with the multiplication by the values of χ_i'. However, $M_{2,i}$ is by definition the maximal abelian p-extension of L' where this happens, thus $B_{2,i} = C_{2,i}$.
Let us then take the composite $\prod M_{1,i}$ of all the $M_{1,i}$, which is still a subfield of K_{m+1}, and likewise $\prod M_{2,i}$, which is a subfield of L_{m+1}. We can see that by the definition these two fields correspond to each other as composites of corresponding fields, and by Proposition 3.2.5 any element of the Galois group $G(M/\prod M_{1,i})$ is conjugate to an element of $G(M/\prod M_{2,i})$ by an element of E. Furthermore, we know that $\mathbb{F}_p[H]^{n+1}$ is a normal subgroup of E, therefore if we consider the subgroups A_1 and A_2 of $\mathbb{F}_p[H]^{n+1}$ corresponding to fields $N\prod M_{1,i}$ and $N\prod M_{2,i}$ respectively, we also get that any element of A_1 is conjugate to an element of A_2 by an element of E. Finally, since $C_{2,i}$ corresponds to $NM_{2,i}$, we know that $A_2 = \sum_i C_{2,i}$, and by the correspondence $A_1 \supseteq \sum_i C_{1,i}$. Furthermore, by the split exact sequence, this conjugation corresponds to the action on $\mathbb{F}_p[H]^{n+1}$ given by

left multiplication by an element of H . Therefore, fix an element

$$a = \sum_{t_1 \in T_1} (t_1 - 1)u_0 + \sum_{i=1}^{m} (s_{1,i} - \chi_i(s_{1,i}))u_i$$

in A. Then, for some $h \in H$, we get $ha \in A_2$ which we may rewrite as

$$h \sum_{t_1 \in T_1} (t_1 - 1)u_0 \in B_{2,0}$$

and

$$h(s_{1,i} - \chi_i(s_{1,i}))u_i \in B_{2,i}.$$

Now, expanding the first one, we get

$$h \sum_{t_1 \in T_1} (t_1 - 1) \in \sum_{t_2 \in T_2} (t_2 - 1)\mathbb{F}_p[H]u_0$$

and since

$$\sum_{t_2 \in T_2} t_2 \sum_{t_2 \in T_2} (t_2 - 1) = 0 \in \mathbb{F}_p[H],$$

we can rewrite this as

$$\sum_{t_2 \in T_2} t_2 h \sum_{t_1 \in T_1} (t_1 - 1) = 0 \in \mathbb{F}_p[H]u_0.$$

We then fix an element $t_1' \in T_1$. The coefficient of $ht_1' \in H$ in the left side of the sum must be a multiple of p so that the sum is zero in $\mathbb{F}_p[H]u_0$. Observe that the number of elements in the sum which are of the form $t_2'' h t_1''$ for some $t_1'' \in T_1$ and $t_2'' \in T_2$ is less than $|H|^2$ which is itself less than p as we have taken $p > |H|^2$. Therefore the number of elements of the form $t_2'' h t_1'' = ht_1'$ (which are all elements of H) is also less than p.

We then get that ht_1' must cancel out with a term of the form $-t_2' h$ for some $t_2' \in T_2$, that is $t_2' h = ht_1'$, and so we get $h^{-1} T_2 h \subseteq T_1$, therefore h^{-1} induces an injective homomorphism $L' \to K'$.

By the same idea as above, we then observe $h(s_{1,i} - \chi_i(s_{1,i}))u_i \in B_{2,i}$ can be rewritten as

$$\sum_{s \in S_{2,i}} s\chi_i'(s)^{-1} h(s_{1,i} - \chi_i(s_{1,i})) = 0 \in \mathbb{F}_p[H]u_i.$$

Then, using the same argument used before for ht_1', we then have the coefficient of $hs_{1,i}$ in the sum must be 0, and so for some $s' \in S_{2,i}$ we must have $hs_{1,i} = s'h$ and $\chi_i'(s') = \chi_i(s_{1,i})$. Then, $h_{2,i} = s_{2,i} T_2 = s' T_2$ by definition of χ_i'. Also, as $h^{-1} s' = s_{1,j} h^{-1}$ the actions defined by $h^{-1}\sigma(h_{1,j})$ and $h_{1,j} h^{-1}$ on L' coincide. Since the $h_{1,i}$ generate H_1, it follows that h^{-1} determines an injection $L' \to K'$

which induces σ. Since L' was a Galois subextension of L_m/L chosen arbitrarily, we may construct the set $\mathfrak{A}_{L'}$ of all the injections $L' \hookrightarrow K'$ constructed with the above method for every finite Galois extension L' of L contained in L_m, and since it is non-empty and finite (as $h \in H$, and H is finite).
We can observe that the $\mathfrak{A}_{L'}$ define a projective system of non-empty finite sets (as do the $\mathfrak{A}_{K'}$ in the proof of Theorem 1.3.2), so we may take their inverse limit over L' and obtain that the set of injections $\tau_m : L_m \hookrightarrow K_m$ inducing σ_m is non-empty, as desired.
For the last statement, observe that we may take the projective limit over all finite Galois extensions of L contained in L_{m-1} and construct an injective homomorphism $\tau_{m-1} : L_{m-1} \hookrightarrow K_{m-1}$ coinciding with the restriction of τ_m to L_{m-1}. We may also observe that $\tau(L_{m-1})$ is fixed by all $g' \in G_K[m, m-1]$, and as $\sigma_m(g')$ also fixes L_{m-1}, and therefore we may pass to the quotient $\bar{g}$ of g in G_K^{m-1} in $\tau_m\sigma_m(g) = g\tau_m$, thus we get $\tau_{m-1}\sigma_{m-1}(\bar{g}) = \bar{g}\tau_{m-1}$ for all $\bar{g} \in G_K^{m-1}$ as desired. □

We see that this proof requires us to lose an additional abelian step from where we can define the mapping of primes θ_m before as we need to construct $M_{1,i}$ and $M_{2,i}$ and have them correspond by σ_m while being able to apply Proposition 3.2.6.

3.3 Uniqueness

In the previous section, we showed that if certain conditions hold then, up to losing one step, we can construct an injection of fields that induces the homomorphism of profinite groups we were starting with. The main results in this section are conditions for which this injection of fields is unique.

We start this section by adapting a few results of Uchida [Uch3], which he uses to prove uniqueness for the absolute Galois group to the m-step case.

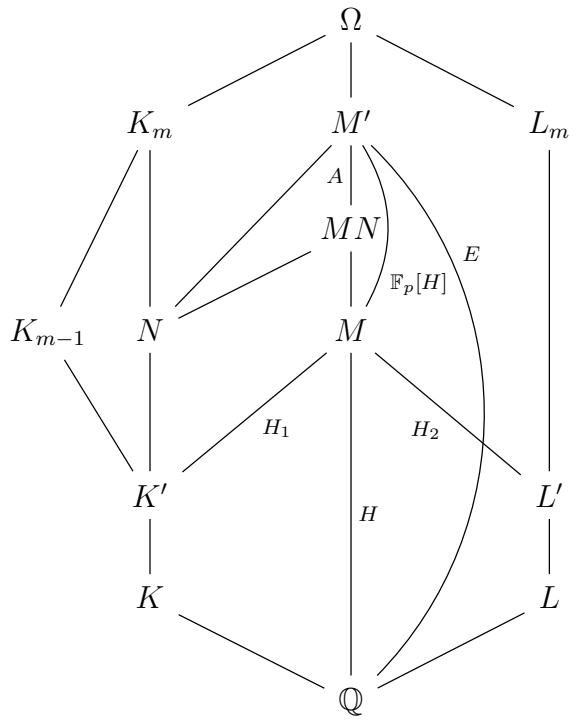
Proposition 3.3.1. *Let K and L be number fields and assume that K and L are contained in the same separable closure Ω of $\mathbb{Q}$. Let $m \geq 1$ be an integer, and consider their m-step solvably closed extensions K_m and L_m contained in Ω. Then, we have that if K_{m-1} is not contained in L_m, the composite K_mL_m is an infinite extension of L_m.*

Proof. Assume K_{m-1} is not contained in L_m. Then, there must be a finite extension K' of K contained in K_{m-1} such that K' is not contained in L_m. We may take a finite Galois extension $M/\mathbb{Q}$ such that M contains both K' and L, and let us denote $H = G(M/\mathbb{Q})$ and $H_1 = G(M/K')$. By Proposition 1.1.15, if we let p be a prime number such that p does not divide $|H|$, and consider the split group extension

$$1 \to \mathbb{F}_p[H] \to E \to H \to 1$$

there exists a Galois extension M' of $\mathbb{Q}$ such that $G(M'/\mathbb{Q}) \cong E$ and $G(M'/M) \cong \mathbb{F}_p[H]$.

Let N be the maximal abelian p-extension of K contained in M', and observe N and M are linearly disjoint extension of K' as p does not divide $|H|$. Then, consider the composite $MN \subseteq M'$. Then, the composite MN is the maximal abelian p-extension of M contained in M' (and so, a quotient of $\mathbb{F}_p[H]$) such that the action of $H_1 = G(M/K)$ on $G(MN/M)$ is trivial. We may observe that MN corresponds to the subgroup A of $\mathbb{F}_p[H]$ determined by all the elements where the action of H_1 is not trivial, that is $G(M'/MN) = A = \sum_{h_1 \in H_1}(h_1 - 1)\mathbb{F}_p[H]$.



Let us then consider the field $L' = K'L \cap L_m$. Since K' is not contained in L_m, it follows that it is also not contained in L'. If we consider the subgroup H_2 of H corresponding to L', it is not contained in H_1, and if we construct the subgroup $A' = \sum_{h_2 \in H_2}(h_2 - 1)\mathbb{F}_p[H]$ we have that A' is not contained in A and so the action of H_2 on $\mathbb{F}_p[H]/A$ is not trivial, and so there is no abelian extension N' of L' such that $N'M = NM$.

Consider the Galois group $G(K'L_m/K'L)$, which is canonically isomorphic to $G(L_m/L')$. Since N is an abelian extension of $K' \subseteq K_{m-1}$, we have $N \subseteq K_m$, and immediately we have NL_m is an extension of L_m contained in K_mL_m. If we assume that NL_m is contained in $K'L_m$, then NL is a subfield of NL_m, and since N/K' is abelian the extension $NL/K'L$ is also abelian. Therefore, by the isomorphism of Galois groups above we can find an abelian extension N' of L' such that $NL = N'K'$. However, this means that MN coincides with MN', which is a composition of N', an abelian extension of L', and M. We then get a

contradiction, and so NL_m is a non-trivial abelian p-extension of $K'L_m$ contained in K_mL_m.
It now follows that K_mL_m contains an extension of L_m whose degree is a multiple of p, and repeating this argument for the infinitely many primes p not dividing $|H|$ we get that K_mL_m must necessarily be an infinite extension of L_m. □

Corollary 3.3.2. *Let $m \geq 1$ be a positive integer, and let K and L be number fields contained in a same separable closure Ω of $\mathbb{Q}$, and consider their maximal m-step solvable extension K_m and L_m contained in Ω. Assume that there exists a number field M such that $MK_m = ML_m$. Then, K_{m-1} is contained in L_m. In particular, $K \subseteq L_m$.*

Proof. Since $MK_m = ML_m \supseteq K_m$, we get that K_mL_m is contained in ML_m, and is therefore a finite extension of L_m. By 3.3.1, we get that this must necessarily mean K_{m-1} is contained in L_m.
The second assertion follows immediately as $K \subseteq K_{m-1}$ □

We now want to find conditions for which an injective homomorphism $\tau : L_m \hookrightarrow K_m$ inducing a homomorphism of profinite groups $\sigma_m : G_K^m \to G_L^m$ (as in Theorem 3.2.7) is unique.

Proposition 3.3.3. *Let $m \geq 1$ be a positive integer, and let $\sigma_m : G_K^m \to G_L^m$ be a homomorphism of profinite groups with open image and let τ and ρ be homomorphisms of fields $\tau, \rho : L_m \hookrightarrow K_m$ such that $\tau\sigma_m(g) = g\tau$ and $\rho\sigma_m(g) = g\rho$ for all $g \in G_K^m$. Let $\widetilde{L}$ be the field corresponding to the image of σ_m. Then:*

(i) $\forall 1 \leq i \leq m$, *we have* $\tau(L_{i-1}) \subset \rho(L_i)$. *In particular* $\tau(L) \subset \rho(L^{\mathrm{ab}})$ *and* $\tau(L_{m-1}) \subset \rho(L_m)$

(ii) $\tau(L) \subseteq \rho(\widetilde{L})$

(iii) $\forall 1 \leq i < j \leq m$ *we have* $\rho(L_j)$ *is a Galois extension of* $\tau(L_i)$.

Proof. Let Λ denote be the subfield of K_m corresponding to the kernel of σ_m, and observe that since $\rho(L_m)$ and $\tau(L_m)$ are contained in K_m we may apply Proposition 3.3.1 and Corollary 3.3.2. Furthermore, for every $1 \leq i \leq m$ we may consider the homomorphism $\sigma_i : G_K^i \to G_L^i$ induced from σ_m, and we will denote by $\Lambda_{(i)}$ the kernel of of σ_i, not to be confused with the maximal i-step solvable extension of Λ.

(i) By construction, we have that $K\tau(L_i) = \Lambda_{(i)} = K\rho(L_i)$. Then, by Corollary 3.3.2, we get $\tau(L_{i-1}) \subseteq \rho(L_i)$.

(ii) From the definition, it follows that we have $\rho(\widetilde{L}) = \rho(L_m) \cap K$. As a consequence of (i) we get $\tau(L)$ is contained in $\rho(L_m)$. Furthermore, by

construction $\tau(L) \subseteq K$, as it is fixed by every element of G_K^m. It then follows $\rho(\widetilde{L}) = \rho(L_m) \cap K \supseteq \tau(L)$ as desired.

(iii) By (i), we get $\rho(L) \subset \tau(L_i) \subset \rho(L_j)$. The assertion now follows immediately as $rho(L_j)/rho(L)$ is a Galois extension, as it is isomorphic to L_j/L.

□

We will use these properties to show some conditions for uniqueness as follows:

Corollary 3.3.4. *Let $m \geq 1$ be a positive integer, and let $\sigma_m : G_K^m \to G_L^m$ be a homomorphism of profinite groups with open image, and let $\widetilde{L}$ be the subfield of L_m corresponding to the image of σ_m.*
Assume that $\widetilde{L} \subseteq L_{m-1}$. Then, if τ and ρ are homomorphisms $\tau, \rho : L_m \hookrightarrow K_m$ such that $\tau\sigma_m(g) = g\tau$ and $\rho\sigma_m(g) = g\rho$, we have $\tau(\widetilde{L}) = \rho(\widetilde{L})$.

Proof. Observe that since $\widetilde{L} \subseteq L_{m-1}$, we have $\tau(L_{m-1}) \cap K = \tau(\widetilde{L})$. Furthermore, since $\rho(L_m) \cap K = \rho(\widetilde{L})$ and by Proposition 3.3.3.(i) we have $\tau(L_{m-1}) \subseteq \rho(L_m)$, we get $\rho(\widetilde{L}) \supseteq \tau(\widetilde{L})$. However, since ρ and τ restrict to an isomorphism of fields to their image, $\rho(\widetilde{L})$ and $\tau(\widetilde{L})$ must have the same degree over $\mathbb{Q}$. It then follows $\tau(\widetilde{L}) = \rho(\widetilde{L})$. □

We then may apply this to

Proposition 3.3.5. *Let $m \geq 2$ be a positive integer, and let $\sigma_m : G_K^m \to G_L^m$ be a homomorphism of profinite groups with open image, and let $\widetilde{L}$ be the subfield of L_m corresponding to the image of σ_m.*
Assume that $\widetilde{L} \subseteq L_{m-1}$ and that there exists an injective homomorphism of fields $\tau : L_m \to K_m$ inducing σ_m by $g\tau = \tau\sigma_m(g)$ for all $g \in G_K^m$. Then, τ is uniquely determined by this property.

Proof. Let $\rho : L_m \hookrightarrow K_m$ an injective homomorphism such that $g\rho = \rho\sigma_m(g)$ for all $g \in G_K^m$. Then, we may apply Corollary 3.3.4 and show $\tau(\widetilde{L}) = \rho(\widetilde{L})$.
By construction the fields $K\rho(L_{m-1})$ and $K\tau(L_{m-1})$ must both coincide with the subfield Λ' corresponding to the kernel of σ_{m-1}. Also, since $K \cap \rho(L_m) = \tau(\widetilde{L})$, of $\rho(\widetilde{L})$, then $\rho(L_{m-1})$ is an extension of $\rho(\widetilde{L})$ linearly disjoint with K, and from the isomorphism $G(\Lambda/K) \cong G(\rho(L_m)/\rho(\widetilde{L}))$, it follows that $K\rho(L_{m-1}) \cap \rho(L_m) = \rho(L_{m-1})$.
Observe that since $K\rho(L_{m-1}) = K\tau(L_{m-1})$, as both fields need to correspond to the kernel Λ of
$sigma_m$, we also get that $K\rho(L_{m-1}) \supseteq \tau(L_{m-1})$. Thus, since from Proposition 3.3.3 $\tau(L_{m-1})$ is also contained in $\rho(L_m)$, it follows $\tau(L_{m-1}) \subseteq K\rho(L_{m-1}) \cap \rho(L_m) = \rho(L_{m-1})$. Reversing the argument gives us $\rho(L_{m-1}) = \tau(L_{m-1})$, and since $\rho(L_m)$ and $\tau(L_m)$ are maximal abelian extensions of the same field $\tau(L_{m-1})$

contained in the same field K_m they coincide as well.
By definition, we now get that $\tau \circ \rho^{-1}$ is an automorphism of Λ, and if for all $g \in G_K^m$ we consider the induced action on $G(\Lambda/K) \cong G(\tau(L_m)/\tau(\widetilde{L}))$ we get $\tau\rho^{-1}g = \tau\sigma_m(g)\rho^{-1} = g\tau\rho^{-1}$, and so $\tau\rho^{-1}$ centralises $G(\tau(L_m)/\tau(\widetilde{L}))$. We are now able to conclude by using Proposition 2.2.5, where we set $K = \tau(widetildeL)$, $\widetilde{K} = \tau(L_{m-1})$ and $\widetilde{K}^{\mathrm{ab}} = \tau(L_m)$, that as the centraliser of $G(\tau(L_m)/\tau(\widetilde{L}))$ in $\mathrm{Aut}(\tau(L_m))$ must be trivial, $\tau\rho^{-1}$ is the identity and so $\rho = \tau$, as desired. □

Observe that the condition in the above proposition is satisfied whenever σ_m is surjective. The condition $g\tau = \tau\sigma_m(g)$ gives us that $\tau(\widetilde{L}) \subseteq K$. We then have the following corollary:

Corollary 3.3.6. *Let $m \geq 1$ be a positive integer, and let $\sigma_m : G_K^m \to G_L^m$ be a homomorphism of profinite groups with open image, and assume that there exists an injective homomorphism $\tau : L_m \to K_m$ inducing σ_m by $g\tau = \tau\sigma_m(g)$, and assume that $\tau(L_{m-1})$ contains K. Then, τ is the unique morphism inducing σ_m.*

Proof. By construction $\tau(\widetilde{L})$ is contained in K. It then follows immediately that since $\tau(\widetilde{L})$ is contained in $\tau(L_{m-1})$ and τ is an isomorphism, we get $\widetilde{L}$ is contained in L_{m-1}. Proposition 3.3.5 then gives us the uniqueness of τ. □

We now give a way to have this condition on K be independent of L and τ. In the following, we will denote by $\mathbb{Q}_m$ the maximal m-step solvably closed extension of $\mathbb{Q}$ contained in K_m. Note that m is in general not a prime, and so this should not be confused with the m-adic completion of $\mathbb{Q}$.

Corollary 3.3.7. *Let $m \geq 1$ be a positive integer and let $\sigma_m : G_K^m \to G_L^m$ be a homomorphism of profinite groups with open image, and assume that $K \subseteq \mathbb{Q}_{m-1}$ contained in K_m. Then, if there exists a homomorphism $\tau : L_m \to K_m$ inducing σ_m by $\tau\sigma_m(g) = g\tau$ for all $g \in G_K^m$, it is uniquely determined.*

Proof. Since $\tau(L)_{m-1} = \tau(L_{m-1})$, we have $\mathbb{Q}^{m-1}$ is contained in $\tau(L_{m-1})$ necessarily, as the composite extension $\mathbb{Q}_{m-1}\tau(L)/\tau(L)$ is an $m-1$-step solvable extension. Therefore, K is contained $\tau(L_{m-1})$ and we may conclude by Corollary 3.3.6. □

Combining Theorem 3.2.7 with the conditions on uniqueness we described above, we get the two following statements, which are the main results in this section and this chapter:

Theorem 3.3.8. *Let K and L be number fields, let $m \geq 1$ be an integer and let $\sigma_{m+4} : G_K^{m+4} \to G_L^{m+4}$ be a homomorphism of profinite groups with open image such that the induced homomorphism of profinite groups $\sigma_{m+3} : G_K^{m+3} \to G_L^{m+3}$ restricts to an injection on every subgroup of G_K^{m+3} satisfying property $(\star_l)$ for some prime number l. Furthermore, assume that the field corresponding to the*

image of σ_{m+4} is contained in L_{m-1}.
Then, there exists a unique injective homomorphism of fields $\tau_m : L_m \to K_m$ such that $\tau_m \sigma_m(g) = g\tau_m$ for all $g \in G_K^m$.

Proof. Observe that we are in the conditions of Theorem 3.2.7, that is σ_{m+4} satisfies condition (†) (Definition 3.2.2) and therefore we have an injective homomorphism of fields $\tau : L_m \to K_m$ inducing σ_m exists.
Let $\widetilde{L}$ be the field corresponding to the image of σ_{m+4}. Observe that since $\tau(\widetilde{L}) = \tau(L_{m+4}) \cap K = \tau(L_{m-1}) \cap K$, the field $\widetilde{L}$ corresponds to the image of all of the homomorphism $\sigma_{m+3}, \sigma_{m+2}, \sigma_{m+1}, \sigma_m$ induced by σ_{m+4} as well.
Uniqueness of τ now follows by Theorem 3.3.5, as the field corresponding to the image of σ_m is $\widetilde{L}$ which is contained in L_{m-1}. □

As with Corollary 3.3.7, we are able to say that if K contained in the $m-1$-step solvably closed extension $\mathbb{Q}^{m-1}$ of $\mathbb{Q}$, the condition on $\widetilde{L}$ must be automatically satisfied when τ exists so we obtain the following:

Theorem 3.3.9. *Let K and L be number fields, let $m \geq 1$ be an integer and assume K contained in the $(m-1)$-step solvably closed extension $\mathbb{Q}_{m-1} \subseteq K_m$ of $\mathbb{Q}$. Let $\sigma_{m+4} : G_K^{m+4} \to G_L^{m+4}$ be a homomorphism of profinite groups with open image such that the induced homomorphism of profinite groups $\sigma_{m+3} : G_K^{m+3} \to G_L^{m+3}$ restricts to an injection on every subgroup of G_K^{m+3} satisfying property $(\star_l)$ for some prime number l.*
Then, there exists a unique injective homomorphism of fields $\tau_m : L_m \to K_m$ such that $\tau_m \sigma_m(g) = g\tau_m$ for all $g \in G_K^m$.

Proof. We are in the conditions of Theorem 3.2.7, namely σ_{m+4} satisfies condition (†). Then, there exists an injective homomorphism $\tau_m : L_m \hookrightarrow K_m$ inducing σ_m as desired. The uniqueness now follows immediately from Corollary 3.3.7. □

This concludes the construction of conditional results for an m-step solvably closed Hom-Form.

Chapter 4

The m-step Hom-Form over $\mathbb{Q}$

In the previous chapter, we obtained conditional result on existence and uniqueness. In this chapter we will be investigating what happens if we are working with a homomorphism of m-step solvably closed Galois groups $G_K^m \to G_L^m$ with open image when $K = \mathbb{Q}$, and show that we are able to obtain a conditional version of the m-step solvable Hom-Form, where the conditions we ask for are weaker than the conditions required in Theorem 3.3.5.

Proposition 4.1. *Let $K = \mathbb{Q}$, $m \geq 0$ be an integer, and let $\sigma_{m+2} : G_K^{m+2} \to G_L^{m+2}$ be a homomorphism of profinite groups such that $\sigma(G_K^{m+2})$ is open in G_L^{m+2}. Then, the induced homomorphism $\sigma_m : G_K^m \to G_L^m$ is surjective and $L = \mathbb{Q}$.*

Proof. By 3.1.1, we have that since σ_{m+2} has open image then the induced morphism σ_m also has open image. Then, let $\widetilde{L} \subseteq L_m$ be the finite extension of L corresponding to $\sigma_m(G_K^m)$. Let E' be a totally imaginary quadratic extension of $\widetilde{L}$. Since E' is an abelian extension of a subextension of L_m, E' is contained in L_{m+1} and so we have a subgroup of G_L^{m+1} corresponding to it. By taking the inverse image of this subgroup with respect to σ_{m+1}, we obtain a corresponding extension E of K, which must also be a quadratic extension of K.
Let s be a positive integer. For any prime number p, as $\mathbb{Z}_p^s$ is an abelian group any $\mathbb{Z}_p^s$-extension of E (resp. of E') must be abelian, and since E is a subfield of K_{m+1} (resp. E' is a subfield of L_{m+1}) this $\mathbb{Z}_p^s$-extension must be a subfield of K_{m+2} (resp. L_{m+2}).
Furthermore, since $G(L_{m+2}/E')$ has to be the homomorphic image of $G(K_{m+2}/E)$, the $\mathbb{Z}_p$-rank of E is $\geq$ than the $\mathbb{Z}_p$-rank of E' and as we set that $E'/\widetilde{L}$ is totally imaginary, the $\mathbb{Z}_p$-rank of E' will be $\geq$ than $[\widetilde{L} : \mathbb{Q}] + 1$.
However, since $K = \mathbb{Q}$, E is a quadratic field and so the $\mathbb{Z}_p$ rank of E will be ≤ 2, so from the inequalities above we get $2 \geq [\widetilde{L} : \mathbb{Q}] + 1$, that is $[\widetilde{L} : \mathbb{Q}] = 1$, which gives σ_m is surjective and $\widetilde{L} = L = \mathbb{Q}$ □

We are then able to reduce our investigation to studying the surjective homomorphism of profinite groups $\sigma_m : G_{\mathbb{Q}}^m \to G_{\mathbb{Q}}^m$. Since the two separable closures

of $\mathbb{Q}$ we are considering do not necessarily coincide, we will still refer to them as $\overline{K}$ and $\overline{L}$, and accordingly we will refer to the copies of $\mathbb{Q}$ corresponding to each closure as K and L.

While the above result holds in general, we will now assume that the image of any subgroup of G_K^m satisfying property $(\star_l)$ contains no torsion elements, that is case (iii) in Proposition 3.1.5 does not happen. Under this assumption, if the inertia part of a decomposition group in G_K^m is mapped non-trivially by σ_m, then we are necessarily in case (i) of 3.1.5.

Recall again that for a homomorphism of profinite groups $\sigma_m : G_K^m \to G_L^m$, we say that a subextension L' of L_m/L corresponds to a subextension K' of K_m/K if $\sigma_m^{-1}(G(L_m/L')) = G(K_m/K')$.

If $K = \mathbb{Q}$ and σ_m is surjective, as is the case in the proposition above, let L' be a Galois subextension of L_m/L. Then K'/K is Galois as well, and by taking quotients from σ_m we obtain an isomorphism $G(K'/K) \cong G(L'/L)$.

The following statements are a transposition of results by Uchida (cf. Lemma 1 in [Uch3]) where we set conditions to be able to use them in the m-step solvably closed case, as the original proof still works after a few minor changes.

Proposition 4.2. *Let $m \geq 2$, and let $\sigma_m : G_K^m \twoheadrightarrow G_L^m$ be a surjective homomorphism of profinite groups induced by a homomorphism of profinite groups $\sigma_{m+2} : G_K^{m+2} \to G_L^{m+2}$ with open image, where $K = L = \mathbb{Q}$. Assume that the image by σ_m of any subgroup of G_K^m satisfying property $(\star_l)$ contains no torsion elements. Then:*

- *Let M be the unique $\mathbb{Z}_2$-extension of $\mathbb{Q}$. Then, M corresponds to itself by σ_m (that is, $\sigma_m(G(K_m/M)) = G(L_m/M)$).*
- *Let $n \geq 3$ and let ζ_{2^n} denote a primitive 2^n-th roots of unity of $\mathbb{Q}$. Then, the field $L(\zeta_{2^n})$ corresponds to $K(\zeta_{2^n})$ by σ_m.*
- *For $n \geq 3$, let s be the $\mathbb{Z}_p$-rank of $L(\zeta_{2^n})$. Then the unique $\mathbb{Z}_p^s$-extension of $L(\zeta_{2^n})$ (which is contained in L_m) corresponds to the unique $\mathbb{Z}_p^s$-extension of $K(\zeta_{2^n})$ by σ_m.*

Proof. All the extensions of K and L we will be considering in this proof are contained in either K_2 or L_2, and therefore are contained in K_m and L_m.

- Consider the subgroup $H' \subseteq G_L^m$ corresponding to $G(L_m/M)$. Then, if let M' be the subfield of K_m determined by $\sigma_m^{-1}(H')$, if follows from the discussion above $G(M'/K)$ must be isomorphic to $G(M/L) \cong \mathbb{Z}_2$. It then follows that $M' = M$.
- Consider the abelian extension $L(\sqrt{-1}, \sqrt{2}) = L(\zeta_{2^3})/L$, which has Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and observe that the only prime number that ramifies

in $L(\zeta_{2^3})/L$ is 2. Let N be the extension of K corresponding to $L(\eta_{2^3})$ by σ_m, and observe that σ_m induces an isomorphism $G(N/K) \cong G(L(\zeta_{2^3})/L)$ by quotients. Since the $\mathbb{Z}_2$-extension of L corresponds to the $\mathbb{Z}_2$-extension of K by σ_m, it follows that $L(\sqrt{-1})$ (which is contained in $L(\zeta_{2^3})$ corresponds to $K(\sqrt{-1})$ by σ, and therefore the prime 2 is ramified in N/K.
Assume then any odd prime p ramifies in N/K, let $\mathfrak{p}$ be any prime of K_m above p, $D_\mathfrak{p} \subset G_K^m$ its decomposition group, and let $I_\mathfrak{p}$ be the inertia subgroup. Then, the image of $I_\mathfrak{p}$ in $G(N/K)$ is non-trivial. Since σ_m induces an isomorphism $G(N/K) \xrightarrow{\sim} G(L(\eta_{2^3})/L)$, this means that a 2-Sylow $I_{\mathfrak{p},2}$ has non-trivial image by σ_m. By Proposition 3.1.5 and Lemma 3.1.7, this means a 2-Sylow subgroup of $D_\mathfrak{p}$ is mapped injectively to a 2-Sylow subgroup of some prime $\mathfrak{q}$ of L_m with residue characteristic $\neq 2$, which ramifies in the extension $L(\zeta_{2^3})/L$, where we have already seen only 2 ramifies. We then get a contradiction and the only prime that ramifies in N/K is 2, which means $N = K(\sqrt{-1}, \sqrt{2}) = K(\zeta_{2^3})$.
Furthermore, it now follows immediately that for every $n \geq 3$, we can apply the same idea of proof to $L(\zeta_{2^n})$, as it is only ramified at 2, and show that the extension corresponding to it by σ_m is also only ramified at 2, which by equality of degrees over $\mathbb{Q}$ means $L(\zeta_{2^n})$ corresponds to $K(\zeta_{2^n})$ by σ_m.

- From the above point, we know $L(\zeta_{2^n})$ corresponds to $K(\zeta_{2^n})$ by σ_m, which as σ_m is surjective by 4.1 means σ_m induces a surjective homomorphism $G(K_m/K(\zeta_{2^3})) \to G(L_m/L(\zeta_{2^3}))$.
Let us then consider the unique $\mathbb{Z}_p^s$-extension of $L(\zeta_{2^n})$, which we will denote by L'. Let us also denote by K' the extension of K that corresponds to L' by σ_m. By taking quotients, this means σ_m induces an isomorphism $G(K'/K(\zeta_{2^n})) \xrightarrow{\sim} G(L'/L(\zeta_{2^n}))$ and K' is a $\mathbb{Z}_p^s$-extension of $K(\zeta_{2^3})$.
We may now conclude by observing that $K(\zeta_{2^3}) = L(\zeta_{2^3})$, they have the same $\mathbb{Z}_p$-rank s, which gives us K' is uniquely determined.

□

Our goal is now to recover the local conditions for our σ, as Uchida does.

Proposition 4.3. *Assume $m \geq 2$, and let $\sigma_m : G_K^m \twoheadrightarrow G_L^m$ be a surjective homomorphism of profinite groups induced by a homomorphism of profinite groups $\sigma_{m+2} : G_K^{m+2} \to G_L^{m+2}$ with open image such that $K = L = \mathbb{Q}$. Assume that the image by σ_m of any subgroup of G_K^m satisfying property $(\star_l)$ contains no torsion elements.*
Let P the set of odd prime numbers. Then, a mapping of primes $\theta : P \to \mathfrak{Primes}_L^{\mathrm{na}}$ (obtained as in 3.1.16) is defined, and for $p \in P$ we have $\theta(p) = p$.
Furthermore, if we let P_{m-1} be the set of all primes of K_{m-1} with odd residue

characteristic, a mapping of primes $\theta_{m-1} : P_{m-1} \to \mathfrak{Primes}^{\mathrm{na}}_{L_{m-1}}$ *is also defined, and this map preserves the residue characteristic (that is, it is compatible with* θ*).*

Proof. Let q be an odd prime, and consider the field $L(\sqrt{q})$, where q ramifies. As this is an abelian extension of L it is contained in L_1. By Proposition 4.2 since $L(\sqrt{q})$ is not contained in $L(\eta_{2^3})$ the field K' corresponding to $L(\sqrt{q})$ by σ_m is not a subfield of $K(\zeta_{2^3})$ as well. Then, it follows that there must be an odd prime number p ramifying in K'.

Let then $\mathfrak{p}$ be a prime of K_m above p, and consider a 2-Sylow subgroup$D_{\mathfrak{p},2}$ of the decomposition subgroup $D_{\mathfrak{p}} \subset G^m_K$. Since p is odd $char(\mathfrak{p}) \neq 2$, which means $D_{\mathfrak{p},2}$ satisfies property $(\star_l)$. Since p ramifies in the quadratic extension K'/K, we also have that the image of the inertia group $I_{\mathfrak{p},2} \subseteq D_{\mathfrak{p},2}$ in the Galois group $G(K'/K)$ is non-trivial, and since $G(L(\sqrt{2})/L) \cong G(K'/K)$, we have that $\sigma(I_{\mathfrak{p},2})$ must be non-trivial as well. By Proposition 3.1.5 it now follows that σ_m restricts to an isomorphism on $D_{\mathfrak{p},2}$, which then satisfies property $(\dagger_2)$.

Since $D_{\mathfrak{p},2}$ satisfies property $(\dagger_2)$ (and so it satisfies $(\star_2)$), it follows by Proposition 3.1.14 there is a subgroup of G^{m+1}_K satisfying property $(\dagger_2)$ which is mapped to $D_{\mathfrak{p},2}$ by the quotient, and in particular we get that the image of $D_{\mathfrak{p}}$ in G^{m-1}_K is mapped by σ_{m-1} to a subgroup of the decomposition group $D_{\bar{\mathfrak{q}}} \subseteq G^{m-1}_L$ of a uniquely determined prime $\bar{\mathfrak{q}}$ of L_{m-1} by Proposition 3.1.13. We can then define θ_{m-1} at the image $\bar{\mathfrak{p}} \in \mathfrak{Primes}^{\mathrm{na}}_{K_{m-1}}$ of $\mathfrak{p}$.

We may also define the induced map θ at p, and let us denote $r = \theta(p)$. It now follows that r must necessarily be ramified in the extension $L(\sqrt{q})/L$, which implies $r = q$. Since our starting assumption was that q was an odd prime number, it follows every odd prime is in the image of θ.

Now, we want to show $q = p$. We may choose an integer n large enough so that p does not split completely in $K(\zeta_{2^n})$, and let s be the $\mathbb{Z}_p$-rank of $K(\zeta_{2^n})$. Since p does not split completely, we get that there are at most $[K(\zeta_{2^n}) : K]/2$ primes in $K(\zeta_{2^n})$ dividing p. Furthermore, since it is an abelian extension of $K = \mathbb{Q}$, the Leopoldt conjecture holds in $K(\zeta_{2^n})$, and so it follows s is greater than the number of prime divisors of p.

Let us denote by E the $\mathbb{Z}^s_p$-extension of $K(\zeta_{2^n})$. If the inertia subgroup associated to a prime divisor of p in E is of rank 1, then there is a quotient of rank at least 1 of the decomposition group $D_{\mathfrak{q}}$ where the inertia subgroup maps trivially, it follows that $K(\zeta_{2^n})$ has an unramified $\mathbb{Z}_p$-extension, which is impossible.

Then, at least one of these inertia groups needs to contain a subgroup isomorphic to $\mathbb{Z}^2_p$, and let us fix a prime $\mathfrak{p}'$ of $K(\zeta_{2^n})$ above p such that this is true for the inertia subgroup $I_{\mathfrak{p}'}$ of $\mathfrak{p}'$.

Then, considering its image $\sigma_m(I_{\mathfrak{p}'})$, we may observe that the inertia group of some prime $\mathfrak{q}'$ above q in the $\mathbb{Z}^s_p$-extension of $L(\eta_{2^n})$ will contain a subgroup isomorphic to $\mathbb{Z}^2_p$, but since $\mathfrak{q}'$ was above q this implies $q = p$. It then follows that θ, which

we had already shown has every odd prime number in its image, is defined for all odd prime numbers of $K = \mathbb{Q}$ and coincides with the identity. $\square$

From all these results, we get that if we start with a homomorphism $\sigma_{m+3} : G_{\mathbb{Q}}^{m+3} \to G_L^{m+3}$ with open image, $L = \mathbb{Q}$, the induced homomorphism $\sigma_{m+1} : G_{\mathbb{Q}}^{m+1} \to G_{\mathbb{Q}}^{m+1}$ is surjective and induces a map of primes $\theta_m : P_m \to \mathfrak{Primes}_{L_m}^{\mathrm{na}}$ where P_m is the set of all primes of K_m with odd residue characteristic p, and this map preserves the residue characteristic.

Proposition 4.4. *Let $m \geq 1$ be an integer, $K = \mathbb{Q}$, and let $\sigma_{m+3} : G_K^{m+3} \to G_L^{m+3}$ be a homomorphism of profinite groups with open image. Assume that the image by the homomorphism $\sigma_{m+1} : G_K^{m+1} \to G_L^{m+1}$ of any subgroup of G_K^{m+1} satisfying property $(\star_l)$ contains no torsion elements. Then the induced map $\sigma_m : G_K^m \to G_L^m$ is an isomorphism.*

Proof. By Proposition 4.1, it follows that $L = \mathbb{Q}$, the induced maps $\sigma_{m+1} : G_K^{m+1} \to G_L^{m+1}$ and $\sigma_m : G_K^m \to G_L^m$ are surjective. Furthermore, we also have the map θ as defined in Proposition 4.3.
Let Λ be the subfield of K_m corresponding to the kernel of σ_m. Let L' be an arbitrary finite Galois extension of $\mathbb{Q}$, and let K' be the finite Galois extension of $\mathbb{Q}$ corresponding to it by σ_m.
Since σ_m induces an isomorphism $\sigma : G(\Lambda/\mathbb{Q}) \cong G(L_m/\mathbb{Q})$, we may take K' as a subfield of Λ, and we have an induced homomorphism $\sigma' : G(K'/\mathbb{Q}) \xrightarrow{\sim} G(L'/\mathbb{Q})$. Let p be an odd prime number splitting completely in L'/L, and observe that by Proposition 4.3 $\theta(\mathfrak{p}) = \mathfrak{p}$. Let $\mathfrak{p}$ be a prime of L' above p. Then, the decomposition group $D_{\mathfrak{p}'} \subset G(K'/K)$ is mapped (isomorphically) by σ' to a decomposition group of a prime $\mathfrak{q}'$ of L' above p. Then, it follows from this isomorphism that p also splits completely in K'/K. An application of Theorem 1.1.13 then gives us an embedding of K' in L_m is contained in L', but since they have the same degree over $\mathbb{Q}$ this is an isomorphism $K' \xrightarrow{\sim} L'$.
Now, we may take the projective limit over the L' contained in L_m of the sets of isomorphisms $K' \to L'$, which are finite and non-empty, and we obtain that there exists an isomorphism $\tau : \Lambda \xrightarrow{\sim} L_m$ by ([RZ], Proposition 1.1.4).
Assume there exists a Λ' be a non-trivial finite extension of Λ Galois over $\mathbb{Q}$ contained in K_m. Then, we can by τ construct an extension L'' of L_m such that $G(L''/L_m) \cong G(\Lambda'/\Lambda)$. However, since $\Lambda' \subseteq K_m$, then $G(\Lambda'/\mathbb{Q})$ is m-step solvable, and so must be $G(L''/\mathbb{Q})$ but this contradicts the maximality of L_m, and so $\Lambda = K_m$, which in turn implies he kernel of σ_m is trivial and σ_m is an isomorphism. $\square$

Under the assumptions of Proposition 4.4, when $m \geq 3$ we are now able to prove immediately that the induced isomorphism σ_{m-3} has a unique field isomorphism τ_{m-3} inducing it using Saïdi and Tamagawa's result (see Theorem 2.1.6).

However, since we have shown σ_m is an isomorphism, the map θ_m is naturally defined at every prime of K_m, as every subgroup of G_K^m is mapped isomorphically by σ_m to its image, and we obtain the map of primes θ_m is defined for every non-archimedean prime of K_m, similarly to Corollary 2.2.11. We may then use the construction of Theorem 3.2.7 we can get the following, which requires us to lose fewer steps:

Theorem 4.5. *Let $m \geq 0$ and let $\sigma_{m+4} : G_K^{m+4} \to G_L^{m+4}$ be a homomorphism of profinite groups with open image and assume $K = \mathbb{Q}$ and the image by the homomorphism $\sigma_{m+2} : G_K^{m+2} \to G_L^{m+2}$ induced by σ_{m+4} of any subgroup of G_K^{m+2} satisfying property $(\star_l)$ contains no torsion elements. Then $L = \mathbb{Q}$, and the induced homomorphism $\sigma_{m+1} : G_K^{m+1} \to G_L^{m+1}$ is an isomorphism. Furthermore, if $m \geq 2$ there exists a unique isomorphism of fields $\tau_m : K_m \to L_m$ such that $\sigma_m(g) = \tau_m g \tau_m^{-1}$ for all $g \in G_K^m$.*

Proof. We have that $L = \mathbb{Q}$ and σ_{m+1} is an isomorphism from Proposition 4.1 and Proposition 4.4.
Assume then $m \geq 2$. Proposition 4.3 gives us that the mapping of primes $\theta_{m+1} : P_{m+1} \to \mathfrak{Primes}_{L_{m+1}}^{\mathrm{na}}$ is defined at the set of all primes of K_{m+1} above an odd prime number. However, since σ_{m+1} is an isomorphism, it follows that for any odd prime number l, any l-Sylow subgroup of the decomposition group of a prime of K_{m+1} above 2 is mapped injectively by the isomorphism σ_{m+1}, that is $P_m = \mathfrak{Primes}_{K_m}^{\mathrm{na}}$ and we are in the conditions of Proposition 3.2.1.
We are then able to use Theorem 3.2.7 to get the existence of our τ_m, and since $\mathbb{Q} = \widetilde{L}$ is contained in L_{m-1}, and the uniqueness also follows from Theorem 3.3.5 □

Bibliography

[Bru] Armand Brumer. "On the units of algebraic number fields". *Mathematika* 14.2 (1967), pp. 121–124.

[Gas] Fritz Gassmann. "Bemerkungen zur vorstehenden Arbeit von Hurwitz". *Mathematische Zeitschift* 25 (1926), pp. 665–675.

[Gras] Georges Gras. *Class Field Theory: from Theory to Practice*. Springer-Verlag, 2003.

[Gro1] Alexander Grothendieck. "Letter to G. Faltings (translation into English)". *Geometric Galois Actions*. Ed. by Leila Schneps and Pierre Lochak. Vol. 1. London Mathematical Society Lecture Note Series. Cambridge University Press, 1997, pp. 285–293.

[Gro2] Alexander Grothendieck. "Sketch of a Programme (translation into English)". *Geometric Galois Actions*. Ed. by Leila Schneps and Pierre Lochak. Vol. 1. London Mathematical Society Lecture Note Series. Cambridge University Press, 1997, pp. 243–284.

[Leo] Heinrich-Wolfgang Leopoldt. "Zur Arithmetik in abelschen Zahlkörpern." *Journal für die reine und angewandte Mathematik* 209 (1962), pp. 54–71. URL: `http://eudml.org/doc/150514`.

[Neu] Jurgen Neukirch. *Algebraic Number Theory*. Springer-Verlag, 1999.

[NSW] Jurgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. 2nd ed. Springer-Verlag, 2008.

[Per] Robert Perlis. "On the equation $\zeta_k(\mathrm{s}) = \zeta'_k(\mathrm{s})$". *Journal of Number Theory* 9.3 (1977), pp. 342–360.

[Pop] Florian Pop. "On Grothendieck's Conjecture of Birational Anabelian Geometry". *Annals of Mathematics* 139.1 (1994), pp. 145–182.

[RZ] Luis Ribes and Pavel Zalesskii. *Profinite Groups*. Springer Berlin Heidelberg, 2000.

[S-T] Mohamed Saïdi and Akio Tamagawa. *The m-step solvable anabelian geometry of number fields*. 2019. arXiv: `1909.08829 [math.NT]`.

[Ser] Jean-Pierre Serre. *Galois Cohomology*. Springer-Verlag, 1997.

[Uch1] Kôji Uchida. “Isomorphisms of Galois Groups of Algebraic Function Fields”. *Annals of Mathematics* 106 (1977), p. 589.

[Uch2] Kôji Uchida. “Isomorphisms of Galois groups of solvably closed Galois extensions”. *Tohoku Mathematical Journal* 31 (1979), pp. 359–362.

[Uch3] Kôji Uchida. “Homomorphisms of Galois groups of solvably closed Galois extensions”. *Journal of the Mathematical Society of Japan* 33.4 (1981), pp. 595–604.