

SOLVING EMBEDDING PROBLEMS WITH BOUNDED RAMIFICATION

Nantsoina Cynthia Ramiharimanana



Dissertation presented for the degree of Doctor of Philosophy
in Mathematics at Stellenbosch University

Promoters: Prof. Moshe Jarden Prof. Barry Green
(Tel Aviv University) (Stellenbosch University)

December 2016

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the owner of the copyright thereof (unless to the extent explicitly otherwise stated) and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: December 2016

Signature: N.C. Ramiharimanana

Copyright ©2016 Stellenbosch University

All rights reserved

Abstract

Given a Galois extension K/K_0 of number fields, a finite group G , and an epimorphism $\alpha: G \rightarrow \text{Gal}(K/K_0)$ with solvable kernel, our goal is to embed K into a Galois extension N of K_0 with Galois group $\text{Gal}(N/K_0) \cong G$ such that the restriction map $\text{res}_{N/K}: \text{Gal}(N/K_0) \rightarrow \text{Gal}(K/K_0)$ coincides with α and $|\text{Ram}(N/K_0)| \leq |\text{Ram}(K/K_0)| + \Omega(|\text{Ker}(\alpha)|)$. Here $\text{Ram}(N/K_0)$ is the finite set of primes of K_0 that ramify in N and $\Omega(|\text{Ker}(\alpha)|)$ is the number of the prime divisors, counted with multiplicity, of $|\text{Ker}(\alpha)|$.

We achieve our goal under two conditions: first, the number of roots of unity in K should be relatively prime to the order of $\text{Ker}(\alpha)$. The second one demands that each local embedding problem resulted from the original one should be "weakly solvable". In fact, our solution locally coincides with finitely many "local weak solutions" given in advance.

Our result strengthens a former result of Neukirch in [Neu79], where the same embedding problem satisfying the same conditions is solved without giving a bound on the ramification.

In particular, the above mentioned local conditions are satisfied if the epimorphism α has a section. This leads to a well known result of Shafarevich that does not assume the condition on the roots of unity but pays with a huge number of ramified primes (that appears when one analyses Shafarevich's proof).

Like in [Neu79], our proof uses class field theory in its cohomological approach. The bounding of the ramification is based, in addition to the above mentioned tools, on a strengthening of a lemma of [GeJ98].

Opsomming

Laat K/K_0 'n Galois uitbreiding van getalleliggame wees, G 'n eindige groep, en $\alpha: G \rightarrow \text{Gal}(K/K_0)$ 'n epimorfisme met oplosbare kern. Ons doel is om K in 'n Galois uitbreiding N van K_0 in-te-bed sodat die Galois groep $\text{Gal}(N/K_0) \cong G$, en sodat die beperkingsafbeelding $\text{res}_{N/K}: \text{Gal}(N/K_0) \rightarrow \text{Gal}(K/K_0)$ ooreenstem met α en $|\text{Ram}(N/K_0)| \leq |\text{Ram}(K/K_0)| + \Omega(|\text{Ker}(\alpha)|)$. Hier is $\text{Ram}(N/K_0)$ die eindige versameling van priemdelers van K_0 wat in N vertak, en $\Omega(|\text{Ker}(\alpha)|)$ is die aantal priemdelers van $|\text{Ker}(\alpha)|$, getel met multiplisiteit.

Ons bereik hierdie doelstelling onderhewig aan twee voorwaardes: Eerstens moet die aantal wortels van eenheid in K relatief priem wees aan die orde van $\text{Ker}(\alpha)$. Tweedens eis ons dat elke lokale inbeddingsprobleem, wat volg uit die oorspronklike een, "swak oplosbaar" moet wees. Meer presies gestel, sal ons oplossing lokaal ooreenstem met 'n eindige aantal "lokaal swak oplossings" wat vooraf gegee word.

Ons resultaat versterk 'n vroeër resultaat van Neukirch in [Neu79], waar 'n inbeddingsprobleem wat dieselfde voorwaardes bevredig opgelos word, maar sonder die grens op die aantal vertakkings.

In die besonder word die lokale voorwaardes bevredig mits die epimorfisme α 'n snitafbeelding besit. Hieruit volg dan ook die bekende resultaat van Shafarevich, wat nie die voorwaarde oor die wortels van eenheid benodig nie, maar gevolglik 'n baie groot aantal priemdelers wat vertak veroorsaak (hierdie opmerking word gesien wanneer sy bewys in detail bestudeer word).

Soos in [Neu79], maak ons gebruik van klasliggaamteorie met 'n kohomologiese benadering. Die begrensdeheid van die aantal priemdelers wat vertak maak ook gebruik van 'n versterking van 'n hulpstelling uit [GeJ98].

Acknowledgements

I would like to express my sincere gratitude to my advisors Prof. Moshe Jarden and Prof. Barry Green for giving me the opportunity to continue my studies and to work on this project. They allowed me to grow as a researcher scientist. Their incredible assistance, support and guidance made this thesis possible. Special thanks go to Prof. Moshe Jarden for his patience with my questions, for our valuable discussions, and for his constructive comments that enormously strengthened and improved this work.

I am thankful to Prof. Wulf-Dieter Geyer, Prof. Kay Wingberg, and Dr. Sebastian Petersen for their useful comments on some materials that I used in this work (private communication). I am also grateful to Prof. Lior-Barry Soroker, Mrs Meira Hilel, and Mrs Rina Jarden for their valuable assistance during my visit at the School of Mathematics at Tel Aviv University. Thank you to DAAD (Deutscher Akademischer Austausch Dienst), to AIMS-SA (African Institute for Mathematical Sciences - South Africa), to the Mathematical Department at Stellenbosch University, and to the School of Mathematics at Tel Aviv University for their financial and material support throughout this work.

I thank and praise the almighty God for proving me strength to proceed successfully. I cordially thank my family (Dad, Mom, sisters and brother) for their deepest love, support and patience during my studies. I always felt their presence even if I was far away from home. "Thank you" to my LePisou for sharing with me courage, love and wonderful way of living life.

This thesis is dedicated to my parents.

Contents

Declaration	i
Abstract	ii
Opsomming	iii
Acknowledgements	iv
Notation	viii
Introduction	1
1 Preliminaries	9
1.1 Topological group homomorphisms	9
1.2 Embedding problems and ramification	10
1.3 A basic set of primes and the reciprocity law	17
1.4 Cohomology groups and special mappings	22
2 Bound on the ramification of homomorphisms	28
2.1 Preliminary result	29
2.2 Isomorphism of $\text{Hom}(\text{Gal}(K), A)$ and $\text{Hom}(C_K, A)$	30
2.3 Construction of $h \in \text{Hom}(\text{Gal}(K), C_l)$	33
2.4 Bound on the ramification of $h \in \text{Hom}(\text{Gal}(K), A)$	40
3 Bound on the ramification of cohomology classes	45
3.1 Definitions and a preliminary result	46

3.2	Corestriction map	47
3.3	Bound on the ramification of 1-cocycles	53
4	Solving embedding problems with bounded ramification	61
4.1	The principal homogeneous space over $H^1(\text{Gal}(K_0), A)$	62
4.2	Embedding problem whose kernel is a simple $\text{Gal}(K_0)$ -module	66
4.3	Embedding problem with solvable kernel	73
4.4	Solving embedding problems with solvable kernels in $K_{0,\text{tot},S}$.	78
	Bibliography	83

Notation

$K =$ a number field.

$\tilde{K} =$ a fixed algebraic closure of K .

$\text{irr}(x, K) =$ the monic irreducible polynomial over K of an element $x \in \tilde{K}$

$\text{Gal}(L/K) =$ the Galois group of a Galois extension L/K .

$\text{Gal}(K) = \text{Gal}(\tilde{K}/K) =$ the absolute Galois group of K .

$\text{res}_{L/K} =$ the restriction map $\text{Gal}(L/K_0) \rightarrow \text{Gal}(K/K_0)$ for a tower of Galois extensions $K_0 \subseteq K \subseteq L$.

$\mathbb{P}(K) =$ the set of all primes of K .

$\mathbb{P}_{\text{fin}}(K) =$ the set of all finite primes of K .

$\mathbb{P}_{\infty}(K) =$ the set of infinite primes of K .

$\hat{K}_{\mathfrak{p}} =$ a fixed completion of K at \mathfrak{p} .

$K_{\mathfrak{p}} =$ a fixed henselization of K at \mathfrak{p} .

$\text{Ram}(L/K) =$ the finite set of primes of K which ramify in L .

$I(L/K) =$ the inertia group of a Galois extension of local fields L/K of characteristic zero.

$\zeta_n =$ a fixed n -th primitive root of unity in \tilde{K} for a positive integer n .

$\mu(K) =$ the set of roots of unity in the field K .

$l =$ a variable for prime numbers.

$C_l =$ the multiplicative cyclic group of order l .

$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z} =$ the Prüfer group.

$\bigcup_{i=1}^n A_i =$ the disjoint union of sets A_1, \dots, A_n .

Introduction

A sharpened version of the inverse Galois problem is the so called **embedding problem**. Given a Galois extension K/K_0 of number fields, a finite group G , and an epimorphism $\alpha: G \rightarrow \text{Gal}(K/K_0)$, one looks for a Galois extension N of K_0 that contains K such that $\text{Gal}(N/K_0) \cong G$ and the restriction map $\text{res}_{N/K}: \text{Gal}(N/K_0) \rightarrow \text{Gal}(K/K_0)$ coincides with α . Equivalently, one looks for a continuous epimorphism $\psi: \text{Gal}(K_0) \rightarrow G$ such that $\alpha \circ \psi = \text{res}_{\tilde{K}_0/K}$. We refer to ψ as a **proper solution** of the embedding problem (whereas, if ψ is only a homomorphism as above, we say that ψ is a **solution** of the embedding problem). The fixed field N of $\text{Ker}(\psi)$ in \tilde{K}_0 is the **solution field** of the embedding problem. The question about the proper solvability of finite embedding problems is of course far from being settled. But, in those cases where an embedding problem as above is solvable, we ask whether a solution field N can be found with a **bound on the ramification**, i.e. bound on the number of the primes of K_0 that are ramified in N .

PREVIOUS WORKS. The combinatorial arguments of Shafarevich in [Sha54] (which was corrected in [Sha89] for $l = 2$) lead for each finite l -group G to a Galois extension N of K with Galois group G such that $|\text{Ram}(N/K)|$ has an exponential growth in $|G|$.

In [GeJ98], Geyer and Jarden use the method of Scholz [Sch37] and Reichardt [Rei37] in order to realize each l -group G over a global field K under the condition $\zeta_l \notin K$. If $|G| = l^n$, they construct a Galois extension N of K with $\text{Gal}(N/K) \cong G$ and $|\text{Ram}(N/K)| \leq n + r(K)$, where $r(K)$ depends only on arithmetical invariants of K . If $K = \mathbb{Q}$ or $K = \mathbb{F}_q(t)$, then $r(K) = 0$, so the result of [GeJ98] reproduces in this case the result of Serre in [Se92] that $|\text{Ram}(N/K)| \leq n$.

The result of [GeJ98] is generalized by Markin and Ullom in [MaU11]. The latter work constructs for each number field K and every finite nilpotent group G a Galois extension N of K with Galois group G . Moreover, if

$(G_i)_i$ is a lower central series of G and $d(G_i/G_{i+1})$ is the minimal number of generators of G_i/G_{i+1} , then $|\text{Ram}(N/K)| \leq \sum_i d(G_i/G_{i+1}) + r(K)$.

Going back to the case of a finite embedding problem $\alpha: G \rightarrow \text{Gal}(K/K_0)$ for number fields, Neukirch observes in [Neu79] that for each prime divisor \mathfrak{p} of K_0 , the completion $\hat{K}_{\mathfrak{p}}/\hat{K}_{0,\mathfrak{p}}$ of K/K_0 at \mathfrak{p} gives rise to a local embedding problem. In the spirit of Scholz-Reichardt, [Neu79] proves that if $\text{Ker}(\alpha)$ is solvable, $\gcd(|\text{Ker}(\alpha)|, |\mu(K)|) = 1$, and each of the local embedding problems is solvable, then the original global embedding problem is properly solvable. Moreover, one may find a proper solution that coincides on $\text{Gal}(\hat{K}_{0,\mathfrak{p}})$ with a given local solution $\varphi_{\mathfrak{p}}$ for finitely many \mathfrak{p} 's. However, [Neu79] gives no bound on the ramification of the proper solution.

THE MAIN RESULT. It is exactly the latter gap that our work intends to fill out. To this end we recall that if $n = \prod_{i=1}^m l_i^{r_i}$ is the decomposition of a positive integer n into a product of powers of distinct primes l_1, \dots, l_m , then $\Omega(n) = \sum_{i=1}^m r_i$. For each $\mathfrak{p} \in \mathbb{P}(K_0)$, we identify $\text{Gal}(\hat{K}_{0,\mathfrak{p}})$ with $\text{Gal}(K_{0,\mathfrak{p}})$ as a subgroup of $\text{Gal}(K_0)$. We prove the following result:

THEOREM A: Let K/K_0 be a finite Galois extension of number fields, set $\Gamma = \text{Gal}(K/K_0)$ and consider a finite embedding problem

$$(0.1.1) \quad \begin{array}{ccccccc} & & & & \text{Gal}(K_0) & & \\ & & & & \downarrow \rho = \text{res}_{\hat{K}_0/K} & & \\ 1 & \longrightarrow & H & \longrightarrow & G & \xrightarrow{\alpha} & \Gamma & \longrightarrow & 1 \end{array}$$

with a solvable kernel H . Suppose that

- (a1) $\gcd(|H|, |\mu(K)|) = 1$ and
- (a2) for each $\mathfrak{p} \in \mathbb{P}(K_0)$ there exists a homomorphism $\psi_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \rightarrow G$ such that $\alpha \circ \psi_{\mathfrak{p}} = \rho|_{\text{Gal}(\hat{K}_{0,\mathfrak{p}})}$ (we call $\psi_{\mathfrak{p}}$ a **local solution**).

Let T be a finite set of primes of K_0 that contains $\text{Ram}(K/K_0)$ and for each $\mathfrak{p} \in T$ let $\varphi_{\mathfrak{p}}$ be a local solution. Then, there exists an epimorphism

$\psi: \text{Gal}(K_0) \rightarrow G$ such that $\alpha \circ \psi = \rho$ and there exists a set $R \subset \mathbb{P}(K_0) \setminus T$ with $|R| = \Omega(|H|)$ that satisfy the following conditions

- (b1) For each $\mathfrak{p} \in T$ there exists $a \in H$ such that $\psi(\sigma) = a^{-1}\varphi_{\mathfrak{p}}(\sigma)a$ for all $\sigma \in \text{Gal}(\hat{K}_{0,\mathfrak{p}})$.
- (b2) The fixed field N in \tilde{K}_0 of $\text{Ker}(\psi)$ satisfies $\text{Ram}(N/K_0) \subseteq T \cup R$, hence $|\text{Ram}(N/K_0)| \leq |T| + \Omega(|H|)$.

SPECIAL CASES. Note that if the short exact sequence in (0.1.1) splits, then the condition in Theorem A about the local solvability is automatically satisfied. Thus in this case, Theorem A holds under the mere conditions that H is solvable and $\text{gcd}(|H|, |\mu(K)|) = 1$.

Also, let S be a finite subset of $\mathbb{P}(K_0)$ and denote the maximal Galois extension of K_0 in which each $\mathfrak{p} \in S$ totally splits by $K_{0,\text{tot},S}$. Suppose that $K \subseteq K_{0,\text{tot},S}$. Then, assume that $S \subseteq T$ and take $\varphi_{\mathfrak{p}}$ for each $\mathfrak{p} \in S$ as the trivial homomorphism. We find that the solution field N of (0.1.1) is contained in $K_{0,\text{tot},S}$.

Finally, we note that if $|G| = l^n$ is an l -group and if we take $K = K_0$, that is Γ is trivial, Theorem A gives a Galois extension N of K with Galois group G such that $|\text{Ram}(N/K)| \leq n$. This improves the estimate of the main result of [GeJ98] mentioned above.

OUTLINE OF THE PROOF OF THEOREM A. We prove the theorem by induction on the order of H . We start with a reduction step.

Part 1: *A reduction step.* We choose a maximal proper subgroup H_1 of H which is normal in G . This breaks up the embedding problem (0.1.1) into two embedding problems. This first one is

$$(0.1.2) \quad \begin{array}{ccccccc} & & G & & \text{Gal}(K_0) & & \\ & & \downarrow \pi & & \downarrow \rho & & \\ 1 & \longrightarrow & H/H_1 & \longrightarrow & G/H_1 & \xrightarrow{\bar{\alpha}} & \Gamma \longrightarrow 1, \end{array}$$

where $\bar{\alpha} \circ \pi = \alpha$ and $\pi: G \rightarrow G/H_1$ is the quotient map.

Part 2: *Induction step.* The second one appears as soon as we find a proper solution $\bar{\psi}: \text{Gal}(K_0) \rightarrow G/H_1$ of embedding problem (0.1.2):

$$(0.1.3) \quad \begin{array}{ccccccc} & & & & \text{Gal}(K_0) & & \\ & & & & \downarrow \bar{\psi} & & \\ 1 & \longrightarrow & H_1 & \longrightarrow & G & \xrightarrow{\pi} & G/H_1 \longrightarrow 1. \end{array}$$

We have $|H_1| < |H|$. But in order to proceed to the induction, we assume that embedding problem (0.1.3) satisfies in its objects conditions (a1) and (a2) of Theorem A. In particular

- (c1) $\gcd(|H_1|, |\mu(\bar{K})|) = 1$ where \bar{K} is the fixed field of $\text{Ker}(\bar{\psi})$ in \tilde{K}_0 ,
- (c2) for each $\mathfrak{p} \in \mathbb{P}(K_0)$ there exists a homomorphism $\psi'_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \rightarrow G$ such that $\pi \circ \psi'_{\mathfrak{p}} = \bar{\psi}|_{\text{Gal}(\hat{K}_{0,\mathfrak{p}})}$, i.e. each local embedding problem is solvable.

The first step of the induction also supplies a finite subset \bar{R} of $\mathbb{P}(K_0) \setminus T$ such that $\text{Ram}(\bar{K}/K_0) \subseteq T \cup \bar{R}$ and $|\bar{R}| = \Omega(|H/H_1|)$.

Replacing T in Theorem A by $T \cup \bar{R}$, an induction hypothesis on the order of the kernel gives a proper solution ψ to embedding problem (0.1.3) that satisfies conclusions (b1) and (b2) of Theorem A, again with respect to the objects associated with (0.1.3). In particular, if N is the fixed field of $\text{Ker}(\psi)$ in \tilde{K}_0 , then there exists a subset R_1 of $\mathbb{P}(K_0) \setminus (T \cup \bar{R})$ such that $|R_1| = \Omega(|H_1|)$ and $\text{Ram}(N/K_0) \subseteq T \cup \bar{R} \cup R_1$. Then, ψ is a solution of (0.1.1) that satisfies (b1) and (b2) for the original embedding problem (0.1.1). Setting $R = \bar{R} \cup R_1$, we have $\text{Ram}(N/K_0) \subseteq T \cup R$ and $|R| = \Omega(|H|)$.

Part 3: *The kernel is a simple module.* The choice of H_1 in Part 1 implies that H/H_1 is a minimal normal subgroup of G/H_1 . Since H is solvable, there exist a prime number l and a positive integer r such that $A = H/H_1 \cong C_l^r$. The action of $\bar{G} = G/H_1$ on A by conjugation makes A a simple multiplicative

Γ -module (via lifting with α), hence also a simple $\text{Gal}(K_0)$ -module (through ρ). The next result strengthens the solvability with bounded ramification of Embedding problem (0.1.2) such that Embedding problem (0.1.3) satisfies the induction hypothesis.

PROPOSITION B: Let K/K_0 be a finite Galois extension of number fields, set $\Gamma = \text{Gal}(K/K_0)$ and $\rho = \text{res}_{\tilde{K}_0/K}$. Then consider the finite embedding problem:

$$(0.1.4) \quad \begin{array}{ccccccc} & & G & & \text{Gal}(K_0) & & \\ & & \downarrow \gamma & & \downarrow \rho & & \\ 1 & \longrightarrow & A & \longrightarrow & \bar{G} & \xrightarrow{\bar{\alpha}} & \Gamma & \longrightarrow & 1, \end{array}$$

with $A \cong C_l^r$ a simple $\text{Gal}(K_0)$ -module and where $\gamma: G \rightarrow \bar{G}$ is an epimorphism of finite groups with a non-trivial solvable kernel. Let n be a multiple of $l|\text{Ker}(\gamma)|$. Suppose

- (d1) $\gcd(n, |\mu(K)|) = 1$,
- (d2) for each $\mathfrak{p} \in \mathbb{P}(K_0)$ there exists a homomorphism $\psi_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \rightarrow \bar{G}$ such that $\bar{\alpha} \circ \psi_{\mathfrak{p}} = \rho|_{\text{Gal}(\hat{K}_{0,\mathfrak{p}})}$.

Let T be a finite subset of $\mathbb{P}(K_0)$ that contains $\text{Ram}(K/K_0)$ and for each $\mathfrak{p} \in T$ let $\bar{\varphi}_{\mathfrak{p}}$ be a local solution. Then, there exists an epimorphism $\bar{\psi}: \text{Gal}(K_0) \rightarrow \bar{G}$ such that $\bar{\alpha} \circ \bar{\psi} = \rho$ and there exists a set $\bar{R} \subset \mathbb{P}(K_0) \setminus T$ with $|\bar{R}| = \Omega(|A|) = r$ that satisfy the following conditions

- (e1) For each $\mathfrak{p} \in T$ there exists $a \in A$ such that $\psi(\sigma) = a^{-1}\bar{\varphi}_{\mathfrak{p}}(\sigma)a$ for all $\sigma \in \text{Gal}(\hat{K}_{0,\mathfrak{p}})$.
- (e2) The fixed field \bar{K} in \tilde{K}_0 of $\text{Ker}(\bar{\psi})$ satisfies $\text{Ram}(\bar{K}/K_0) \subseteq T \cup \bar{R}$.
- (e3) $\gcd(n, |\mu(\bar{K})|) = 1$,
- (e4) for each $\mathfrak{p} \in \mathbb{P}(K_0)$ there exists a homomorphism $\psi'_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \rightarrow G$ such that $\gamma \circ \psi'_{\mathfrak{p}} = \bar{\psi}|_{\text{Gal}(\hat{K}_{0,\mathfrak{p}})}$.

Conditions (e3) and (e4) take care of the induction hypothesis (c1) and (c2) respectively.

Using Condition (d1) (which implies that $\zeta_l \notin K$), Condition (d2) and the assumption that A is a simple $\text{Gal}(K_0)$ -module, we conclude from the local-global principle (Lemma 1.2.8) that there exists a homomorphism $\psi_0: \text{Gal}(K_0) \rightarrow \bar{G}$ such that $\bar{\alpha} \circ \psi_0 = \rho$. However, we still have to adjust ψ_0 such that it will be surjective, to find a subset \bar{R} of $\mathbb{P}(K_0) \setminus T$ such that Condition (e2) holds, and to satisfy Condition (e4). In order to achieve those conditions, we follow [Neu79]. We choose an appropriate crossed homomorphism $\chi: \text{Gal}(K_0) \rightarrow A$, and consider the adjusted solution $\bar{\psi} = \psi_0 \cdot \chi$ of (0.1.4).

In order to make $\bar{\psi}$ surjective, we use the Chebotarev density theorem in order to choose a prime $\mathfrak{q} \in \mathbb{P}(K_0) \setminus T$ that totally splits in $K(\zeta_n)$ and a cyclic unramified homomorphism $\bar{\varphi}_{\mathfrak{q}}: \text{Gal}(\hat{K}_{0,\mathfrak{q}}) \rightarrow \langle a \rangle \leq A$ with $a \neq 1$, such that the solution $\bar{\psi}$ will satisfy $\bar{\psi}|_{\text{Gal}(\hat{K}_{0,\mathfrak{q}})} = \bar{\varphi}_{\mathfrak{q}}$. This implies that $A \cap \text{Im}(\bar{\psi}) \neq 1$. Since A is a simple $\text{Gal}(K_0)$ -module, this together with the assumption that ρ is surjective implies that $\text{Im}(\bar{\psi}) = \bar{G}$, that is $\bar{\psi}$ is a proper solution of (0.1.3) (Lemma 4.2.1).

Moreover, the "ramification of χ " eliminates the "ramification of ψ_0 " up to a set $\bar{R} = \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$ that satisfies $\bar{R} \subset \mathbb{P}(K_0) \setminus T$, $|\bar{R}| = \Omega(|A|)$ and $\text{Ram}(\bar{K}/K_0) \subseteq T \cup \bar{R}$, where \bar{K} is the fixed field in \hat{K}_0 of $\text{Ker}(\bar{\psi})$. The primes \mathfrak{q}_i are chosen by the Chebotarev density theorem. That theorem gives us freedom to choose the \mathfrak{q}_i 's away from T and away from the divisors of l . In addition, the \mathfrak{q}_i 's are also chosen in such a way that $\bar{\psi}|_{\text{Gal}(\hat{K}_{0,\mathfrak{q}_i})}$ is unramified or cyclically ramified.

Next we prove Condition (e4). The choice of the \mathfrak{q}_i 's leaves us with three possibilities for each $\mathfrak{p} \in \mathbb{P}(K_0)$. The first possibility is that $\mathfrak{p} \in T$. In this case Condition (e1) and the properties of the homomorphism γ allows us to lift $\bar{\psi}|_{\text{Gal}(\hat{K}_{0,\mathfrak{p}})}$ to a homomorphism $\psi'_{\mathfrak{p}}$ such that $\gamma \circ \psi'_{\mathfrak{p}} = \bar{\psi}|_{\text{Gal}(\hat{K}_{0,\mathfrak{p}})}$. The second possibility is that $\mathfrak{p} \in \bar{R}$. As mentioned in the previous paragraph, either $\bar{\psi}|_{\text{Gal}(\hat{K}_{0,\mathfrak{p}})}$ is unramified or cyclically ramified, so we can use

Lemma 1.2.6 or Lemma 1.2.7 to lift $\bar{\psi}|_{\text{Gal}(\hat{K}_{0,\mathfrak{p}})}$ to a homomorphism $\psi'_{\mathfrak{p}}$ with $\gamma \circ \psi'_{\mathfrak{p}} = \bar{\psi}|_{\text{Gal}(\hat{K}_{0,\mathfrak{p}})}$. Finally, if $\mathfrak{p} \notin T \cup \bar{R}$, then \mathfrak{p} is unramified in \bar{K} . In this case, we use Lemma 1.2.6 to lift $\bar{\psi}|_{\text{Gal}(\hat{K}_{0,\mathfrak{p}})}$.

THE CROSSED HOMOMORPHISM χ . The construction of the crossed homomorphism χ mentioned in the preceding paragraphs with bounded ramification is a central ingredient of this work. It occupies the greater part of Chapters 2 and 3. The element x of $H^1(\text{Gal}(K_0), A)$ that χ represents is itself a product $x = (\text{cor}_{\text{Gal}(K)}^{\text{Gal}(K_0)} h) \cdot z$, where z is an element of $H^1(\text{Gal}(K_0), H)$ established in Lemma 3.3.4 (due to [Neu79]) and $h: \text{Gal}(K) \rightarrow A$ is a homomorphism produced by Proposition 2.4.1. Note that $\text{Gal}(K)$ acts trivially on A , hence h can be viewed as an element of $H^1(\text{Gal}(K), A)$. Proposition 2.4.1 is one of the main ingredients of the proof of Proposition B. It constructs the homomorphism $h: \text{Gal}(K) \rightarrow A$ with a bound on its ramification that leads to a bound on the ramification of χ , and hence that of $\bar{\psi}$ in Proposition B. It is proved by induction over r starting from Corollary 2.3.6 which is a translation of Lemma 2.3.5 by class field theory. Lemma 2.3.5 itself is modelled after Lemma 7.1 of [GeJ98].

OUTLINE OF THE CONTENTS OF THE CHAPTERS

Chapter 1. Preliminaries. This chapter introduces the basic notions and tools needed in our work. First we explain what embedding problems are and what do we mean by ramification of homomorphisms. Then, we introduce the basic Galois extension K/K_0 and a basic set S_0 of primes of K . Each finite set S of primes of K that contains S_0 satisfies $C_K = I_{K,S}/K_S$, where C_K is the idele class group of K , $I_{K,S}$ is the group of S -ideles, and K_S is the group of S -units. The fourth and last section of the chapter reviews the notion of cohomology groups, the inflation map, and the restriction map.

Chapter 2. Bound on the ramification of homomorphisms. Strengthening a

result of [GeJ98], we construct a homomorphism $h: C_K \rightarrow C_l$ with a bound on its ramification. This bound eventually leads to a bound of the ramification of the solution of the embedding problem we solve in this work. Using class field theory, we establish an isomorphism $\text{Hom}(\text{Gal}(K), A) \cong \text{Hom}(C_K, A)$, where A is an abelian group and use this isomorphism to translate h into a homomorphism from $\text{Gal}(K)$ into A . Finally, in the main new result of the chapter (Proposition 2.4.1), we use induction on r and construct a homomorphism from $\text{Gal}(K)$ to C_l^r with a bound on the ramification.

Chapter 3. *Bound on the ramification of crossed homomorphisms.* We construct a crossed homomorphism $\chi: \text{Gal}(K) \rightarrow A$ with a bound on its ramification, where $A = C_l^r$ is a simple $\text{Gal}(K_0)$ -module. A major tool in the construction is a commutative diagram that involves restriction and corestriction maps. The main new result of this chapter is Proposition 3.3.5.

Chapter 4. *Solving embedding problems with bounded ramification.* This chapter contains the main results of this work. Following [Neu79], we prove in the first section that the set of all solutions of an embedding problem with an abelian kernel A , up to equivalence, is a principal homogeneous space over $H^1(\text{Gal}(K_0), A)$. In particular, the product of a solution and a crossed homomorphism is again a solution. The second section deals with the solution of embedding problems having an abelian kernel which is a simple $\text{Gal}(K/K_0)$ -module. In the third section we carry out the induction step and conclude the proof of the main theorem. The main new results of the chapter are Proposition 4.2.2, Theorem 4.3.2, Theorem 4.4.1, and Corollary 4.4.4.

Chapter 1

Preliminaries

This work is dominated for its large part by class field theory and cohomology theory. The aim of this chapter is to provide the necessary notions about these theories that are used in this work. Also we fix some notations and technical terms about embedding problems and ramification of homomorphisms.

1.1 Topological Group Homomorphisms

First, let us establish some conventions about homomorphisms of topological groups that we will assume for the rest of this work.

Let G and A be topological groups. Subgroups are by definition closed, so $\langle t \rangle$ is the closed subgroup generated by t , for $t \in G$. Every homomorphism $\varphi: G \rightarrow A$ in the category of topological groups is, by definition, continuous. Therefore, whenever we speak about a homomorphism $\varphi: G \rightarrow A$, we tacitely assume that φ is continuous.

In the rare occasions, when φ is constructed from a previously given con-

tinuous homomorphisms and we only know that $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$, then we refer to φ as an "abstract homomorphism".

Whenever A is a finite group, we consider A as a topological group with the discrete topology. In this case, an abstract homomorphism φ from a topological group G to A is a homomorphism if and only if $\text{Ker}(\varphi)$ is open in G .

In particular, if G is a profinite group and A is finite, then an abstract homomorphism $\varphi: G \rightarrow A$ is a homomorphism if and only if $\text{Ker}(\varphi)$ is an open subgroup of G . If, in addition, N/K is a Galois extension and $G = \text{Gal}(N/K)$, then φ is a homomorphism if and only if K has a finite extension L in N with $\varphi(\text{Gal}(N/L)) = 1$.

Next we consider a \mathfrak{p} -adic field F with a valuation v , a ring of integers \mathcal{O} , and a prime element π . Then, $F^\times = \langle \pi \rangle \times U$, where U is the group of units of \mathcal{O} . One knows that U is a profinite group under the \mathfrak{p} -adic topology (Proof of Proposition 5.1, p. 135 of [Neu99]). In particular, for each integer m , the group $\langle \pi^m \rangle U$ is an open subset of F^\times . Therefore, $h(U) = 1$ is a sufficient condition for an abstract homomorphism $h: F^\times \rightarrow A$ to be a homomorphism.

1.2 Embedding Problems and Ramification

In this section we briefly review embedding problems and ramification of homomorphisms. We define the equivalence class of a solution, and give special cases where the local embedding problems have solutions. Recall that every given homomorphism of profinite groups is assumed to be continuous.

Let K_0 be a number field and $\mathfrak{p} \in \mathbb{P}(K_0)$. We write $\hat{K}_{0,\mathfrak{p}}$ for the completion of K_0 at \mathfrak{p} , considering K_0 as a subfield of $\hat{K}_{0,\mathfrak{p}}$. Then we embed \tilde{K}_0 into $\widehat{\tilde{K}_{0,\mathfrak{p}}}$, thereby extending \mathfrak{p} to \tilde{K}_0 . Then $K_{0,\mathfrak{p}} = \tilde{K}_0 \cap \hat{K}_{0,\mathfrak{p}}$ is a Henselian

closure (resp. real closure or algebraic closure) of K_0 with respect to \mathfrak{p} if \mathfrak{p} is nonarchimedean (resp. real or complex). Note that $K_{0,\mathfrak{p}}$ is unique up to K_0 -isomorphism. The absolute Galois group $\text{Gal}(K_{0,\mathfrak{p}})$ of $K_{0,\mathfrak{p}}$ is the absolute decomposition group $D_{\mathfrak{p}}$ of \mathfrak{p} . If $\mathfrak{p} \in \mathbb{P}_{\text{fin}}(K_0)$ then by Krasner's Lemma ([Jar91], Lem. 12.1), $\widetilde{K_0 K_{0,\mathfrak{p}}} = \widehat{K_{0,\mathfrak{p}}}$. If \mathfrak{p} is an infinite real prime, then $\widehat{K_{0,\mathfrak{p}}} = \mathbb{R}$ and $\widetilde{K_0 K_{0,\mathfrak{p}}} = \mathbb{C}$. Hence $\widetilde{K_0 K_{0,\mathfrak{p}}} = \widehat{K_{0,\mathfrak{p}}}$. If \mathfrak{p} is an infinite complex prime, then $\widehat{K_{0,\mathfrak{p}}} = \mathbb{C}$, so $\widetilde{K_0 K_{0,\mathfrak{p}}} = \widehat{K_{0,\mathfrak{p}}}$. It follows that in each case $\text{res}_{\widetilde{K_0 K_{0,\mathfrak{p}}}}: \text{Gal}(\widehat{K_{0,\mathfrak{p}}}) \rightarrow \text{Gal}(K_{0,\mathfrak{p}})$ is an isomorphism. For each $\mathfrak{p} \in \mathbb{P}_{\text{fin}}(K_0)$, we denote $\widehat{K_{0,\mathfrak{p},\text{ur}}}$ the maximal unramified extension of $\widehat{K_{0,\mathfrak{p}}}$ and $\hat{I}_{\mathfrak{p}} = \text{Gal}(\widehat{K_{0,\mathfrak{p},\text{ur}}})$ the inertia group.

Next consider a finite Galois extension K of K_0 and a prime $\mathfrak{p} \in \mathbb{P}_{\text{fin}}(K_0)$. Choose a primitive element x of K/K_0 and let $f = \text{irr}(x, K_0)$. Then, consider the decomposition $f = f_1 \cdots f_m$ of f into irreducible factors over $\widehat{K_{0,\mathfrak{p}}}$. For each $1 \leq i \leq m$ choose a root x_i of f_i in $\widetilde{K_0}$ assuming $x_1 = x$. Then, the map $x \mapsto x_i$ extends the inclusion map $K_0 \rightarrow \widehat{K_{0,\mathfrak{p}}}$ into an embedding $\lambda_i: K \rightarrow \widehat{K_{0,\mathfrak{p}}}(x_i)$. In particular, $\lambda_1: K \rightarrow \widehat{K_{0,\mathfrak{p}}}(x)$ is the inclusion map. We extend λ_i to an embedding $\lambda_i: \widetilde{K_0} \rightarrow \widehat{K_{0,\mathfrak{p}}}$. The \mathfrak{p} -adic valuation $\text{ord}_{\mathfrak{p}}$ of $\widehat{K_{0,\mathfrak{p}}}$ uniquely extends to a discrete valuation of $\widehat{K_{0,\mathfrak{p}}}(x_i)$ that we also denote by $\text{ord}_{\mathfrak{p}}$. Pulling $\text{ord}_{\mathfrak{p}}$ back to K via λ_i defines a prime $\mathfrak{P}_i \in \mathbb{P}(K)$. Specifically, $\text{ord}_{\mathfrak{P}_i}(y) = \text{ord}_{\mathfrak{p}}(\lambda_i(y))$ for each $y \in K$. By [Jan73], p. 88, Thm. 5.1 or [Lan70], p. 38, Thm. 2, $\mathfrak{P}_1, \dots, \mathfrak{P}_m$ are the distinct primes of K that lie over \mathfrak{p} and $\widehat{K_{\mathfrak{P}_i}} = \widehat{K_{0,\mathfrak{p}}}(x_i)$ is a completion of K at \mathfrak{P}_i . Furthermore, $K_{\mathfrak{P}_i} = (\widehat{K_{\mathfrak{P}_i}})^{\lambda_i^{-1}}$ is a Henselization of K at \mathfrak{P}_i and $\text{Gal}(K_{\mathfrak{P}_i})^{\lambda_i} = \text{Gal}(\widehat{K_{\mathfrak{P}_i}})$. Let $\widehat{K_{\mathfrak{P}_i,\text{ur}}}$ be the maximal unramified extension of $\widehat{K_{\mathfrak{P}_i}}$ and $\hat{I}_{\mathfrak{P}_i} = \text{Gal}(\widehat{K_{\mathfrak{P}_i,\text{ur}}})$ the inertia group of \mathfrak{P}_i . Then, $K_{\mathfrak{P}_i,\text{ur}} = (\widehat{K_{\mathfrak{P}_i,\text{ur}}})^{\lambda_i^{-1}}$ is the maximal unramified extension of $K_{\mathfrak{P}_i}$ with absolute Galois group $I_{\mathfrak{P}_i} = \hat{I}_{\mathfrak{P}_i}^{\lambda_i}$.

If \mathfrak{P} is a prime lying over \mathfrak{p} , then $\mathfrak{P} = \mathfrak{P}_i$ for some $1 \leq i \leq m$. We write $\lambda_{\mathfrak{P}}$ for λ_i and $x_{\mathfrak{P}}$ for x_i . Then, $\widehat{K_{\mathfrak{P}}} = \widehat{K_{0,\mathfrak{p}}}(x_{\mathfrak{P}})$, $K_{\mathfrak{P}} = (\widehat{K_{\mathfrak{P}}})^{\lambda_{\mathfrak{P}}^{-1}}$, $\text{Gal}(K_{\mathfrak{P}})^{\lambda_{\mathfrak{P}}} = \text{Gal}(\widehat{K_{\mathfrak{P}}})$, and $I_{\mathfrak{P}}^{\lambda_{\mathfrak{P}}} = \hat{I}_{\mathfrak{P}}$.

Let G be a profinite group and $\psi: \text{Gal}(K_0) \rightarrow G$ a homomorphism. Then, the fixed field N of $\text{Ker}(\psi)$ in \tilde{K}_0 is a Galois extension of K_0 with $\text{Gal}(N/K_0) \leq G$. If ψ is surjective then $\text{Gal}(N/K_0) \cong G$.

Definition 1.2.1. For each homomorphism $\psi: \text{Gal}(K_0) \rightarrow G$ and $\mathfrak{p} \in \mathbb{P}(K_0)$, we define the homomorphism $\psi_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \rightarrow G$ such that $\psi_{\mathfrak{p}}(\sigma) = \psi(\sigma|_{\tilde{K}_0})$

Definition 1.2.2 (Embedding Problem). Let K/K_0 be a Galois extension of number fields, G a profinite group, and $\alpha: G \rightarrow \text{Gal}(K/K_0)$ an epimorphism. The **embedding problem** associated with α consists of embedding K into a Galois extension N of K_0 with an isomorphism $\beta: \text{Gal}(N/K_0) \rightarrow G$ satisfying $\alpha \circ \beta = \text{res}_{N/K}$. It is equivalent to finding a continuous epimorphism $\psi: \text{Gal}(K_0) \rightarrow G$ such that, if $\rho = \text{res}_{\tilde{K}_0/K}$, then $\alpha \circ \psi = \rho$.

$$(1.2.1) \quad \begin{array}{ccccccc} & & & & \text{Gal}(K_0) & & \\ & & & & \downarrow \rho & & \\ & & & \swarrow \psi & & & \\ 1 & \longrightarrow & \text{Ker}(\alpha) & \longrightarrow & G & \xrightarrow{\alpha} & \text{Gal}(K/K_0) \longrightarrow 1 \end{array}$$

A homomorphism ψ that makes the diagram (1.2.1) commute is a **solution** and the fixed field N of $\text{Ker}(\psi)$ is a **solution field** of the embedding problem (we also say ψ is a **Gal(K/K_0)-homomorphism**). The homomorphism ψ is a **proper solution** if it is surjective .

For each $\mathfrak{p} \in \mathbb{P}(K_0)$, the global embedding problem (1.2.1) gives rise to a **local embedding problem**

$$(1.2.2) \quad \begin{array}{ccccccc} & & & & \text{Gal}(\hat{K}_{0,\mathfrak{p}}) & & \\ & & & & \downarrow \rho_{\mathfrak{p}} & & \\ 1 & \longrightarrow & \text{Ker}(\alpha) & \longrightarrow & G_{\mathfrak{p}} & \xrightarrow{\alpha_{\mathfrak{p}}} & \Gamma_{\mathfrak{p}} \longrightarrow 1 \end{array}$$

where $\rho_{\mathfrak{p}}(\sigma) = \rho(\sigma|_{\tilde{K}_0})$ for each $\sigma \in \text{Gal}(\hat{K}_{0,\mathfrak{p}})$, $\Gamma_{\mathfrak{p}} = \rho_{\mathfrak{p}}(\text{Gal}(\hat{K}_{0,\mathfrak{p}}))$, $G_{\mathfrak{p}} = \alpha^{-1}(\Gamma_{\mathfrak{p}})$, $\alpha_{\mathfrak{p}} = \alpha|_{G_{\mathfrak{p}}}$, and $\text{Ker}(\alpha) = \text{Ker}(\alpha_{\mathfrak{p}})$. If ψ is a solution of embedding problem (1.2.1) then $\psi_{\mathfrak{p}}$ (Def. 1.2.1) is a solution of the local embedding

problem (1.2.2).

The solutions of an embedding problem form equivalence classes as follows.

Definition 1.2.3 (Conjugate Homomorphisms). Let $\psi_1: \text{Gal}(K_0) \longrightarrow G$ and $\psi_2: \text{Gal}(K_0) \longrightarrow G$ be homomorphisms that make (1.2.1) commute, that is $\alpha \circ \psi_1 = \alpha \circ \psi_2 = \rho$. We say that ψ_1 and ψ_2 are **Ker(α)-conjugate** if there exists an element $a \in \text{Ker}(\alpha)$ such that

$$(1.2.3) \quad \psi_2(\sigma) = a^{-1}\psi_1(\sigma)a \text{ for all } \sigma \in \text{Gal}(K_0).$$

This is an equivalence relation on the set of the solutions of (1.2.1). We denote by $[\psi_1]$ the equivalence class of ψ_1 . Let $\Gamma = \text{Gal}(K/K_0)$. We denote by $\mathcal{H}\text{om}_{\Gamma, \rho, \alpha}(\text{Gal}(K_0), G)$ the set of all equivalence classes of homomorphisms which make (1.2.1) commute (or Γ -homomorphisms).

Note that if ψ_1 and ψ_2 are **Ker(α)-conjugate**, then $\text{Ker}(\psi_1) = \text{Ker}(\psi_2)$. Thus, every element of an equivalence class $[\psi]$ yields the same solution field of the embedding problem. Also, if ψ is surjective, then so is every element of $[\psi]$. We denote by $\mathcal{H}\text{om}_{\Gamma, \rho, \alpha}(\text{Gal}(K_0), G)_{\text{sur}}$ the subset of all equivalence classes of epimorphisms.

Similarly, let $\psi_{1, \mathfrak{p}}: \text{Gal}(\hat{K}_{0, \mathfrak{p}}) \longrightarrow G$ and $\psi_{2, \mathfrak{p}}: \text{Gal}(\hat{K}_{0, \mathfrak{p}}) \longrightarrow G$ be homomorphisms which make (1.2.2) commute ($\Gamma_{\mathfrak{p}}$ -homomorphisms). Then $\psi_{1, \mathfrak{p}}$ and $\psi_{2, \mathfrak{p}}$ are **Ker($\alpha_{\mathfrak{p}}$)-conjugate** if there exists an element $a \in \text{Ker}(\alpha_{\mathfrak{p}})$ such that

$$(1.2.4) \quad \psi_{2, \mathfrak{p}}(\sigma) = a^{-1}\psi_{1, \mathfrak{p}}(\sigma)a \text{ for all } \sigma \in \text{Gal}(K_{0, \mathfrak{p}}).$$

Note that $\text{Ker}(\alpha) = \text{Ker}(\alpha_{\mathfrak{p}})$. To simplify the notation, we only say that $\psi_{1, \mathfrak{p}}$ and $\psi_{2, \mathfrak{p}}$ are **Ker(α)-conjugate**. We denote by $\mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \alpha_{\mathfrak{p}}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G)$ the set of all equivalence classes $[\psi_{\mathfrak{p}}]$.

Note that if $\psi_1: \text{Gal}(K_0) \longrightarrow G$ and $\psi_2: \text{Gal}(K_0) \longrightarrow G$ are **Ker(α)-conjugate**, then so are $\psi_{1, \mathfrak{p}}$ and $\psi_{2, \mathfrak{p}}$ (Def. 1.2.1), for each $\mathfrak{p} \in \mathbb{P}(K_0)$. Hence, we have

the canonical map

$$(1.2.5) \quad \begin{aligned} \mathcal{H}\text{om}_{\Gamma, \rho, \alpha}(\text{Gal}(K_0), G) &\longrightarrow \prod_{\mathfrak{p}} \mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \alpha_{\mathfrak{p}}}(\text{Gal}(K_{0, \mathfrak{p}}), G) \\ [\psi] &\longmapsto ([\psi_{\mathfrak{p}}])_{\mathfrak{p}}. \end{aligned}$$

Now let us define some properties of a homomorphism.

Definition 1.2.4. Let $\psi: \text{Gal}(K_0) \rightarrow G$ be a homomorphism and let L be the fixed field of $\text{Ker}(\psi)$ in \tilde{K}_0 . Let $\mathfrak{p} \in \mathbb{P}_{\text{fin}}(K_0)$. We say that

- (a) ψ **totally decomposes** at \mathfrak{p} if $\psi_{\mathfrak{p}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}})) = 1$ (i.e. $\psi(K_{0, \mathfrak{p}}) = 1$), that is $L \subseteq K_{0, \mathfrak{p}}$. In this case \mathfrak{p} **totally splits** in L . In the case where L/K_0 is finite, then L has $[L : K_0]$ primes that lie over \mathfrak{p} .
- (b) ψ is **unramified** at \mathfrak{p} if \mathfrak{p} is unramified in L , that is $\psi_{\mathfrak{p}}(\hat{I}_{\mathfrak{p}}) = 1$. We denote the set of primes at which ψ ramifies by $\text{Ram}(\psi)$. Then $\text{Ram}(\psi) = \text{Ram}(L/K_0)$.
- (c) ψ is **cyclic** if it factors through a cyclic extension of K_0 , that is, there exists a cyclic extension K'/K_0 such that $\psi(\text{Gal}(K')) = 1$.

Remark 1.2.5. Note that if a Γ -homomorphism $\psi: \text{Gal}(K_0) \rightarrow G$ is unramified at a prime \mathfrak{p} then each Γ -homomorphism in the equivalence class $[\psi] \in \mathcal{H}\text{om}_{\Gamma, \rho, \alpha}(\text{Gal}(K_0), G)$ is also unramified at \mathfrak{p} since $\text{Ker}(\psi') = \text{Ker}(\psi)$ for each $\psi' \in [\psi]$. In this case we say that $[\psi]$ is **unramified** at \mathfrak{p} . \square

Special local embedding problems. In view of the canonical map (1.2.5), a necessary condition for the global embedding problem (1.2.1) to have a solution is that each corresponding local embedding problem (1.2.2) has a solution.

The following lemma ensures that the local embedding problem (1.2.2) induced by the global embedding problem 1.2.1) has a solution if \mathfrak{p} is unramified in K .

Lemma 1.2.6. Let $\lambda: G \longrightarrow \bar{G}$ be an epimorphism of profinite groups. Let $\mathfrak{p} \in \mathbb{P}(K_0)$, and let $\bar{\psi}_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \longrightarrow \bar{G}$ be an unramified homomorphism. Then, $\bar{\psi}_{\mathfrak{p}}$ can be lifted to an unramified \bar{G} -homomorphism $\psi_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \longrightarrow G$. Thus $\mathcal{H}\text{om}_{\bar{G},\bar{\psi}_{\mathfrak{p}},\lambda}(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), G) \neq \emptyset$.

Proof. Since $\bar{\psi}_{\mathfrak{p}}$ is unramified, there exists a unique homomorphism $\bar{\varphi}_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}})/\hat{I}_{\mathfrak{p}} \longrightarrow \bar{G}$ such that $\bar{\varphi}_{\mathfrak{p}} \circ \pi = \bar{\psi}_{\mathfrak{p}}$, where $\pi: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \longrightarrow \text{Gal}(\hat{K}_{0,\mathfrak{p}})/\hat{I}_{\mathfrak{p}}$ is the quotient map. One knows that $\text{Gal}(\hat{K}_{0,\mathfrak{p}})/\hat{I}_{\mathfrak{p}} \cong \hat{\mathbb{Z}}$ ([Se79], p. 55). Let $\bar{\sigma}$ be the image of $1 \in \hat{\mathbb{Z}}$ under this isomorphism. Let $\bar{g} \in \bar{G}$ such that $\bar{g} = \bar{\varphi}_{\mathfrak{p}}(\bar{\sigma})$, and let $g \in G$ such that $\lambda(g) = \bar{g}$. Define a continuous homomorphism $\bar{\varphi}'_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}})/\hat{I}_{\mathfrak{p}} \longrightarrow G$ by $\bar{\varphi}'_{\mathfrak{p}}(\bar{\sigma}) = g$. Then $\lambda \circ \bar{\varphi}'_{\mathfrak{p}} = \bar{\varphi}_{\mathfrak{p}}$. Consider the continuous homomorphism $\psi_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \xrightarrow{\pi} \text{Gal}(\hat{K}_{0,\mathfrak{p}})/\hat{I}_{\mathfrak{p}} \xrightarrow{\bar{\varphi}'_{\mathfrak{p}}} G$. We have, $\lambda \circ \psi_{\mathfrak{p}} = \lambda \circ \bar{\varphi}'_{\mathfrak{p}} \circ \pi = \bar{\varphi}_{\mathfrak{p}} \circ \pi = \bar{\psi}_{\mathfrak{p}}$. Thus, $\psi_{\mathfrak{p}}$ is a \bar{G} -homomorphism, i.e. $[\psi_{\mathfrak{p}}] \in \mathcal{H}\text{om}_{\bar{G},\bar{\psi}_{\mathfrak{p}},\lambda}(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), G)$.

$$\begin{array}{ccc}
 & \text{Gal}(\hat{K}_{0,\mathfrak{p}}) & \\
 & \downarrow \pi & \\
 & \text{Gal}(\hat{K}_{0,\mathfrak{p}})/\hat{I}_{\mathfrak{p}} & \\
 \psi_{\mathfrak{p}} \swarrow & \downarrow \bar{\varphi}_{\mathfrak{p}} & \searrow \bar{\psi}_{\mathfrak{p}} \\
 G & \xrightarrow{\lambda} & \bar{G}
 \end{array}$$

Moreover, for each $\tau \in \hat{I}_{\mathfrak{p}}$, we have $\psi_{\mathfrak{p}}(\tau) = \bar{\varphi}'_{\mathfrak{p}}(\pi(\sigma)) = \bar{\varphi}'_{\mathfrak{p}}(1) = 1$. Thus $\psi_{\mathfrak{p}}$ is unramified. \square

If the given homomorphism ramifies at the prime \mathfrak{p} , under some other conditions, the case where it is locally cyclic at \mathfrak{p} allows us to solve the corresponding local embedding problem.

Lemma 1.2.7. Let $\lambda: G \rightarrow \bar{G}$ be an epimorphism of profinite groups with finite kernel. Suppose $C_l \leq \bar{G}$. Set $e = |\text{Ker}(\lambda)|$ and let n be a multiple

of el . Let $\mathfrak{p} \in \mathbb{P}(K_0)$ with $\mathfrak{p} \nmid l$. Suppose $\zeta_n \in K_{0,\mathfrak{p}}$. If $\bar{\psi}_{\mathfrak{p}}: \text{Gal}(K_{0,\mathfrak{p}}) \rightarrow C_l \leq \bar{G}$ is ramified ($\bar{\psi}_{\mathfrak{p}}(I_{\mathfrak{p}}) \neq 1$), then $\bar{\psi}_{\mathfrak{p}}$ can be lifted to a \bar{G} -homomorphism $\psi_{\mathfrak{p}}: \text{Gal}(K_{0,\mathfrak{p}}) \rightarrow G$.

$$\begin{array}{ccc} & \text{Gal}(K_{0,\mathfrak{p}}) & \\ & \swarrow \psi_{\mathfrak{p}} & \downarrow \bar{\psi}_{\mathfrak{p}} \\ G' & \xrightarrow{\lambda} & \bar{G} \end{array}$$

Proof. Let $N_{\mathfrak{p}}$ be the fixed field of $\text{Ker}(\bar{\psi}_{\mathfrak{p}})$. Then $N_{\mathfrak{p}}/\hat{K}_{0,\mathfrak{p}}$ is a cyclic ramified extension of degree l . Since $\mathfrak{p} \nmid l$, the ramification is tame. By Proposition 1(i) of ([CaF67], p. 32), there exists a prime element π of $\hat{K}_{0,\mathfrak{p}}$ with $N_{\mathfrak{p}} = \hat{K}_{0,\mathfrak{p}}(\sqrt[l]{\pi})$. Let $\bar{\sigma}$ be a generator of $\text{Gal}(N_{\mathfrak{p}}/\hat{K}_{0,\mathfrak{p}})$ and choose $\sigma \in G$ with $\lambda(\sigma) = \bar{\sigma}$.

Denote the order of σ by d , let $\lambda' = \lambda|_{\langle \sigma \rangle}$, and set $e' = |\text{Ker}(\lambda')|$. Since $\text{Ker}(\lambda')$ is a subgroup of $\text{Ker}(\lambda)$, we have $e'|e$. Since $d = e'l$, $e'|e$ and $el|n$, then $d|n$. Hence, $\zeta_d \in \hat{K}_{0,\mathfrak{p}}$. Thus, $N'_{\mathfrak{p}} = \hat{K}_{0,\mathfrak{p}}(\sqrt[d]{\pi})$ is a cyclic extension of $\hat{K}_{0,\mathfrak{p}}$ of degree d that contains $N_{\mathfrak{p}}$. Since $N_{\mathfrak{p}}$ is the fixed field of $\text{Ker}(\bar{\psi}_{\mathfrak{p}})$, there exists an epimorphism $\bar{\varphi}_{\mathfrak{p}}: \text{Gal}(N'_{\mathfrak{p}}/\hat{K}_{0,\mathfrak{p}}) \rightarrow \text{Gal}(N_{\mathfrak{p}}/\hat{K}_{0,\mathfrak{p}})$ such that $\bar{\psi}_{\mathfrak{p}} = \bar{\varphi}_{\mathfrak{p}} \circ \text{res}_{\hat{K}_{0,\mathfrak{p}}/N'_{\mathfrak{p}}}$.

We choose a generator τ of $\text{Gal}(N'_{\mathfrak{p}}/\hat{K}_{0,\mathfrak{p}})$ such that $\bar{\varphi}_{\mathfrak{p}}(\tau) = \bar{\sigma}$. Consider the homomorphism $h: \text{Gal}(N'_{\mathfrak{p}}/\hat{K}_{0,\mathfrak{p}}) \rightarrow G$ with $h(\tau) = \sigma$. Then, the homomorphism $\psi_{\mathfrak{p}} = h \circ \text{res}_{\hat{K}_{0,\mathfrak{p}}/N'_{\mathfrak{p}}}$ satisfies $\lambda \circ \psi_{\mathfrak{p}} = \bar{\psi}_{\mathfrak{p}}$.

$$\begin{array}{ccccc} & & \text{Gal}(\hat{K}_{0,\mathfrak{p}}) & & \\ & \swarrow \text{res}_{\hat{K}_{0,\mathfrak{p}}/N'_{\mathfrak{p}}} & \downarrow & \searrow \bar{\psi}_{\mathfrak{p}} & \\ \text{Gal}(N'_{\mathfrak{p}}/\hat{K}_{0,\mathfrak{p}}) & \xrightarrow{\bar{\varphi}_{\mathfrak{p}}} & \text{Gal}(N_{\mathfrak{p}}/\hat{K}_{0,\mathfrak{p}}) & & \\ \downarrow h & & \downarrow & & \\ G & \xrightarrow{\lambda} & \bar{G} & & \end{array}$$

□

The condition that each local embedding problem has a solution is not sufficient for the global embedding problem to have a solution. However, under

some additional conditions, we have the following local-global principle.

Lemma 1.2.8 ([Neu79], Lem. 4). Consider the embedding problem (1.2.1). Suppose $\text{Ker}(\alpha) \cong C_l^r$, for some prime number l , is a simple $\text{Gal}(K_0)$ -module (with the action induced by the homomorphism α and then by ρ). If $\zeta_l \notin K$, then

$$\mathcal{H}\text{om}_{\Gamma, \rho, \alpha}(\text{Gal}(K_0), G) \neq \emptyset \text{ if and only if } \prod_{\mathfrak{p}} \mathcal{H}\text{om}_{\Gamma, \rho, \alpha}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G) \neq \emptyset.$$

One of the important tools in bounding the ramification of a solution of an embedding problem is the Chebotarev density theorem.

Chebotarev Density Theorem. Let L/K_0 be a finite Galois extension of Global fields and let \mathcal{C} be a conjugacy class in $\text{Gal}(L/K_0)$. Then the Dirichlet density of $\{\mathfrak{p} \in \mathbb{P}(K_0) \mid \left(\frac{L/K_0}{\mathfrak{p}}\right) = \mathcal{C}\}$ exists and is equal to $\frac{|\mathcal{C}|}{[L: K_0]}$.

The Artin symbol $\left(\frac{L/K_0}{\cdot}\right)$ is defined only for the primes $\mathfrak{p} \in \mathbb{P}(K_0)$ which are unramified in L , so the prime chosen in accordance with the Chebotarev density theorem is consequently unramified ([FrJ08], Thm. 6.3.1).

Note that a prime \mathfrak{p} of K_0 totally splits in L (i.e L has $[L: K_0]$ primes that lie over \mathfrak{p}) if and only if the Frobenius $\left[\frac{L/K_0}{\mathfrak{P}}\right]$ is equal to 1, for $\mathfrak{P} \in \mathbb{P}(L)$ with $\mathfrak{P}|\mathfrak{p}$. Thus, applying the Chebotarev density theorem in the case where $\mathcal{C} = 1$, we conclude that K_0 has infinitely many primes that totally split in L .

1.3 A Basic Set of Primes and the Reciprocity Law

The reciprocity law plays a significant role in the construction of a homomorphism with a bound on its ramification. In this section, we present results from class field theory which we apply in this work. For details, we refer the

reader to chapters 4, 5 and 6 of [Neu99] , or to chapters 6 and 7 of [CaF67].

Let K be a number field and let $\mathfrak{P} \in \mathbb{P}(K)$. If \mathfrak{P} is archimedean, then $\hat{K}_{\mathfrak{P}} = \mathbb{R}$ or $\hat{K}_{\mathfrak{P}} = \mathbb{C}$. In this case, set $U_{\mathfrak{P}} = \hat{K}_{\mathfrak{P}}^{\times}$ and $\pi_{\mathfrak{P}} = 1$. If \mathfrak{P} is nonarchimedean, then $\hat{K}_{\mathfrak{P}}$ is a complete discrete valuation field with a finite residue field. In this case, we denote the corresponding normalized valuation by $v_{\mathfrak{P}}$, and we choose a prime element $\pi_{\mathfrak{P}}$ in $\hat{K}_{\mathfrak{P}}$, that is $v_{\mathfrak{P}}(\pi_{\mathfrak{P}}) = 1$. We set $U_{\mathfrak{P}}$ to be the group of units of $\hat{K}_{\mathfrak{P}}$.

For a finite set S of primes of K such that $\mathbb{P}_{\infty}(K) \subseteq S$, we define the group of S -**units** of K as $K_S = \{x \in K \mid v_{\mathfrak{P}}(x) = 0 \text{ for all } \mathfrak{P} \notin S\}$.

An **idele** of K is an element $\alpha = (\alpha_{\mathfrak{P}})_{\mathfrak{P}} \in \prod_{\mathfrak{P} \in \mathbb{P}(K)} \hat{K}_{\mathfrak{P}}^{\times}$, where $\alpha_{\mathfrak{P}} \in U_{\mathfrak{P}}$ for all but finitely many \mathfrak{P} . The ideles of K form a multiplicative group denoted by I_K . That is, I_K is the restricted product of the multiplicative groups $\hat{K}_{\mathfrak{P}}$ with respect to the subgroups $U_{\mathfrak{P}}$. A basis of neighbourhoods of $1 \in I_K$ is given by the sets

$$\prod_{\mathfrak{P} \in S} V_{\mathfrak{P}} \times \prod_{\mathfrak{P} \notin S} U_{\mathfrak{P}},$$

where S runs over the finite sets of primes of K with $\mathbb{P}_{\infty}(K) \subseteq S$ and $V_{\mathfrak{P}}$ runs over a basis of neighbourhoods of $1 \in \hat{K}_{\mathfrak{P}}^{\times}$. In particular

$$U_K = \prod_{\mathfrak{P} \in \mathbb{P}_K} U_{\mathfrak{P}}$$

is open in I_K . The group I_K is a locally compact topological group ([Neu99], p. 361).

(1.3.1) If A is a finite group, then an abstract homomorphism $h: I_K \rightarrow A$ is continuous if and only if $h(U_{\mathfrak{P}}) = 1$ for almost all $\mathfrak{P} \in \mathbb{P}(K)$ and $h|_{\hat{K}_{\mathfrak{P}}^{\times}}$ is continuous for the rest of the \mathfrak{P} 's.

For a finite set S of primes of K , the group $I_{K,S} = \prod_{\mathfrak{P} \in S} \hat{K}_{\mathfrak{P}}^{\times} \times \prod_{\mathfrak{P} \notin S} U_{\mathfrak{P}}$ is the group of S -**ideles** of K .

The multiplicative group K^\times is embedded diagonally in I_K . Each $x \in K^\times$ corresponds under this embedding to the idele $(x_{\mathfrak{P}})_{\mathfrak{P}}$ with $x_{\mathfrak{P}} = x$ for each $\mathfrak{P} \in \mathbb{P}(K)$. We view K^\times as a subgroup of I_K and call its elements **principal ideles**. The subgroup K^\times is discrete and therefore closed in I_K (Chapter 5, Section 1 of [Neu99]).

The factor group $C_K = I_K/K^\times$ is called the **idele class group** of K . It is a Hausdorff locally compact group ([Neu99], p. 361).

Let J_K and P_K be the group of fractional ideals and principal fractional ideals of K respectively. The **class group** $\text{Cl}_K = J_K/P_K$ is a finite group ([Neu99], p. 36, Thm. 6.3). Its order h_K is the **class number** of K . The connection between idele and ideal classes of K is given by $\text{Cl}_K \cong I_K/U_K K^\times$ (see p. 360, Prop. 1.3 of [Neu99]). This connection implies that each element of C_K can be represented by an S -idele for some finite set S of primes in the following way.

Setup 1.3.1. (Basic Set) Let $\alpha_1, \dots, \alpha_{h_K}$ be representatives of I_K modulo $U_K K^\times$. Let S_0 be the set of infinite primes and all finite primes \mathfrak{P} such that $v_{\mathfrak{P}}(\alpha_{i,\mathfrak{P}}) \neq 0$ for at least one i . Let S be a finite set of primes with $S_0 \subseteq S$. Then $I_K = I_{K,S} K^\times$. Indeed, for an idele $\alpha \in I_K$, there exists $i \in \{1, \dots, h_K\}$ such that $\alpha \in \alpha_i U_K K^\times$. Thus $\alpha = \alpha_i u x$ for some $u \in U_K$ and $x \in K^\times$. Since $S_0 \subseteq S$, for each $\mathfrak{P} \in \mathbb{P}(K) \setminus S$, $v_{\mathfrak{P}}(\alpha_{i,\mathfrak{P}}) = 0$. Hence, $\alpha_i \in I_{K,S}$, so $\alpha_i u \in I_{K,S}$. It follows that $\alpha \in I_{K,S} K^\times$. By definition, $I_{K,S} \cap K^\times = K_S^\times$. Therefore,

$$(1.3.2) \quad C_K = I_{K,S}/K_S^\times$$

See also p. 360, Prop. 1.4 of [Neu99].

Definition. (Basic set) We add the primes of K that divide a fixed prime number l to the set S_0 defined in the preceding paragraph and call it a **basic set** of K .

The following well known Lemma is useful for determining a quotient of the idele class group C_K .

Lemma 1.3.2. Let a be an element of K^\times . We assume that a is an l -power in $\hat{K}_{\mathfrak{P}}$ for every prime $\mathfrak{P} \in \mathbb{P}(K)$. Then, a is an l -power in K .

Proof. Assume toward contradiction that a is not an l -power in K . Then, $X^l - a$ is irreducible over K ([Lan93], p. 297, Thm. 9.1). We denote the splitting field of $X^l - a$ over K by N and choose a root x of $X^l - a$. Then, $H = \text{Gal}(N/K(x))$ is a proper subgroup of $G = \text{Gal}(N/K)$. Hence, $G \setminus \bigcup_{\sigma \in G} H^\sigma$ is a proper subset of G (Lem. 13.3.2, [FrJ08]). By Chebotarev density theorem, K has a prime divisor \mathfrak{P} which is unramified in N such that $\left(\frac{N/K}{\mathfrak{P}}\right) \subseteq G \setminus \bigcup_{\sigma \in G} H^\sigma$. This implies that $X^l - a$ has no root in $\hat{K}_{\mathfrak{P}}$, which is a contradiction. \square

Remark 1.3.3. Let S be a finite set of primes of K with $\mathbb{P}_\infty(K) \subseteq S$ and l a prime number. By Lemma 1.3.2, $K_S \cap I_{K,S}^l = K_S^l$. We use a bar to denote the reduction of elements and subgroups of $I_{K,S}$ modulo $I_{K,S}^l$. Hence,

$$\overline{K_S} = K_S/K_S^l \cong K_S I_{K,S}^l / I_{K,S}^l.$$

Therefore,

$$\overline{I_{K,S}/K_S} \cong (I_{K,S}/I_{K,S}^l) / (K_S I_{K,S}^l / I_{K,S}^l) \cong I_{K,S} / K_S I_{K,S}^l$$

is a quotient of $C_K = I_{K,S}/K_S$ (see equality 1.3.2). \square

Now, let L/K be a finite Galois extension. A basic tool for our work is the Artin reciprocity law:

Proposition 1.3.4 (Global reciprocity law). ([Neu99], p. 391, Thm. 5.5 or [CaF67], p. 172, Thm. 5.1 (B)) For every finite Galois extension L/K of number fields, we have a canonical isomorphism

$$r_{L/K}: \text{Gal}(L/K)^{\text{ab}} \longrightarrow C_K / N_{L/K} C_L$$

where $\text{Gal}(L/K)^{\text{ab}}$ is the maximal abelian factor group of $\text{Gal}(L/K)$. The inverse of $r_{L/K}$ gives the continuous surjective norm residue symbol

$$(\cdot, L/K): C_K \longrightarrow \text{Gal}(L/K)^{\text{ab}}$$

with kernel $N_{L/K}C_L$ (see the definition of $N_{L/K}: C_L \longrightarrow C_K$ in [Neu99], p. 373).

Proposition 1.3.5 (Existence Theorem). ([Neu99], p. 395, Thm. 6.1 or [CaF67], p. 172, Thm. 5.1(D)) The map $L \mapsto N_{L/K}C_L$ is a 1-1 correspondence between the finite abelian extensions L/K and the closed subgroups of finite index in C_K .

Now, suppose L/K is a finite Galois extension of nonarchimedean local fields. Similarly, we have the local reciprocity law.

Proposition 1.3.6 (Local reciprocity law). ([Neu99], p. 320, Thm. 1.3)

- (a) For every finite Galois extension L/K of nonarchimedean local fields, we have an isomorphism

$$r_{L/K}: \text{Gal}(L/K)^{\text{ab}} \longrightarrow K^\times / N_{L/K}L^\times$$

which gives the continuous surjective norm residue symbol

$$(\cdot, L/K): K^\times \longrightarrow \text{Gal}(L/K)^{\text{ab}}$$

with kernel $N_{L/K}L^\times$.

- (b) If L/K is abelian, then $(\cdot, L/K)$ maps the group of units U_K of K onto the inertia group $I(L/K)$ (p. 354, Thm. 6.2, [Neu99]).

The reciprocity law is compatible with the restriction map of finite Galois extensions:

Proposition 1.3.7. ([Neu99], p. 302, Prop. 6.4) Let $K \subseteq L \subseteq L'$ be a tower of finite Galois extension of number fields (resp. of nonarchimedean

local fields). Then we have the commutative diagram:

$$\begin{array}{ccc}
 C_K & \xrightarrow{(\cdot, L'/K)} & \text{Gal}(L'/K)^{\text{ab}} \\
 & \searrow^{(\cdot, L/K)} & \downarrow \text{res} \\
 & & \text{Gal}(L/K)^{\text{ab}}
 \end{array}$$

(resp.

$$\begin{array}{ccc}
 K^\times & \xrightarrow{(\cdot, L'/K)} & \text{Gal}(L'/K)^{\text{ab}} \\
 & \searrow^{(\cdot, L/K)} & \downarrow \text{res} \\
 & & \text{Gal}(L/K)^{\text{ab}} \quad).
 \end{array}$$

We have an embedding of $\hat{K}_{\mathfrak{P}}^\times$ into I_K which associates each element $\alpha \in \hat{K}_{\mathfrak{P}}^\times$ to $(\alpha_\Omega)_\Omega \in I_K$ with $\alpha_{\mathfrak{P}} = \alpha$ and $\alpha_\Omega = 1$ for $\Omega \neq \mathfrak{P}$. Under this embedding, $\hat{K}_{\mathfrak{P}}^\times \cap K^\times = 1$, so we can consider $\hat{K}_{\mathfrak{P}}^\times$ as a subgroup of C_K . Then we have the compatibility of the local and the global reciprocity law.

Proposition 1.3.8. ([Neu99], p. 391, Prop. 5.6) Let L/K be a finite abelian extension of number fields and $\mathfrak{P} \in \mathbb{P}_{\text{fin}}(K)$. Then, the following diagram commutes

$$\begin{array}{ccc}
 \hat{K}_{\mathfrak{P}}^\times & \xrightarrow{(\cdot, \hat{L}_{\mathfrak{P}}/\hat{K}_{\mathfrak{P}})} & \text{Gal}(\hat{L}_{\mathfrak{P}}/\hat{K}_{\mathfrak{P}}) \\
 \downarrow & & \downarrow \\
 C_K & \xrightarrow{(\cdot, L/K)} & \text{Gal}(L/K) .
 \end{array}$$

1.4 Cohomology Groups and Special Mappings

The modules we use in this work are multiplicative and we use exponential notation from the right for the action of the groups on the modules. In contrast, books about cohomology (e.g. [NSW00]) mostly consider additive

modules on which groups act from the left. This difference does not change the essence of the cohomology theory, because the category of left modules is equivalent to the category of right modules. However, the explicit formulas of cochains do change when we go from action from the left to action from the right.

In this section we briefly introduce the basic concepts of cohomology of modules with right action, and some special mappings. Our introduction follows Chapter I of [NSW00].

Let G be a profinite group and A a multiplicative abelian group on which G acts from the right. The image of the action of an element σ of G on an element a of A is written as a^σ .

(A) Continuous Maps ([NSW00], p. 10,11). For each integer $n \geq 0$ the multiplicative group $X^{(n)} = \text{Map}_{\text{cont}}(G^{n+1}, A)$ of all continuous maps $x: G^{n+1} \rightarrow A$, with A carrying the discrete topology, becomes a right G -module by setting

$$x^\tau(\sigma_0, \dots, \sigma_n) = x(\sigma_0\tau^{-1}, \dots, \sigma_n\tau^{-1})^\tau \text{ for } x \in X^{(n)} \text{ and } \tau, \sigma_0, \dots, \sigma_n \in G.$$

The **coboundary operator** $\partial = \partial^n: X^{(n-1)} \rightarrow X^{(n)}$ is defined for each $n \geq 1$ analogously to the case of left modules by

$$(\partial^n x)(\sigma_0, \dots, \sigma_n) = \prod_{i=0}^n x(\sigma_0, \dots, \hat{\sigma}_i, \dots, \sigma_n)^{(-1)^i},$$

where the hat on σ_i hints that σ_i has to be omitted. We also set $\partial^0(a)$ as the constant function $G \rightarrow A$ that maps each $\sigma \in G$ onto a . One proves that the sequence

$$(1.4.1) \quad A \xrightarrow{\partial^0} X^{(0)} \xrightarrow{\partial^1} X^{(1)} \longrightarrow \dots$$

is exact ([NSW00], p. 10, Prop. 1.2.1).

(B) Cochains ([NSW00], p. 11). We write $C^n = C^n(G, A)$ for the group of all n -dimensional **homogeneous cochains**, that is all $x \in X^{(n)}$ that are fixed by G . Thus, $x \in X^{(n)}$ is a homogeneous cochain if and only if it satisfies

$$(1.4.2) \quad x(\sigma_0, \dots, \sigma_n)^\tau = x(\sigma_0\tau, \dots, \sigma_n\tau) \text{ for all } \sigma_0, \dots, \sigma_n, \tau \in G.$$

Note that $\partial^n(C^{n-1}) \leq C^n$. Hence, the exact sequence (1.4.1) gives rise to a **complex**

$$(1.4.3) \quad C^0 \xrightarrow{\partial^1} C^1 \xrightarrow{\partial^2} C^2 \longrightarrow \dots \quad ,$$

i.e. $\partial^{n+1} \circ \partial^n = 1$. In particular, $\text{Im}(\partial^n) \leq \text{Ker}(\partial^{n+1})$ for each $n \geq 0$. We write

$$\begin{aligned} Z^n(G, A) &= \text{Ker}(\partial^{n+1}: C^n(G, A) \longrightarrow C^{n+1}(G, A)) \\ B^n(G, A) &= \text{Im}(\partial^n: C^{n-1}(G, A) \longrightarrow C^n(G, A)) \end{aligned}$$

for the multiplicative groups of (homogeneous) **cocycles** and (homogeneous) **coboundaries**. By definition, $B^0(G, A) = 1$ and we also have $B^n(G, A) \leq Z^n(G, A)$, so we write $H^n(G, A) = Z^n(G, A)/B^n(G, A)$ for the n th **cohomology group** of the G -module A with $H^0(G, A) = A^G = \{a \in A \mid a^g = a \text{ for each } g \in G\}$.

(C) Inhomogeneous cochains ([NSW00], p. 12). We write $\mathcal{C}^0 = \mathcal{C}^0(G, A) = A$ and $\mathcal{C}^n(G, A) = \text{Map}_{\text{cont}}(G^n, A)$ for the group of all **inhomogeneous n -cochains**, $n = 1, 2, \dots$. There is an isomorphism $C^n \longrightarrow \mathcal{C}^n$ that maps each $x \in C^n$ to the inhomogeneous cochains $y \in \mathcal{C}^n$ defined by

$$y = x(1) \text{ for } n = 0 \text{ and } y(\sigma_1, \dots, \sigma_n) = x(\sigma_1\sigma_2, \sigma_1\sigma_2\sigma_3, \dots, \sigma_1\sigma_2 \cdots \sigma_n, \sigma_n, 1) \text{ for } n \geq 1.$$

The inverse map is defined by

$$(1.4.4) \quad x(\sigma_0, \dots, \sigma_n) = y(\sigma_0\sigma_1^{-1}, \sigma_1\sigma_2^{-1}, \dots, \sigma_{n-1}\sigma_n^{-1})^{\sigma_n}.$$

The coboundary operation $\partial^n: C^{n-1} \longrightarrow C^n$ yields by this isomorphism a coboundary operation $\partial^n: \mathcal{C}^{n-1} \longrightarrow \mathcal{C}^n$ that have the following explicit

(inhomogeneous) form:

$$\begin{aligned}
 (\partial^n y)(\sigma_1, \dots, \sigma_n) &= y(\sigma_1, \dots, \sigma_{n-1})^{\sigma_n} \\
 &\cdot y(\sigma_2, \dots, \sigma_n)^{(-1)^n} \\
 &\cdot \prod_{i=1}^{n-1} y(\sigma_1, \dots, \sigma_{i-1}, \sigma_i \sigma_{i+1}, \sigma_{i+2}, \dots, \sigma_n)^{(-1)^i}.
 \end{aligned}$$

In particular,

$$\begin{aligned}
 (1.4.5) \quad (\partial^1 a)(\sigma) &= a^\sigma a^{-1} \text{ for } a \in A = \mathcal{C}^0, \\
 (\partial^2 y)(\sigma_1, \sigma_2) &= y(\sigma_1)^{\sigma_2} \cdot y(\sigma_2) \cdot y(\sigma_1 \sigma_2)^{-1} \text{ for } y \in \mathcal{C}^1.
 \end{aligned}$$

Setting

$$\begin{aligned}
 \mathcal{Z}^n(G, A) &= \text{Ker}(\partial^{n+1}: \mathcal{C}^n(G, A) \longrightarrow \mathcal{C}^{n+1}(G, A)) \\
 \mathcal{B}^n(G, A) &= \text{Im}(\partial^n: \mathcal{C}^{n-1}(G, A) \longrightarrow \mathcal{C}^n(G, A)),
 \end{aligned}$$

the isomorphisms $\mathcal{C}^n(G, A) \longrightarrow \mathcal{C}^n(G, A)$ yield isomorphisms

$$H^n(G, A) \cong \mathcal{Z}^n(G, A) / \mathcal{B}^n(G, A).$$

The groups of cochains $\mathcal{C}^n(G, A)$ (resp. $\mathcal{C}^n(G, A)$) are functors in A . The boundary operators $\partial: \mathcal{C}^{n-1}(G, A) \longrightarrow \mathcal{C}^n(G, A)$ are morphisms between these functors ([NSW00], p. 34, §3). Hence, also the coboundary groups $\mathcal{B}^n(G, A)$ and the cocycles groups $\mathcal{Z}^n(G, A)$ are functorial in A .

As for left modules, each short exact sequence $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ of discrete G -module gives rise for each $n \geq 0$ to a **long exact sequence** of cohomology groups:

$$\begin{aligned}
 0 \rightarrow A^G \rightarrow B^G \rightarrow C^G \xrightarrow{\delta} H^1(G, A) \rightarrow \dots \\
 \dots \rightarrow H^n(G, A) \rightarrow H^n(G, B) \rightarrow H^n(G, C) \xrightarrow{\delta} H^{n+1}(G, A)
 \end{aligned}$$

where δ 's are the **connecting homomorphisms** ([NSW00], p. 26, Thm. 1.3.2).

In this work, particularly in chapter 4, we work with the inhomogeneous

1-cocycles.

(D) The group $H^1(G, A)$ ([NSW00], p. 16). By definitions of $\mathcal{Z}^1(G, A)$ and $\mathcal{B}^1(G, A)$ and from (1.4.5), the inhomogeneous 1-cocycles (**crossed homomorphisms**) are functions $\chi: G \rightarrow A$ such that

$$\chi(\sigma\tau) = \chi(\sigma)^\tau \chi(\tau) \text{ for all } \sigma, \tau \in G,$$

and the inhomogeneous **1-coboundaries** are the functions that satisfy

$$\chi(\sigma) = a^\sigma a^{-1} \text{ for all } \sigma \in G,$$

for some $a \in A$.

Now we assume for the rest of this section that A is a finite G -module. If G acts trivially on A , then $H^1(G, A) = \text{Hom}(G, A)$. Since $\text{Aut}(A)$ is finite and the map $G \rightarrow \text{Aut}(A)$ is continuous, G has an open normal subgroup N such that each $\nu \in N$ acts trivially on A . We claim that an abstract crossed homomorphism χ is continuous exactly when $\text{Ker}(\chi)$ is an open subgroup of G . Indeed, in this case, $H = N \cap \text{Ker}(\chi)$ is an open subgroup of G . Given $\eta \in H$ and $\sigma \in G$, we have $\chi(\sigma\eta) = \chi(\sigma)^\eta \chi(\eta) = \chi(\sigma)$. It follows that $\chi^{-1}(a)$ is an open subset of G for each $a \in A$, as claimed.

(E) Special Mappings ([Rib70], p. 106-134). Let $g: G \rightarrow G'$ be a continuous homomorphism of profinite groups, let A (resp. A') be a G -module (resp. G' -module), and let $f: A' \rightarrow A$ be a group homomorphism. We say that g and f are **compatible** maps if

$$f((a')^{g(\sigma)}) = f(a')^\sigma \text{ for all } \sigma \in G \text{ and } a' \in A'.$$

(1.4.6) Each pair of compatible maps g, f yields homomorphisms of the groups of cochains $(g, f): \mathcal{C}^n(G', A') \rightarrow \mathcal{C}^n(G, A)$, for $n \geq 0$, defined by

$$(g, f)(x')(\sigma_1, \dots, \sigma_n) = f(x'(g(\sigma_1), \dots, g(\sigma_n))).$$

(1.4.7) The homomorphism (g, f) commutes with ∂ and therefore induces homomorphisms $H^n(G', A') \longrightarrow H^n(G, A)$ for $n \geq 0$.

(F) The restriction map. If H is a closed subgroup of G and A a G -module, then A is an H -module. Consider the compatible maps $H \hookrightarrow G$ and $A \xrightarrow{\text{id}} A$. Then, (1.4.6) and (1.4.7) give rise to homomorphisms

$$\text{res}: H^n(G, A) \longrightarrow H^n(H, A), n \geq 0$$

called the **restriction** maps. The restriction maps are functorial in the G -modules, and commute with the connecting homomorphisms ([NSW00], p. 46, Prop. 1.5.2). That is, if $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$ is a short exact sequence of G -modules, then the diagram

$$\begin{array}{ccc} H^n(G, C) & \xrightarrow{\delta} & H^{n+1}(G, A) \\ \text{res} \downarrow & & \downarrow \text{res} \\ H^n(H, C) & \xrightarrow{\delta} & H^{n+1}(H, A) \end{array}$$

is commutative. For $n = 1$, if $x \in H^1(G, A)$ is represented by $\chi: G \rightarrow A$, then $x|_H = \text{res}(x) \in H^1(H, A)$ is represented by $\chi|_H: H \rightarrow A$, with $\chi|_H(\sigma) = \chi(\sigma)$ for all $\sigma \in H$.

(G) The inflation map. Let H be an open normal subgroup of G and let A be a G -module. Then G/H acts continuously on A^H by $a^{\sigma H} = a^\sigma$ for each $\sigma \in G$ and $a \in A^H$, so A^H is a G/H -module. The projection $G \rightarrow G/H$ and the inclusion $A^H \hookrightarrow A$ are compatible maps. Hence, again by (1.4.6) and (1.4.7), they induce homomorphisms

$$\text{inf}: H^n(G/H, A^H) \longrightarrow H^n(G, A), n \geq 0$$

called **inflation** maps.

For $n = 1$, if $\bar{x} \in H^1(G/H, A^H)$ and $\bar{\chi}: G/H \rightarrow A^H$ its representative, then $\chi: G \rightarrow G/H \xrightarrow{\bar{\chi}} A^H \hookrightarrow A$ is a representative of $\text{inf}(\bar{x}) \in H^1(G, A)$. Furthermore, we have the following exact sequence ([NSW00], p. 66, Prop. 1.6.6):

$$(1.4.8) \quad 1 \longrightarrow H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G, A) \xrightarrow{\text{res}} H^1(H, A) .$$

Chapter 2

Bound on the ramification of homomorphisms

In this chapter, we construct a continuous homomorphism $h: \text{Gal}(K) \rightarrow A$, where $A = C_l^r$ for some prime number l and a positive integer r , which coincides with some given local homomorphisms $h_{\mathfrak{P}}: \text{Gal}(\hat{K}_{\mathfrak{P}}) \rightarrow A$, where \mathfrak{P} ranges over a finite set S of primes of K . Moreover, we give a bound on the ramification of h that depends on the finite set S and on r .

The construction of h as above is an essential ingredient in solving a finite embedding problem with solvable kernel and with a bound on the ramification. The first step for this type of embedding problem is to solve an embedding problem with an abelian kernel. Let K/K_0 be a Galois extension of number fields. Consider the embedding problem

$$(2.0.1) \quad \begin{array}{ccccccc} & & & & \text{Gal}(K_0) & & \\ & & & & \downarrow \rho & & \\ 1 & \longrightarrow & A & \longrightarrow & \bar{G} & \xrightarrow{\bar{\alpha}} & \text{Gal}(K/K_0) \longrightarrow 1 \end{array}$$

where A is a simple $\text{Gal}(K/K_0)$ -module. One solves (2.0.1) with bounded ramification in two steps. The first step provides a solution $\psi_0: \text{Gal}(K_0) \rightarrow \bar{G}$ without giving any bound on the ramification. In the second step we multiply ψ_0 by a crossed homomorphism $\chi: \text{Gal}(K_0) \rightarrow A$ and obtain the desired

solution $\bar{\psi} = \psi_0 \cdot \chi$ with an explicit bound on the ramification. For that, the ramification of χ itself has to be bounded. We construct χ in Chapter 3 as the image of h under a certain corestriction map, multiplied by another suitable crossed homomorphism. Both χ and h ramify at most at the same number of primes.

As always, all of our homomorphisms and crossed homomorphisms need to be continuous.

2.1 Preliminary Result

When solving an embedding problem with solvable kernel with bounded ramification, the solution $\bar{\psi}$ of the first step, i.e. an embedding problem with abelian kernel, must satisfy some conditions that ensure the solvability of the resulting embedding problem in the next step. First it has to be compatible with finitely many local solutions which are given in advance. Next, we have to ensure that each local embedding problem arising in the next step is solvable. We do this by using Lemma 1.2.6 and Lemma 1.2.7. This forces us to ensure that each ramified local embedding problem of the next step is cyclic. Finally, we have to bound the ramification of $\bar{\psi}$ (see Def. 1.2.4(b)). These three conditions are inherited by the solution $\bar{\psi}$ from the homomorphism h that we construct in this chapter.

We say that a Galois extension L/K is an **l -extension** if the order of the Galois group $\text{Gal}(L/K)$ is a power of l .

We improve the following result in Lemma 2.3.5, in terms of the choice of the prime $\mathfrak{Q} \in \mathbb{P}(K)$, in order to construct our homomorphism h that satisfies the three conditions described above.

Lemma 2.1.1. ([GeJ98], Lem. 7.1) Let S be a finite set of primes of K which contains the basic set S_0 (Setup 1.3.1). Let L be a finite l -extension

of K and let n be a positive integer. For each $\mathfrak{P} \in S$ let $h_{\mathfrak{P}}: \hat{K}_{\mathfrak{P}} \rightarrow C_l$ be a homomorphism. Suppose $\zeta_l \notin K$. Then there exists a prime $\mathfrak{Q} \in \mathbb{P}(K) \setminus S$ and there exists a continuous homomorphism $h: C_K \rightarrow C_l$ such that

- (a) $L(\zeta_l^n) \subseteq \hat{K}_{\mathfrak{Q}}$,
- (b) for each $\mathfrak{P} \in S$, $h|_{\hat{K}_{\mathfrak{P}}} = h_{\mathfrak{P}}$,
- (c) $h(U_{\mathfrak{Q}}) = C_l$,
- (d) for each $\mathfrak{P} \in \mathbb{P}(K) \setminus (S \cup \{\mathfrak{Q}\})$, $h(U_{\mathfrak{P}}) = 1$.

2.2 Isomorphism of $\text{Hom}(\text{Gal}(K), A)$ and $\text{Hom}(C_K, A)$

The construction of the homomorphism $h: \text{Gal}(K) \rightarrow A$ with $A \cong C_l^n$ starts with the construction of a homomorphism $\bar{h}: C_K \rightarrow A$, as in Lemma 2.1.1, where C_K is the idele class group of K . An application of a natural isomorphism $\psi: \text{Hom}(\text{Gal}(K), A) \rightarrow \text{Hom}(C_K, A)$ then gives the desired h . In this section we define the isomorphism ψ by using the reciprocity law (Section 1.3).

Every homomorphism from C_K and $\hat{K}_{\mathfrak{P}}^{\times}$ (as a subgroup of C_K) is tacitly assumed to be continuous. We identify the Galois group $\text{Gal}(\hat{K}_{\mathfrak{P}})$ with the Galois group $\text{Gal}(K_{\mathfrak{P}})$ as a subgroup of $\text{Gal}(K)$. Let Hom be the functor of continuous homomorphisms. The local and global reciprocity law give rise to the following commutative diagram.

Lemma 2.2.1. Let A be a finite abelian group and let \mathfrak{P} be a prime of K . Then there is a commutative diagram

$$\begin{array}{ccc} \text{Hom}(\text{Gal}(K), A) & \xrightarrow{\psi} & \text{Hom}(C_K, A) \\ \text{res}_{\mathfrak{P}} \downarrow & & \downarrow \\ \text{Hom}(\text{Gal}(\hat{K}_{\mathfrak{P}}), A) & \xrightarrow{\psi_{\mathfrak{P}}} & \text{Hom}(\hat{K}_{\mathfrak{P}}^{\times}, A) \end{array} ,$$

where the left vertical map is the restriction map defined by $\text{res}_{\mathfrak{P}}(h)(\sigma) = h(\sigma^{\lambda_{\mathfrak{P}}^{-1}})$ for each $h \in \text{Hom}(\text{Gal}(K), A)$ and $\sigma \in \text{Gal}(\hat{K}_{\mathfrak{P}})$ (see the definition of $\lambda_{\mathfrak{P}}$ in Section 1.2), the right vertical map is the natural restriction map, and the horizontal maps are the isomorphisms induced by the global reciprocity map and the local reciprocity map. Furthermore, if \mathfrak{P} is finite and if $f \in \text{Hom}(\text{Gal}(\hat{K}_{\mathfrak{P}}), A)$ then $\psi_{\mathfrak{P}}(f)(U_{\mathfrak{p}}) = f(\hat{I}_{\mathfrak{P}})$.

Proof. Part A: *Definition of the ψ .* Let $\psi: \text{Hom}(\text{Gal}(K), A) \rightarrow \text{Hom}(C_K, A)$ be the map defined by $\psi(f) = f_1$ for a homomorphism $f: \text{Gal}(K) \rightarrow A$, where $f_1: C_K \xrightarrow{(\cdot, L_1/K)} \text{Gal}(L_1/K) \xrightarrow{\bar{f}_1} A$ such that L_1/K is an arbitrary finite abelian extension with $f(\text{Gal}(L_1)) = 1$ and $\bar{f}_1: \text{Gal}(L_1/K) \rightarrow A$ is the unique homomorphism satisfying $\bar{f}_1 \circ \text{res}_{\bar{K}/L_1} = f$ with $\text{res}_{\bar{K}/L_1}: \text{Gal}(K) \rightarrow \text{Gal}(L_1/K)$ the restriction map. The map ψ is well defined. Indeed, let L_2/K be another finite abelian extension with $f(\text{Gal}(L_2)) = 1$, and let $f_2: C_K \xrightarrow{(\cdot, L_2/K)} \text{Gal}(L_2/K) \xrightarrow{\bar{f}_2} A$ be the corresponding image. The extension L_1L_2/K is also finite abelian and $f(\text{Gal}(L_1L_2)) = 1$, so we can consider the corresponding image $f_{12}: C_K \xrightarrow{(\cdot, L_1L_2/K)} \text{Gal}(L_1L_2/K) \xrightarrow{\bar{f}_{12}} A$. Then, by Proposition 1.3.7, the following diagram commutes:

$$\begin{array}{ccc}
 \text{Gal}(K) & \xrightarrow{f} & A \\
 \searrow^{\text{res}_{\bar{K}/L_1L_2}} & & \nearrow^{\bar{f}_{12}} \\
 C_K & \xrightarrow{(\cdot, L_1L_2/K)} & \text{Gal}(L_1L_2/K) \\
 \searrow^{(\cdot, L_1/K)} & & \downarrow^{\text{res}_{L_1L_2/L_1}} \\
 & & \text{Gal}(L_1/K) \\
 \nearrow^{\text{res}_{\bar{K}/L_1}} & & \nearrow^{\bar{f}_1}
 \end{array}$$

That is $f_1 = \bar{f}_1 \circ (\cdot, L_1/K)$ is equal to $f_{12} = \bar{f}_{12} \circ (\cdot, L_1L_2/K)$. Similarly $f_2 = f_{12}$. Hence $f_1 = f_2$ as desired.

Part B: *The map ψ is a homomorphism.* Let $f, g \in \text{Hom}(\text{Gal}(K), A)$ and L/K a finite abelian extension with $f(\text{Gal}(L)) = g(\text{Gal}(L)) = 1$. Then $\psi(f): C_K \xrightarrow{(\cdot, L/K)} \text{Gal}(L/K) \xrightarrow{\bar{f}} A$ and $\psi(g): C_K \xrightarrow{(\cdot, L/K)} \text{Gal}(L/K) \xrightarrow{\bar{g}} A$. Moreover $fg(\text{Gal}(L)) = 1$, so $\psi(fg): C_K \xrightarrow{(\cdot, L/K)} \text{Gal}(L/K) \xrightarrow{\bar{fg}} A$ with $\bar{fg} = \bar{f}\bar{g}$. It follows that for each $\alpha \in C_K$, $\psi(fg)(\alpha) = \bar{fg}((\alpha, L/K)) =$

$\bar{f}((\alpha, L/K))\bar{g}((\alpha, L/K)) = \psi(f)(\alpha)\psi(g)(\alpha)$. Therefore ψ is a homomorphism.

Part C: *Injectivity of ψ* . Let $f \in \text{Hom}(\text{Gal}(K), A)$ and let L be the fixed field of $\text{Ker}(f)$, that is $\text{Ker}(f) = \text{Gal}(L)$. Then, $\text{Gal}(L/K)$ is abelian. If $\psi(f) = 1$, then for each $\alpha \in C_K$, $\bar{f}(\alpha, L/K) = 1$. Since $(\cdot, L/K)$ is surjective (Theorem 1.3.4), $\bar{f} = 1$, so $f = 1$. Therefore ψ is injective.

Part D: *Surjectivity of ψ* . Let $f_1: C_K \rightarrow A$ be a continuous homomorphism. In particular, $\text{Ker}(f_1)$ is an open subgroup of C_K . By Theorem 1.3.5, K has a finite abelian extension L such that $N_{L/K}C_L = \text{Ker}(f_1)$. Hence by Theorem 1.3.4, $(\cdot, L/K): C_K \rightarrow \text{Gal}(L/K)$ is an epimorphism whose kernel is $\text{Ker}(f_1)$. Thus, there exists a homomorphism $\bar{f}: \text{Gal}(L/K) \rightarrow A$ such that $\bar{f} \circ (\cdot, L/K) = f_1$. Then by definition, $f = \bar{f} \circ \text{res}$, with $\text{res}: \text{Gal}(K) \rightarrow \text{Gal}(L/K)$, satisfies $\psi(f) = f_1$. So ψ is surjective.

Part E: *Commutativity of the diagram*. We define $\psi_{\mathfrak{p}}: \text{Hom}(\text{Gal}(\hat{K}_{\mathfrak{p}}), A) \rightarrow \text{Hom}(\hat{K}_{\mathfrak{p}}, A)$ in a similar way to ψ : for each continuous homomorphism $f \in \text{Hom}(\text{Gal}(\hat{K}_{\mathfrak{p}}), A)$ we choose a finite abelian extension L of $\hat{K}_{\mathfrak{p}}$ such that $f(\text{Gal}(L)) = 1$. Let $\bar{f}: \text{Gal}(L/\hat{K}_{\mathfrak{p}}) \rightarrow A$ be the unique homomorphism such that $\bar{f} \circ \text{res}_{\hat{K}_{\mathfrak{p}}/L} = f$. Then, we set $\psi_{\mathfrak{p}}(f) = \bar{f} \circ (\cdot, L/\hat{K}_{\mathfrak{p}})$. The proof that $\psi_{\mathfrak{p}}$ is a well defined isomorphism is done as for ψ , using the local class field theory (Theorem 1.3.6(a)). The commutativity of the diagram follows from Proposition 1.3.8.

Part F: *We prove that $\psi(f)(U_{\mathfrak{p}}) = f(\hat{I}_{\mathfrak{p}})$* . For each $\alpha \in U_{\mathfrak{p}}$ we have by Theorem 1.3.6(b), that $(\alpha, L/\hat{K}_{\mathfrak{p}}) \in I(L/\hat{K}_{\mathfrak{p}})$. Let $\sigma \in \hat{I}_{\mathfrak{p}}$ with $\sigma|_L = (\alpha, L/\hat{K}_{\mathfrak{p}})$. Then

$$(2.2.1) \quad \psi_{\mathfrak{p}}(f)(\alpha) = \bar{f}((\alpha, L/\hat{K}_{\mathfrak{p}})) = \bar{f}(\sigma|_L) = f(\sigma).$$

Thus, $\psi_{\mathfrak{p}}(f)(U_{\mathfrak{p}}) \subseteq f(\hat{I}_{\mathfrak{p}})$.

Conversely, for each $\sigma \in \hat{I}_{\mathfrak{P}}$ there exists $\alpha \in U_{\mathfrak{P}}$ with $(\alpha, L/\hat{K}_{\mathfrak{P}}) = \sigma|_L$. By (2.2.1), $f(\sigma) = \psi_{\mathfrak{P}}(f)(\alpha)$. Hence, $f(\hat{I}_{\mathfrak{P}}) \subseteq \psi_{\mathfrak{P}}(f)(U_{\mathfrak{P}})$, as claimed. \square

2.3 Construction of $h \in \text{Hom}(\text{Gal}(K), C_l)$

Let K/K_0 be a finite Galois extension of number fields. For every finite set S of primes of K with $S_0 \subseteq S$ and homomorphisms $h_{\mathfrak{P}}: \hat{K}_{\mathfrak{P}}^{\times} \rightarrow C_l$ for each $\mathfrak{P} \in S$, we construct a continuous homomorphism $h: C_K \rightarrow C_l$ such that $h|_{\hat{K}_{\mathfrak{P}}^{\times}} = h_{\mathfrak{P}}$ for each $\mathfrak{P} \in S$ and $h(U_{\mathfrak{P}}) = 1$ for each $\mathfrak{P} \in \mathbb{P}_K \setminus (S \cup \{\mathfrak{Q}\})$ for some $\mathfrak{Q} \in \mathbb{P}_K \setminus S$. The construction is carried out as in Lemma 2.1.1. However, we first choose a prime $\mathfrak{q} \in \mathbb{P}(K_0)$ and a prime $\mathfrak{Q} \in \mathbb{P}(K)$ that lies over \mathfrak{q} and satisfies the conditions of the Lemma. This choice gives us the freedom we need in the solution of an embedding problem with kernel C_l^r in Chapter 4. In the construction, we use the equality $I_K = I_{K,S}K^{\times}$, so we assume throughout this section that $S_0 \subseteq S$.

Let S be a finite set of primes of K . We say that $a_1, \dots, a_s \in K_S$ are **multiplicatively independent** modulo K_S^l if for all $l_1, \dots, l_s \in \mathbb{Z}$ and $b \in K_S$, the equality $a_1^{l_1} \cdots a_s^{l_s} = b^l$ implies that $l|l_i$ for $i = 1, \dots, s$.

We start with some elementary results.

Lemma 2.3.1. ([GeJ98], Lem. 5.2) Let S be a finite set of primes of K and l a prime number. If $a_1, \dots, a_s \in K_S$ are multiplicatively independent modulo K_S^l , then the fields $K(\zeta_l, \sqrt[l]{a_1}), \dots, K(\zeta_l, \sqrt[l]{a_s})$ are linearly disjoint and of degree l over $K(\zeta_l)$. Let n be a positive integer. If L/K is an l -extension and $\zeta_l \notin K$, then the fields $L(\zeta_{l^n}, \sqrt[l]{a_1}), \dots, L(\zeta_{l^n}, \sqrt[l]{a_s})$ are linearly disjoint and of degree l over $L(\zeta_{l^n})$.

Lemma 2.3.2. Let S be a finite set of primes of K , l a prime number and assume that $\zeta_l \notin K$. Let a_1, \dots, a_s be multiplicatively independent elements of K_S modulo K_S^l . Let L be an l -extension of K and let m be a

positive integer. Let M be a finite abelian extension of K . Then, the fields $LM(\zeta_{l^m}, \sqrt[l]{a_1}), \dots, LM(\zeta_{l^m}, \sqrt[l]{a_s})$ are linearly disjoint extensions of $LM(\zeta_{l^m})$ of degree l .

Proof. We may write $M = M'M''$, where M' is an abelian l -extension of K , and M'' is an abelian extension of K whose degree is not divisible by l . Then, $L' = LM'$ is a finite l -extension of K . Applying Lemma 2.3.1 to L' , we find that $L'(\zeta_{l^m}, \sqrt[l]{a_1}), \dots, L'(\zeta_{l^m}, \sqrt[l]{a_s})$ are linearly disjoint extensions of $L'(\zeta_{l^m})$ of degree l . In particular, $N = L'(\zeta_{l^m}, \sqrt[l]{a_1}, \dots, \sqrt[l]{a_s})$ is an l -extension of K . Since $l \nmid [M'' : K]$, the field M'' is linearly disjoint from N over K . Hence $LM(\zeta_{l^m}, \sqrt[l]{a_1}), \dots, LM(\zeta_{l^m}, \sqrt[l]{a_s})$ are linearly disjoint extensions of $LM(\zeta_{l^m})$ of degree l . \square

Remark 2.3.3. Let n be a multiple of l^m . Using the notation of Lemma 2.3.2, suppose L/K is a finite abelian l -extension. Then $M = L(\zeta_n)$ is a finite abelian extension of K . It follows that the fields

$$LM(\zeta_{l^m}, \sqrt[l]{a_1}) = M(\sqrt[l]{a_1}), \dots, M(\sqrt[l]{a_s}) = L(\zeta_n, \sqrt[l]{a_s})$$

are linearly disjoint extensions of $M(\zeta_{l^m}) = L(\zeta_n)$ of degree l . \square

Lemma 2.3.4. ([GeJ98], Lem. 4.1) Let l be a prime number and $\Omega \in \mathbb{P}(K)$ with $\Omega \nmid l, \infty$. Suppose that $\zeta_l \in \hat{K}_\Omega$. Then $U_\Omega/U_\Omega^l \cong C_l$.

The following Lemma strengthens Lemma 2.1.1 in terms of the choice of the prime \mathfrak{q} . Specifically, [GeJ98] chooses $\Omega \in \mathbb{P}(K)$ which totally splits in $L(\zeta_{l^m})$, with L/K_0 is a finite Galois extension such that L/K is abelian l -extension. Instead, we choose a prime $\mathfrak{q} \in \mathbb{P}(K_0)$ that totally splits in $L(\zeta_n)$ for a multiple n of l^m .

Lemma 2.3.5. Let $K_0 \subseteq K \subseteq L$ be a tower of finite Galois extensions of number fields such that L/K is abelian l -extension and L/K_0 is Galois. Suppose $\zeta_l \notin K$. Let S be a finite set of primes of K which contains S_0 . Let $n = ql^m$ be a positive integer multiple of l^m for some positive integers

q and m . For each $\mathfrak{P} \in S$ let $h_{\mathfrak{P}}: \hat{K}_{\mathfrak{P}}^{\times} \rightarrow C_l$ be a homomorphism. Then there exists a prime $\mathfrak{q} \in \mathbb{P}(K_0) \setminus S|_{K_0}$ and there exists a homomorphism $h: C_K \rightarrow C_l$ such that:

- (a) \mathfrak{q} totally splits in $L(\zeta_n)$,
- (b) $h|_{\hat{K}_{\mathfrak{P}}^{\times}} = h_{\mathfrak{P}}$ for each $\mathfrak{P} \in S$,
- (c) there exists $\mathfrak{Q} \in \mathbb{P}(K)$ such that $\mathfrak{Q}|_{K_0} = \mathfrak{q}$ and $h(U_{\mathfrak{Q}}) = C_l$, and
- (d) $h(U_{\mathfrak{P}}) = 1$ for each $\mathfrak{P} \in \mathbb{P}(K) \setminus (S \cup \{\mathfrak{Q}\})$.

Proof. We break the proof into several parts.

PART A: *Continuity.* Each abstract homomorphism $h: C_K \rightarrow C_l$ that satisfies (a), (b), (c), and (d) is continuous, hence a homomorphism in the sense of Section 1.1. Indeed, by (d), $h(U_{\mathfrak{P}}) = 1$ for each $\mathfrak{P} \in \mathbb{P}(K) \setminus (S \cup \{\mathfrak{Q}\})$. By (b), $h|_{\hat{K}_{\mathfrak{P}}^{\times}} = h_{\mathfrak{P}}$ is continuous for each $\mathfrak{P} \in S$. Hence, by the statement (1.3.1), it suffices to prove that $h|_{\hat{K}_{\mathfrak{Q}}^{\times}}$ is continuous.

Since $U_{\mathfrak{Q}}$ is a profinite group (Section 1.1) and raising elements to the l th power is continuous, $U_{\mathfrak{Q}}^l$ is closed in $U_{\mathfrak{Q}}$. Since each prime of K dividing l is in $S_0 \subseteq S$ (Setup 1.3.1), $\mathfrak{Q} \nmid l, \infty$. By (a), $\zeta_l \in \hat{K}_{\mathfrak{Q}}^{\times}$. Hence, by Lemma 2.3.4, $U_{\mathfrak{Q}}/U_{\mathfrak{Q}}^l \cong C_l$. Therefore, $U_{\mathfrak{Q}}^l$ is an open subgroup of $U_{\mathfrak{Q}}$. Let $\pi_{\mathfrak{Q}}$ be a prime element of the valuation ring of $\hat{K}_{\mathfrak{Q}}$. Then, $\hat{K}_{\mathfrak{Q}}^{\times} \cong \langle \pi_{\mathfrak{Q}} \rangle \times U_{\mathfrak{Q}}$. Hence, by Section 1.1, $(\hat{K}_{\mathfrak{Q}}^{\times})^l \cong \langle \pi_{\mathfrak{Q}}^l \rangle \times U_{\mathfrak{Q}}^l$ is an open subgroup of $\hat{K}_{\mathfrak{Q}}^{\times}$. Finally, there is a commutative diagram

$$\begin{array}{ccc} \hat{K}_{\mathfrak{Q}}^{\times} & \xrightarrow{h|_{\hat{K}_{\mathfrak{Q}}^{\times}}} & C_l \\ \pi \downarrow & & \uparrow \eta \\ \hat{K}_{\mathfrak{Q}}^{\times}/(\hat{K}_{\mathfrak{Q}}^{\times})^l & \xrightarrow{\theta} & \mathbb{Z}/l\mathbb{Z} \times U_{\mathfrak{Q}}/U_{\mathfrak{Q}}^l \end{array}$$

where π is the quotient map, θ is an isomorphism, and η is a homomorphism. Since $(\hat{K}_{\mathfrak{Q}}^{\times})^l$ is an open subgroup of $\hat{K}_{\mathfrak{Q}}^{\times}$, π is continuous. Since all groups

appearing in the diagram but \hat{K}_Ω^\times are finite, θ and η are continuous. It follows that $h|_{\hat{K}_\Omega^\times}$ is continuous, as claimed.

PART B: *Reduction of the lemma to constructing a continuous homomorphism $g: \overline{I_{K,S}}/\overline{K_S} \rightarrow C_l$.* By the unit theorem, K_S is finitely generated ([CaF67], p. 72), hence $(K_S : K_S^l) = l^s$ for some positive integer s . Choose multiplicatively independent generators a_1, \dots, a_s of K_S modulo K_S^l . For each $\Omega \in \mathbb{P}(K) \setminus S$ we can decompose $I_{K,S}$ as

$$I_{K,S} = \prod_{\mathfrak{p} \in S} \hat{K}_\mathfrak{p}^\times \times U_\Omega \times \prod_{\mathfrak{p} \notin S \cup \{\Omega\}} U_\mathfrak{p}.$$

Use a bar to denote the reduction of elements and subgroups of $I_{K,S}$ modulo $I_{K,S}^l$. In particular

$$(2.3.1) \quad \overline{I_{K,S}} = \prod_{\mathfrak{p} \in S} \overline{\hat{K}_\mathfrak{p}^\times} \times \overline{U_\Omega} \times \prod_{\mathfrak{p} \notin S \cup \{\Omega\}} \overline{U_\mathfrak{p}},$$

and

$$(2.3.2) \quad \overline{K_S} = \langle \bar{a}_1, \dots, \bar{a}_s \rangle.$$

Also, for each $\mathfrak{p} \in S$ the homomorphism $h_\mathfrak{p}: \hat{K}_\mathfrak{p}^\times \rightarrow C_l$ induces a homomorphism $\bar{h}_\mathfrak{p}: \overline{\hat{K}_\mathfrak{p}^\times} \rightarrow C_l$. Since $\overline{I_{K,S}}/\overline{K_S}$ is a quotient of $C_K = I_{K,S}/K_S$ (Remark 1.3.3), it suffices to find a prime $\mathfrak{q} \in \mathbb{P}(K_0) \setminus S|_{K_0}$ which satisfies (a) and to construct a homomorphism $g: \overline{I_{K,S}} \rightarrow C_l$ such that

$$(2.3.3) \quad g|_{\overline{\hat{K}_\mathfrak{p}^\times}} = \bar{h}_\mathfrak{p} \text{ for each } \mathfrak{p} \in S,$$

$$(2.3.4) \quad g(\overline{U_\Omega}) = C_l \text{ for some prime } \Omega \in \mathbb{P}(K) \text{ that lies over } \mathfrak{q},$$

$$(2.3.5) \quad g(\overline{U_\mathfrak{p}}) = 1 \text{ for each } \mathfrak{p} \in \mathbb{P}(K) \setminus (S \cup \{\Omega\}),$$

$$(2.3.6) \quad g(\bar{a}_i) = 1 \text{ for } i = 1, \dots, s$$

By (2.3.2) and (2.3.6), g will induce a homomorphism $\bar{g}: \overline{I_{K,S}}/\overline{K_S} \rightarrow C_l$ which will compose with the quotient map $C_K \rightarrow \overline{I_{K,S}}/\overline{K_S}$ to the desired

homomorphism h .

PART C: *Presentation of \bar{a}_i as an idele.* For each i between 1 and s and each $\mathfrak{P} \in \mathbb{P}(K)$, let $a_{i\mathfrak{P}}$ be a_i considered as an element of $\hat{K}_{\mathfrak{P}}^{\times}$ and let

$$(2.3.7) \quad \delta_i = \prod_{\mathfrak{P} \in S} \bar{h}_{\mathfrak{P}}(\bar{a}_{i\mathfrak{P}})$$

If $\mathfrak{q} \in \mathbb{P}(K_0)$ satisfies (a) and $\mathfrak{q} \nmid l, \infty$, then we choose $\mathfrak{Q} \in \mathbb{P}(K)$ over \mathfrak{q} . Then, \mathfrak{Q} totally splits in $L(\zeta_l)$. It follows that $a_1, \dots, a_s, \zeta_l \in U_{\mathfrak{Q}}$ and $\overline{U}_{\mathfrak{Q}} \cong C_l$ (Lemma 2.3.4). Choose a generator $\bar{u}_{\mathfrak{Q}}$ of $\overline{U}_{\mathfrak{Q}}$. For each i there exists then $0 \leq \beta_i < l$ such that $\bar{a}_{i\mathfrak{Q}} = \bar{u}_{\mathfrak{Q}}^{\beta_i}$. The representation of \bar{a}_i as an idele will therefore take the form:

$$(2.3.8) \quad \bar{a}_i = \prod_{\mathfrak{P} \in S} \bar{a}_{i\mathfrak{P}} \cdot \bar{u}_{\mathfrak{Q}}^{\beta_i} \cdot \prod_{\mathfrak{P} \notin S \cup \{\mathfrak{Q}\}} \bar{a}_{i\mathfrak{P}}.$$

Conditions (2.3.3) and (2.3.5) force that

$$(2.3.9) \quad \begin{aligned} g(\bar{a}_{i\mathfrak{P}}) &= \bar{h}_{\mathfrak{P}}(\bar{a}_{i\mathfrak{P}}) \text{ for } \mathfrak{P} \in S \text{ and} \\ g(\bar{a}_{i\mathfrak{P}}) &= 1 \text{ for } \mathfrak{P} \in \mathbb{P}(K) \setminus (S \cup \{\mathfrak{Q}\}). \end{aligned}$$

Condition (2.3.4) is equivalent to $g(\bar{u}_{\mathfrak{Q}}) \neq 1$. We have therefore to choose \mathfrak{q} such that, in addition to (2.3.9), (a) will hold and to define $g(\bar{u}_{\mathfrak{Q}})$ as a non-trivial element of C_l such that (2.3.6) will be satisfied.

Let N be the Galois closure of $L(\zeta_n, \sqrt[l]{a_1}, \dots, \sqrt[l]{a_s})$ over K_0 . If $\delta_i = 1$ for $i = 1, \dots, s$, we may use the Chebotarev density theorem to choose $\mathfrak{q} \in \mathbb{P}(K_0) \setminus S|_{K_0}$ such that

$$(2.3.10) \quad N \subseteq \hat{K}_{0,\mathfrak{q}}.$$

In particular (a) holds. We choose $\mathfrak{Q} \in \mathbb{P}(K)$ with $\mathfrak{Q}|_{K_0} = \mathfrak{q}$. By its choice, \mathfrak{q} totally splits in K , hence $\hat{K}_{\mathfrak{Q}} = \hat{K}_{0,\mathfrak{q}}$. It follows that $a_{i\mathfrak{Q}} \in U_{\mathfrak{Q}}^l$, so $\beta_i = 0$ for $i = 1, \dots, s$. We therefore define $g(\bar{u}_{\mathfrak{Q}})$ to be a generator of C_l and derive from (2.3.8), (2.3.7) and (2.3.9) that $g(\bar{a}_i) = \delta_i \cdot g(\bar{u}_{\mathfrak{Q}})^{\beta_i} = 1$, so that (2.3.6)

holds.

PART D: *The main case.* Having settled the case where $\delta_i = 1$ for $i = 1, \dots, s$, we may and we will from now on assume that

$$(2.3.11) \quad \delta_1 \neq 1.$$

Under this assumption there exists $0 \leq \varepsilon_i < l$ such that in C_l

$$(2.3.12) \quad \delta_1^{\varepsilon_i} = \delta_i, \quad i = 1, \dots, s.$$

In particular $\varepsilon_1 = 1$. Define

$$(2.3.13) \quad b_1 = a_1 \quad \text{and} \quad b_i = a_i/a_1^{\varepsilon_i}, \quad \text{for } i = 2, \dots, s.$$

Since a_1, \dots, a_s are multiplicatively independent modulo K_S^l , so are b_1, \dots, b_s . By Remark 2.3.3, $L(\zeta_n, \sqrt[l]{b_1}), \dots, L(\zeta_n, \sqrt[l]{b_s})$ are linearly disjoint fields of degree l over $L(\zeta_n)$.

PART E: *Choosing \mathfrak{q} .* Part D allows us to choose $\sigma \in \text{Gal}(N/L(\zeta_n))$ with $(\sqrt[l]{a_1})^\sigma = \zeta_l \sqrt[l]{a_1}$ and $(\sqrt[l]{b_i})^\sigma = \sqrt[l]{b_i}$, $i = 2, \dots, s$. Chebotarev density theorem gives us a prime $\mathfrak{q} \in \mathbb{P}(K_0) \setminus S|_{K_0}$ such that $(\frac{N/K_0}{\mathfrak{q}}) = \text{Con}(\sigma)$. Thus, $L(\zeta_n) \subseteq \hat{K}_{0,\mathfrak{q}}$, so (a) holds.

We choose $\Omega \in \mathbb{P}(K)$ with $\Omega|_{K_0} = \mathfrak{q}$. Since \mathfrak{q} is unramified in N , so is Ω . Therefore $\hat{K}_\Omega(\sqrt[l]{a_1})/\hat{K}_\Omega$ is an unramified extension. It follows that the Frobenius element over \hat{K}_Ω acts on $\sqrt[l]{a_1}$ as σ , in particular the Frobenius element does not fix $\sqrt[l]{a_1}$. This implies that $[\hat{K}_\Omega(\sqrt[l]{a_1}) : \hat{K}_\Omega] = l$, in particular:

$$(2.3.14) \quad a_1 \in U_\Omega \setminus U_\Omega^l.$$

On the other hand $b_i \in U_\Omega^l$ and therefore, by (2.3.13),

$$(2.3.15) \quad \bar{a}_{i\Omega} = \bar{a}_{1\Omega}^{\varepsilon_i}, \quad i = 2, \dots, s.$$

PART F: *Definition of g .* By (2.3.14) and the choice of \bar{u}_Ω in Part B,

$$(2.3.16) \quad \bar{a}_{1\Omega} = \bar{u}_\Omega^\beta \quad \text{with } 0 < \beta < l.$$

We may therefore define $g(\bar{u}_\Omega)$ as the element of C_l that satisfies

$$(2.3.17) \quad g(\bar{u}_\Omega)^\beta = \delta_1^{-1}$$

In particular, by (2.3.11), $g(\bar{u}_\Omega) \neq 1$. By (2.3.15) and (2.3.16), $\bar{a}_{i\Omega} = \bar{u}_\Omega^{\beta\varepsilon_i}$, $i = 2, \dots, s$. Since $\varepsilon_1 = 1$, the latter equality also holds for $i = 1$. This gives (2.3.8) the following form:

$$(2.3.18) \quad \bar{a}_i = \prod_{\mathfrak{P} \in S} \bar{a}_{i\mathfrak{P}} \cdot \bar{u}_\Omega^{\beta\varepsilon_i} \prod_{\mathfrak{P} \notin S \cup \{\Omega\}} \bar{a}_{i\mathfrak{P}}.$$

By (2.3.7) and (2.3.9),

$$(2.3.19) \quad \prod_{\mathfrak{P} \in S} g(\bar{a}_{i\mathfrak{P}}) = \delta_i \text{ and } \prod_{\mathfrak{P} \notin S \cup \{\Omega\}} g(\bar{a}_{i\mathfrak{P}}) = 1.$$

Apply g on (2.3.18) and use (2.3.19), (2.3.17) and (2.3.12) to get that

$$g(\bar{a}_i) = \left(\prod_{\mathfrak{P} \in S} g(\bar{a}_{i\mathfrak{P}}) \right) \cdot g(\bar{u}_\Omega)^{\beta\varepsilon_i} = \delta_i \delta_1^{-\varepsilon_i} = 1.$$

So (2.3.6) holds and the proof is complete. \square

Corollary 2.3.6. Let $K_0 \subseteq K \subseteq L$ be a tower of Galois extension of number fields such that L/K_0 is Galois, L/K is a finite abelian l -extension and $\zeta_l \notin K$. Let S be a finite set of primes of K which contains S_0 . Let $n = ql^m$ be a multiple of l^m for some positive integers q and m . For homomorphisms $h_{\mathfrak{P}}: \text{Gal}(\hat{K}_{\mathfrak{P}}) \rightarrow C_l$, $\mathfrak{P} \in S$, there exists a prime $\mathfrak{q} \in \mathbb{P}(K_0) \setminus S|_{K_0}$ and a homomorphism $h: \text{Gal}(K) \rightarrow C_l$ such that

- (a) \mathfrak{q} totally splits in $L(\zeta_n)$,
- (b) $\text{res}_{\mathfrak{P}}(h) = h_{\mathfrak{P}}$ for each $\mathfrak{P} \in S$, where $\text{res}_{\mathfrak{P}}$ is defined in Lemma 2.2.1,
- (c) there exists $\Omega \in \mathbb{P}(K)$ such that $\Omega|_{K_0} = \mathfrak{q}$ and $\text{res}_{\Omega}(h)(\hat{I}_\Omega) = C_l$,
- (d) $\text{res}_{\mathfrak{P}}(h)(\hat{I}_{\mathfrak{P}}) = 1$ for each $\mathfrak{P} \in \mathbb{P}(K) \setminus (S \cup \{\Omega\})$.

Proof. For each $\mathfrak{P} \in S$, let $h'_{\mathfrak{P}}: \hat{K}_{\mathfrak{P}}^\times \rightarrow C_l$ be the homomorphism that Lemma 2.2.1 attaches to $h_{\mathfrak{P}}$. An application of Lemma 2.3.5 to the system $(h'_{\mathfrak{P}})_{\mathfrak{P}}$, and again a use of Lemma 2.2.1 give us the desired prime $\mathfrak{q} \in \mathbb{P}(K_0) \setminus S|_{K_0}$ and the $h: \text{Gal}(K) \rightarrow C_l$. \square

2.4 Bound on the Ramification

of $h \in \text{Hom}(\text{Gal}(K), A)$

This section contains the main result of this chapter: the construction of $h: \text{Gal}(K) \rightarrow C_l^r$ with a bound on its ramification. We repeat the construction in Corollary 2.3.6 r times to obtain the continuous homomorphism $h: \text{Gal}(K) \rightarrow A$ with $A = C_l^r$, which is unramified at each $\mathfrak{P} \in \mathbb{P}(K) \setminus (S \cup \{\mathfrak{Q}_1, \dots, \mathfrak{Q}_r\})$ for some $\mathfrak{Q}_1, \dots, \mathfrak{Q}_r \in \mathbb{P}(K) \setminus S$.

Given a homomorphism $h_{\mathfrak{P}}: \text{Gal}(\hat{K}_{\mathfrak{P}}) \rightarrow A$ for each $\mathfrak{P} \in S$, considering the system of homomorphisms $(h_{\mathfrak{P},i} = \pi_i \circ h_{\mathfrak{P}})_{\mathfrak{P} \in S}$ where $\pi_i: A \rightarrow C_{l,i}$ is the projection to the i th factor, by using Corollary 2.3.6 we may choose a prime $\mathfrak{q}_i \in \mathbb{P}(K_0) \setminus S|_{K_0}$ and construct a homomorphism $h_i: \text{Gal}(K) \rightarrow C_{l,i}$ that satisfy conditions (a)-(d) of Corollary 2.3.6 for each $i = 1, \dots, r$. Then the homomorphism $h = (h_1, \dots, h_r)$ will satisfy the conclusions of our main proposition (Proposition 2.4.1). However, for the next use (as in the proof of Proposition 3.3.5), we need to know information about $\text{res}_{\mathfrak{Q}_{i,j}}(h)(\text{Gal}(\hat{K}_{\mathfrak{Q}_{i,j}}))$ for each prime $\mathfrak{Q}_{i,j}$ that lies over \mathfrak{q}_i . For that, in addition to the use of Corollary 2.3.6, we enlarge S to $S \cup \bigcup_{t=1}^{i-1} \{\mathfrak{Q} \in \mathbb{P}(K) \mid \mathfrak{Q}|_{K_0} = \mathfrak{q}_t\}$ for each $i = 1, \dots, r$ and add in the system of given homomorphisms the trivial homomorphism $h_{\mathfrak{Q}}: \text{Gal}(\hat{K}_{\mathfrak{Q}}) \rightarrow C_{l,i}$ for each $\mathfrak{Q} \in \bigcup_{t=1}^{i-1} \{\mathfrak{Q} \in \mathbb{P}(K) \mid \mathfrak{Q}|_{K_0} = \mathfrak{q}_t\}$.

Proposition 2.4.1. Let $K_0 \subseteq K \subseteq L$ be a tower of finite Galois extensions of number fields such that L/K_0 is a Galois extension, L/K is an abelian l -extension and $\zeta_l \notin K$. Let $n = ql^m$ for some positive integers q and m , and let $A = C_{l,1} \times \dots \times C_{l,r}$ where each $C_{l,i}$, $i = 1, \dots, r$, is an isomorphic copy of C_l . Let S be a finite set of primes of K which contains S_0 . For each $\mathfrak{P} \in S$ let $h_{\mathfrak{P}}: \text{Gal}(\hat{K}_{\mathfrak{P}}) \rightarrow A$ be a homomorphism. Then there exist distinct primes $\mathfrak{q}_1, \dots, \mathfrak{q}_r \in \mathbb{P}(K_0) \setminus S|_{K_0}$ and there exists a homomorphism $h: \text{Gal}(K) \rightarrow A$ such that

- (a) \mathfrak{q}_i totally splits in $L(\zeta_n)$ for $i = 1, \dots, r$,

- (b) $\text{res}_{\mathfrak{P}}(h) = h_{\mathfrak{P}}$, for each $\mathfrak{P} \in S$,
- (c) for $i = 1, \dots, r$ there exists $\mathfrak{Q}_i \in \mathbb{P}(K)$ with $\mathfrak{Q}_i|_{K_0} = \mathfrak{q}_i$ such that $\text{res}_{\mathfrak{Q}_i}(h)(\text{Gal}(\hat{K}_{\mathfrak{Q}_i})) = 1 \times \cdots \times 1 \times C_{l,i} \times 1 \times \cdots \times 1$,
- (d) For each $\mathfrak{Q} \neq \mathfrak{Q}_i$ that lies over \mathfrak{q}_i , $\text{res}_{\mathfrak{Q}}(h)(\text{Gal}(\hat{K}_{\mathfrak{Q}})) \leq 1 \times \cdots \times 1 \times C_{l,i} \times 1 \times \cdots \times 1$
- (e) $\text{res}_{\mathfrak{P}}(h)(\hat{I}_{\mathfrak{P}}) = 1$ for each $\mathfrak{P} \in \mathbb{P}(K) \setminus (S \cup \{\mathfrak{Q}_1, \dots, \mathfrak{Q}_r\})$.

Proof. For each $i = 1, \dots, r$ and each $\mathfrak{P} \in S$ consider the compositum $h_{\mathfrak{P},i}: \text{Gal}(\hat{K}_{\mathfrak{P}}) \rightarrow C_{l,i}$ of $h_{\mathfrak{P}}$ and the projection $A \rightarrow C_{l,i}$. Then, for each $\mathfrak{P} \in S$

$$(2.4.1) \quad h_{\mathfrak{P}} = (h_{\mathfrak{P},1}, \dots, h_{\mathfrak{P},r})$$

Part A: $i = 1$. Consider the system of homomorphisms $(h_{\mathfrak{P},1}: \text{Gal}(\hat{K}_{\mathfrak{P}}) \rightarrow C_{l,1})_{\mathfrak{P} \in S}$. By Corollary 2.3.6, there exists a prime $\mathfrak{q}_1 \in \mathbb{P}(K_0) \setminus S|_{K_0}$ and there exists a homomorphism $h_1: \text{Gal}(K) \rightarrow C_{l,1}$ such that:

$$(2.4.2) \quad \mathfrak{q}_1 \text{ totally splits in } L(\zeta_n),$$

$$(2.4.3) \quad \text{res}_{\mathfrak{P}}(h_1) = h_{\mathfrak{P},1} \text{ for each } \mathfrak{P} \in S,$$

$$(2.4.4) \quad \text{there exists } \mathfrak{Q}_1 \in \mathbb{P}(K) \text{ with } \mathfrak{Q}_1|_{K_0} = \mathfrak{q}_1 \text{ such that } \text{res}_{\mathfrak{Q}_1}(h_1)(\hat{I}_{\mathfrak{Q}_1}) = C_{l,1},$$

$$(2.4.5) \quad \text{res}_{\mathfrak{P}}(h_1)(\hat{I}_{\mathfrak{P}}) = 1 \text{ for each } \mathfrak{P} \in \mathbb{P}(K) \setminus (S \cup \{\mathfrak{Q}_1\}).$$

Let L_1 be the fixed field of $\text{Ker}(h_1)$ in \tilde{K} . Then, by (2.4.4), L_1/K is a cyclic l -extension, so LL_1/K is a finite abelian l -extension. It follows that the Galois closure L'_1 of LL_1 over K_0 is also a finite abelian l -extension of K . By (2.4.2), \mathfrak{q}_1 totally splits in K . Let $\mathfrak{Q}_1 = \mathfrak{Q}_{1,1}, \mathfrak{Q}_{1,2}, \dots, \mathfrak{Q}_{1,k} \in \mathbb{P}(K)$ be the primes lying over \mathfrak{q}_1 where $k = [K : K_0]$.

Part B: $i = 2$. For each $j = 1, \dots, k$ let $h_{\mathfrak{Q}_{1,j},2}: \text{Gal}(\hat{K}_{\mathfrak{Q}_{1,j}}) \rightarrow C_{l,2}$ be the trivial homomorphism. Consider the system of homomorphisms $(h_{\mathfrak{P},2}: \text{Gal}(\hat{K}_{\mathfrak{P}}) \rightarrow$

$C_{l,2})_{\mathfrak{P} \in S \cup \{\mathfrak{Q}_{1,1}, \dots, \mathfrak{Q}_{1,k}\}}$, with $h_{\mathfrak{P},2}: \text{Gal}(\hat{K}_{\mathfrak{P}}) \xrightarrow{h_{\mathfrak{P}}} A \rightarrow C_{l,2}$. Considering the tower of Galois extensions $K_0 \subseteq K \subseteq L'_1$, where L'_1 is defined in Part A, again by Corollary 2.3.6, there exists $\mathfrak{q}_2 \in \mathbb{P}(K_0) \setminus (S|_{K_0} \cup \{\mathfrak{q}_1\})$ and there exists a homomorphism $h_2: \text{Gal}(K) \rightarrow C_{l,2}$ such that:

$$(2.4.6) \quad \mathfrak{q}_2 \text{ totally splits in } L'_1(\zeta_n),$$

$$(2.4.7) \quad \text{res}_{\mathfrak{P}}(h_2) = h_{\mathfrak{P},2} \text{ for each } \mathfrak{P} \in S \cup \{\mathfrak{Q}_{1,1}, \dots, \mathfrak{Q}_{1,k}\},$$

$$(2.4.8) \quad \text{there exists } \mathfrak{Q}_2 \in \mathbb{P}(K) \text{ with } \mathfrak{Q}_2|_{K_0} = \mathfrak{q}_2 \text{ such that } \text{res}_{\mathfrak{Q}_2}(h_2)(\hat{I}_{\mathfrak{Q}_2}) = C_{l,2},$$

$$(2.4.9) \quad \text{res}_{\mathfrak{P}}(h_2)(\hat{I}_{\mathfrak{P}}) = 1 \text{ for each } \mathfrak{P} \in \mathbb{P}(K) \setminus (S \cup \{\mathfrak{Q}_{1,1}, \dots, \mathfrak{Q}_{1,k}, \mathfrak{Q}_2\}).$$

The choice of the homomorphism $h_{\mathfrak{Q}_{1,j},2}$ to be trivial and (2.4.7) imply that

$$(2.4.10) \quad \text{res}_{\mathfrak{Q}_{1,j}}(h_2)(\text{Gal}(\hat{K}_{\mathfrak{Q}_{1,j}})) = 1, \text{ for each } j = 1, \dots, k$$

In particular $\text{res}_{\mathfrak{Q}_{1,j}}(h_2)(\hat{I}_{\mathfrak{Q}_{1,j}}) = 1$. It follows from (2.4.9) that

$$(2.4.11) \quad \text{res}_{\mathfrak{P}}(h_2)(\hat{I}_{\mathfrak{P}}) = 1 \text{ for each } \mathfrak{P} \in \mathbb{P}(K) \setminus (S \cup \{\mathfrak{Q}_2\})$$

Furthermore, by (2.4.6), \mathfrak{q}_2 totally splits in L'_1 hence also in L_1 . The later field is the fixed field of $\text{Ker}(h_1)$ in \tilde{K} . Hence

$$(2.4.12) \quad \text{res}_{\mathfrak{Q}}(h_1)(\text{Gal}(\hat{K}_{\mathfrak{Q}})) = 1 \text{ for each } \mathfrak{Q} \in \mathbb{P}(K) \text{ that lies over } \mathfrak{q}_2.$$

Part C: *Induction.* Continuing this process inductively we find for each i between 1 and r a prime $\mathfrak{q}_i \in \mathbb{P}(K_0) \setminus (S|_{K_0} \cup \{\mathfrak{q}_1, \dots, \mathfrak{q}_{i-1}\})$ and a homomorphism $h_i: \text{Gal}(K) \rightarrow C_{l,i}$ such that

$$(2.4.13) \quad \mathfrak{q}_i \text{ totally splits in } L'_{i-1}(\zeta_n), \text{ where } L'_{i-1} \text{ is the Galois closure of } LL_1 \cdots L_{i-1} \text{ over } K_0 \text{ with } L_j \text{ the fixed field of } \text{Ker}(h_j) \text{ in } \tilde{K} \text{ for } j = 1, \dots, i-1.$$

$$(2.4.14) \quad \text{res}_{\mathfrak{P}}(h_i) = h_{\mathfrak{P},i} \text{ for each } \mathfrak{P} \in S, \text{ with } h_{\mathfrak{P},i}: \text{Gal}(\hat{K}_{\mathfrak{P}}) \xrightarrow{h_{\mathfrak{P}}} A \rightarrow C_{l,i} \text{ for each } \mathfrak{P} \in S, \text{ and } \text{res}_{\mathfrak{P}}(h_i) = 1 \text{ for each } \mathfrak{P} \in \mathbb{P}(K) \text{ that lies over one of the primes } \mathfrak{q}_1, \dots, \mathfrak{q}_{i-1},$$

(2.4.15) there exists $\mathfrak{Q}_i \in \mathbb{P}(K)$ with $\mathfrak{Q}_i|_{K_0} = \mathfrak{q}_i$ such that $\text{res}_{\mathfrak{Q}_i}(h_i)(\hat{I}_{\mathfrak{Q}_i}) = C_{l,i}$, and

(2.4.16) $\text{res}_{\mathfrak{P}}(h_i)(\hat{I}_{\mathfrak{P}}) = 1$ for each $\mathfrak{P} \in \mathbb{P}(K) \setminus (S \cup \{\mathfrak{Q}_i\})$

(2.4.17) As in (2.4.12), for each $t < i$, $\text{res}_{\mathfrak{Q}}(h_t)(\text{Gal}(\hat{K}_{\mathfrak{Q}})) = 1$ for each $\mathfrak{Q} \in \mathbb{P}(K)$ that lies over \mathfrak{q}_i

Part D: *Conclusion.* We now prove that the homomorphism

$$h := (h_1, \dots, h_r): \text{Gal}(K) \longrightarrow C_{l,1} \times \cdots \times C_{l,r}$$

and the primes $\mathfrak{q}_1, \dots, \mathfrak{q}_r \in \mathbb{P}(K_0)$ satisfy the conditions (a)-(e) of the Proposition.

We consider i between 1 and r . By (2.4.13), \mathfrak{q}_i totally splits in $L(\zeta_n)$, so (a) is satisfied. By (2.4.14), $\text{res}_{\mathfrak{P}}(h_i) = h_{\mathfrak{P},i}$ for each $\mathfrak{P} \in S$. Hence, by (2.4.1), $\text{res}_{\mathfrak{P}}(h) = (h_{\mathfrak{P},1}, \dots, h_{\mathfrak{P},r}) = h_{\mathfrak{P}}$ for each $\mathfrak{P} \in S$, thus (b) is satisfied.

Now,

$$\begin{aligned} \text{res}_{\mathfrak{Q}_i}(h)(\text{Gal}(\hat{K}_{\mathfrak{Q}_i})) &= (\text{res}_{\mathfrak{Q}_i}(h_1)(\text{Gal}(\hat{K}_{\mathfrak{Q}_i})), \dots, \text{res}_{\mathfrak{Q}_i}(h_i)(\text{Gal}(\hat{K}_{\mathfrak{Q}_i})), \\ &\quad \dots, \text{res}_{\mathfrak{Q}_i}(h_r)(\text{Gal}(\hat{K}_{\mathfrak{Q}_i}))). \end{aligned}$$

By (2.4.15), $\text{res}_{\mathfrak{Q}_i}(h_i)(\hat{I}_{\mathfrak{Q}_i}) = C_{l,i}$ which implies

$$(2.4.18) \quad \text{res}_{\mathfrak{Q}_i}(h_i)(\text{Gal}(\hat{K}_{\mathfrak{Q}_i})) = C_{l,i}.$$

On the other hand, for $t < i$, by (2.4.17) we have

$$(2.4.19) \quad \text{res}_{\mathfrak{Q}_i}(h_t)(\text{Gal}(\hat{K}_{\mathfrak{Q}_i})) = 1, \quad \text{for } 1 \leq t \leq i-1.$$

Moreover, for $t > i$, (2.4.14) applied to h_t implies that

$$(2.4.20) \quad \text{res}_{\mathfrak{Q}_i}(h_t)(\text{Gal}(\hat{K}_{\mathfrak{Q}_i})) = 1, \quad t > i.$$

It follows from (2.4.18), (2.4.19), and (2.4.20) that

$$(2.4.21) \quad \text{res}_{\mathfrak{Q}_i}(h)(\text{Gal}(\hat{K}_{\mathfrak{Q}_i})) = 1 \times \cdots \times C_{l,i} \times \cdots \times 1, \quad i = 1, \dots, r.$$

Thus (c) is satisfied.

Let $\mathfrak{Q} \neq \mathfrak{Q}_i$ a prime that lies over \mathfrak{q}_i . We have

$$\begin{aligned} \text{res}_{\mathfrak{Q}}(h)(\text{Gal}(\hat{K}_{\mathfrak{Q}})) &= (\text{res}_{\mathfrak{Q}}(h_1)(\text{Gal}(\hat{K}_{\mathfrak{Q}})), \dots, \text{res}_{\mathfrak{Q}}(h_i)(\text{Gal}(\hat{K}_{\mathfrak{Q}})), \\ &\quad \dots, \text{res}_{\mathfrak{Q}}(h_r)(\text{Gal}(\hat{K}_{\mathfrak{Q}}))). \end{aligned}$$

If $t < i$ or $t > i$ by the same arguments as in in proof of (c)

$$(2.4.22) \quad \text{res}_{\mathfrak{Q}}(h_t)(\text{Gal}(\hat{K}_{\mathfrak{Q}})) = 1.$$

Since the image of h_i is a subgroup of $C_{l,i}$, we have

$$(2.4.23) \quad \text{res}_{\mathfrak{Q}}(h_i)(\text{Gal}(\hat{K}_{\mathfrak{Q}})) \leq C_{l,i}$$

It follows from (2.4.22) and (2.4.23), that $\text{res}_{\mathfrak{Q}}(h)(\text{Gal}(\hat{K}_{\mathfrak{Q}})) \leq 1 \times \dots \times 1 \times C_{l,i} \times 1 \times \dots \times 1$. So, (d) is satisfies

Finally, for each $\mathfrak{P} \in \mathbb{P}(K) \setminus (S \cup \{\mathfrak{Q}_1, \dots, \mathfrak{Q}_r\})$, by (2.4.16), $\text{res}_{\mathfrak{P}}(h)(\hat{I}_{\mathfrak{P}}) = (\text{res}_{\mathfrak{P}}(h_1)(\hat{I}_{\mathfrak{P}}), \dots, \text{res}_{\mathfrak{P}}(h_r)(\hat{I}_{\mathfrak{P}})) = 1 \times \dots \times 1$, so (e) is satisfied, and this completes the proof of the proposition. \square

Chapter 3

Bound on the ramification of cohomology classes

Let K/K_0 be a Galois extension of number fields. Given a simple $\text{Gal}(K_0)$ -module $A = C_l^r$ on which $\text{Gal}(K)$ acts trivially, a finite set T of primes of K_0 , and an element $y_{\mathfrak{p}} \in H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ for each $\mathfrak{p} \in T$, the aim of this chapter is to construct an element $x \in H^1(\text{Gal}(K_0), A)$ which coincides with $y_{\mathfrak{p}}$ for each $\mathfrak{p} \in T$ and the number of the primes of K_0 where x ramifies is bounded depending on T and r . The construction is based on Theorem 1 of [Neu79], where no bound on the ramification is given.

If ψ_0 is a solution of the embedding problem

$$(3.0.1) \quad \begin{array}{ccccccc} & & & & \text{Gal}(K_0) & & \\ & & & & \swarrow & \downarrow \rho & \\ & & & & \psi_0 & & \\ 1 & \longrightarrow & A & \longrightarrow & \bar{G} & \xrightarrow{\bar{\alpha}} & \text{Gal}(K/K_0) \longrightarrow 1 \end{array}$$

and $\chi: \text{Gal}(K_0) \rightarrow A$ is a crossed homomorphism, then $\bar{\psi} = \psi_0 \cdot \chi$ is also a solution of (3.0.1) (Lemma 4.1.1). Our aim is to multiply ψ_0 by a suitable χ in order to give a bound on the ramification of $\bar{\psi}$ which will coincide with the bound on the ramification of χ .

The class $x \in H^1(\text{Gal}(K_0), A)$ of the crossed homomorphism $\chi: \text{Gal}(K_0) \rightarrow A$ is again constructed in a such a way that it coincides with a given local element of $H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ for $\mathfrak{p} \in T$, it is cyclic at each prime where it ramifies, and we have a bound on its ramification. These conditions are similar to the required conditions in the construction of the homomorphism h in Chapter 2. In fact, x inherits these properties from h by the corestriction map.

3.1 Definitions and a Preliminary Result

Let K_0 be a number field and let A be a $\text{Gal}(K_0)$ -module. Let $\mathfrak{p} \in \mathbb{P}(K_0)$. We consider A as a $\text{Gal}(\hat{K}_{0,\mathfrak{p}})$ -module with $a^\sigma = a^{\sigma|_{\hat{K}_0}}$ for each $a \in A$ and $\sigma \in \text{Gal}(\hat{K}_{0,\mathfrak{p}})$ (by our construction of $K_{0,\mathfrak{p}}$ in Section 1.2, if $\sigma \in \text{Gal}(\hat{K}_{0,\mathfrak{p}})$, then $\text{res}_{\hat{K}_0}(\sigma) \in \text{Gal}(K_{0,\mathfrak{p}}) \leq \text{Gal}(K_0)$).

Definition 3.1.1. For each $n \geq 0$ and $\mathfrak{p} \in \mathbb{P}(K_0)$, we define the restriction map $\text{res}_{\mathfrak{p}}: H^n(\text{Gal}(K_0), A) \rightarrow H^n(\text{Gal}(\hat{K}_{0,\mathfrak{p}}))$ with $\text{res}_{\mathfrak{p}}(u)(\sigma_0, \dots, \sigma_n) = u(\sigma_1|_{\hat{K}_0}, \dots, \sigma_n|_{\hat{K}_0})$ for each $u \in C^n(\text{Gal}(K_0), A)$ and $\sigma_0, \dots, \sigma_n \in \text{Gal}(\hat{K}_{0,\mathfrak{p}})^{n+1}$.

If $\mathfrak{p} \in \mathbb{P}_{\text{fin}}(K_0)$ we consider the inflation-restriction exact sequence given by (1.4.8):

$$1 \longrightarrow H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}})/\hat{I}_{\mathfrak{p}}, A^{\hat{I}_{\mathfrak{p}}}) \xrightarrow{\text{inf}} H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A) \xrightarrow{\text{res}} H^1(\hat{I}_{\mathfrak{p}}, A) .$$

Definition 3.1.2.

- (a) An element $x_{\mathfrak{p}} \in H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ is **unramified** if $x_{\mathfrak{p}} \in \text{Im}(\text{inf})$, alternatively, if $\text{res}(x_{\mathfrak{p}}) = 1$. That is, if $\chi_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \rightarrow A$ is a representative of $x_{\mathfrak{p}}$, then there exists $a \in A$ such that for all $\sigma \in \hat{I}_{\mathfrak{p}}$, $\chi_{\mathfrak{p}}(\sigma) = a^\sigma a^{-1}$ (a coboundary representative in $\mathcal{Z}^1(\hat{I}_{\mathfrak{p}}, A)$). Note that if $\text{Gal}(\hat{K}_{0,\mathfrak{p}})$ acts trivially on A , then $x_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \rightarrow A$ is a homomorphism (Section 1.4 (D)). In this case, the definition of the unramification of $x_{\mathfrak{p}}$ at \mathfrak{p} as an element of $H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ coincides with the definition of $x_{\mathfrak{p}}$ being an unramified homomorphism, that is $x_{\mathfrak{p}}(\hat{I}_{\mathfrak{p}}) = 1$ (Def. 1.2.4(b)).

- (b) An element $x_{\mathfrak{p}} \in H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ is **cyclic** if there exists a cyclic extension $L_{\mathfrak{p}}/\hat{K}_{0,\mathfrak{p}}$ such that $x_{\mathfrak{p}}$ lies in the kernel of the restriction map

$$\text{res}: H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A) \longrightarrow H^1(\text{Gal}(L_{\mathfrak{p}}), A).$$

If $\text{Gal}(\hat{K}_{0,\mathfrak{p}})$ acts trivially on A , then $x_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \longrightarrow A$ is a homomorphism. In this case, $x_{\mathfrak{p}}$ is cyclic if it factors through a cyclic extension of $\hat{K}_{0,\mathfrak{p}}$: there exists a cyclic extension $L_{\mathfrak{p}}/\hat{K}_{0,\mathfrak{p}}$ such that $\text{Gal}(L_{\mathfrak{p}}) \leq \text{Ker}(x_{\mathfrak{p}})$ (Def. 1.2.4(c)).

The construction of $x \in H^1(\text{Gal}(K_0), A)$ mentioned in the introduction to the present chapter is based on that of [Neu79] in the following local-global result for elements of $H^1(\text{Gal}(K_0), A)$:

Proposition 3.1.3 ([Neu79], Thm. 1). Let $A = C_l^r$ be a simple $\text{Gal}(K_0)$ -module. Let K/K_0 be a finite Galois extension such that $\text{Gal}(K)$ acts trivially on A , and $\zeta_l \notin K$. Let Ω/K be a finite abelian extension and consider a finite set S of primes of K_0 . For each $\mathfrak{p} \in S$, let $y_{\mathfrak{p}} \in H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$. Then, there exists an element $x \in H^1(\text{Gal}(K_0), A)$ which satisfies the following conditions:

- (a) $\text{res}_{\mathfrak{p}}(x) = y_{\mathfrak{p}}$ for $\mathfrak{p} \in S$ (Def. 3.1.1).
 (b) If $\mathfrak{p} \in \mathbb{P}(K_0) \setminus S$, then $\text{res}_{\mathfrak{p}}(x)$ is cyclic. If in addition $\text{res}_{\mathfrak{p}}(x)$ is ramified, then \mathfrak{p} totally splits in Ω .

We improve this result by giving a bound on the ramification of x that depends on the set S and on r . In addition, we take care of the cyclic property of $x_{\mathfrak{p}}$ at the primes where x ramifies, but not for all $\mathfrak{p} \in \mathbb{P}(K_0) \setminus S$ as in the first part of condition (b) of the above proposition.

3.2 Corestriction Map

In general, if G is a profinite group, H an open subgroup of G , and A a G -module, then the corestriction map lifts an element of $H^1(H, A)$ to an

element of $H^1(G, A)$. We apply the corestriction map to the case where $G = \text{Gal}(K_0)$, $H = \text{Gal}(K)$, and $A = C_l^r$ on which $\text{Gal}(K)$ acts trivially (i.e. $H^1(\text{Gal}(K), A) = \text{Hom}(\text{Gal}(K), A)$). Then, we can lift the homomorphism $h: \text{Gal}(K) \rightarrow A$ constructed in Proposition 2.4.1 to an element of $H^1(\text{Gal}(K_0), A)$ that plays a significant role in the construction of our desired element $x \in H^1(\text{Gal}(K_0), A)$. The local cyclic property of x at each prime where it ramifies, and the bound on its ramification are induced from that of h .

We start with the general definition. Let G be a profinite group, H an open subgroup of G , and A a G -module. We choose a system T of representatives for the left cosets of G modulo H . Thus, $G = \bigcup_{\tau \in T} \tau H$. Then, for each $\sigma \in G$ there exists a unique element $\tilde{\sigma} \in T$ such that $\sigma H = \tilde{\sigma} H$. Hence, there exists a unique element $\eta_\sigma \in H$ such that $\sigma = \tilde{\sigma} \cdot \eta_\sigma$. In particular, for each $\eta \in H$ we have $\tilde{\sigma} H = \sigma H = \sigma \eta H = \widetilde{\sigma \eta} H$ so

$$(3.2.1) \quad \tilde{\sigma} = \widetilde{\sigma \eta}.$$

Having chosen T we define for each $n \geq 0$ a homomorphism

$$\text{cor} = \text{cor}^n: C^n(H, A) \longrightarrow \text{Map}_{\text{cont}}(G^{n+1}, A),$$

called the **corestriction** map, by

$$(3.2.2) \quad \begin{aligned} \text{cor}(x)(\sigma_0, \dots, \sigma_n) &= \prod_{\tau \in T} x(\widetilde{\sigma_0 \tau}^{-1} \sigma_0 \tau, \dots, \widetilde{\sigma_n \tau}^{-1} \sigma_n \tau)^{\tau^{-1}} \\ &= \prod_{\tau \in T} x(\eta_{\sigma_0 \tau}, \dots, \eta_{\sigma_n \tau})^{\tau^{-1}} \end{aligned}$$

Recall the $C^n(H, A)$ is the group of all n -dimensional homogeneous cochains (Section 1.4(B)). This homomorphism has the following properties:

(3.2.3) By the homogeneity (1.4.2) of the cochains and by (3.2.1), $\text{cor}(x)$ is independent of the choice of T .

(3.2.4) The image of each $x \in C^n(H, A)$ under cor is a homogeneous cochain (i.e. $\text{cor}(x) \in C^n(G, A)$). Indeed, if $\sigma \in G$ and T is a system of

representatives of the left cosets of G modulo H , then so is σT . Hence by (3.2.2) and by (3.2.3),

$$\begin{aligned} \text{cor}(x)(\sigma_0\sigma, \dots, \sigma_n\sigma)^{\sigma^{-1}} &= \prod_{\tau \in T} \left(x(\eta_{\sigma_0\sigma\tau}, \dots, \eta_{\sigma_n\sigma\tau})^{\tau^{-1}} \right)^{\sigma^{-1}} \\ &= \prod_{\tau \in T} x(\eta_{\sigma_0\sigma\tau}, \dots, \eta_{\sigma_n\sigma\tau})^{(\sigma\tau)^{-1}} \\ &= \text{cor}(x)(\sigma_0, \dots, \sigma_n) \end{aligned}$$

(3.2.5) By definition (3.2.2), the homomorphisms $\text{cor}^n: C^n(H, A) \longrightarrow C^n(G, A)$ are functorial in A .

(3.2.6) The homogeneity condition (1.4.2) and the definition (3.2.2) imply that the corestriction maps are compatible with the coboundary operators (Section 1.4(A)), in other words $\text{cor} \circ \partial = \partial \circ \text{cor}$. Therefore, the cochain homomorphisms cor^n give rise to homomorphisms of cohomology groups $\text{cor} = \text{cor}^n: H^n(H, A) \longrightarrow H^n(G, A)$.

(3.2.7) By (3.2.2), the homomorphism cor^0 maps $A^H = H^0(H, A)$ into $A^G = H^0(G, A)$. Indeed, for $a \in A^H$ we have $\text{cor}^0(a) = \prod_{\tau \in T} a^{\tau^{-1}} = \prod_{\tau' \in T'} a^{\tau'}$, where $T' = \{\tau^{-1} \mid \tau \in T\}$. Note that $G = \bigcup_{\tau' \in T'} H\tau'$, so cor^0 coincides with the relative norm $\text{norm}_{G/H}: A^H \longrightarrow A^G$.

(3.2.8) The corestriction maps commute with the connecting homomorphisms δ of cohomology groups. In other words, let $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$ be a short exact sequence of G -modules that we also consider as a short exact sequence of H -modules. Then, for each $n \geq 0$, the corresponding diagram

$$\begin{array}{ccc} H^n(H, C) & \xrightarrow{\delta} & H^{n+1}(H, A) \\ \text{cor} \downarrow & & \downarrow \text{cor} \\ H^n(G, C) & \xrightarrow{\delta} & H^{n+1}(G, A) \end{array}$$

is commutative. The proof of this statement goes back to the explicit definition of δ that depends on the "snake lemma" (see [NSW00], p. 27, Prop. 1.3.3) and its proof).

(3.2.9) If $H = G$, then $T = \{1\}$. In this case $\tilde{\sigma} = 1$ for each $\sigma \in G$, so in the notation of (3.2.2), $\tilde{\sigma}_i \tau^{-1} \sigma_i \tau = \sigma_i$ for $i = 1, \dots, n$. Thus, in this case, $\text{cor}(x)(\sigma_1, \dots, \sigma_n) = x(\sigma_1, \dots, \sigma_n)$, in other words cor is the identity map on $H^n(G, A)$.

Now, we come back to the case of number fields. Let K/K_0 be a finite Galois extension of number field and A a $\text{Gal}(K_0)$ -module. Let $\mathfrak{p} \in \mathbb{P}(K_0)$. For each prime $\mathfrak{P} \in \mathbb{P}(K)$ lying over \mathfrak{p} , A is a $\text{Gal}(\hat{K}_{\mathfrak{P}})$ -module with $a^\tau = a^{\tau^{\lambda_{\mathfrak{P}}^{-1}}}$ for each $a \in A$ and $\tau \in \text{Gal}(\hat{K}_{\mathfrak{P}})$ (by the definition of $\lambda_{\mathfrak{P}}$ at the beginning of Section 1.2 if $\tau \in \text{Gal}(\hat{K}_{\mathfrak{P}})$, then $\tau^{\lambda_{\mathfrak{P}}^{-1}} \in \text{Gal}(K_{\mathfrak{P}}) \leq \text{Gal}(K)$).

We want to prove that the following diagram

$$(3.2.10) \quad \begin{array}{ccc} H^n(\text{Gal}(K), A) & \xrightarrow{\text{Res}} & \prod_{\mathfrak{P}|\mathfrak{p}} H^n(\text{Gal}(\hat{K}_{\mathfrak{P}}), A) \\ \text{cor} \downarrow & & \downarrow \text{Cor} \\ H^n(\text{Gal}(K_0), A) & \xrightarrow{\text{res}_{\mathfrak{p}}} & H^n(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A) \end{array}$$

is commutative for each integer $n \geq 0$. In this diagram

- (a) The map $\text{cor}: H^n(\text{Gal}(K), A) \rightarrow H^n(\text{Gal}(K_0), A)$ is the corestriction map defined below using that $\text{Gal}(K)$ is an open subgroup of $\text{Gal}(K_0)$.
- (b) The map $\text{res}: H^n(\text{Gal}(K_0), A) \rightarrow H^n(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ is the restriction map defined by $\text{res}(u) = u_{\mathfrak{p}}$ where $u_{\mathfrak{p}}(\sigma_0, \dots, \sigma_n) = u(\sigma_0|_{\tilde{K}_0}, \dots, \sigma_n|_{\tilde{K}_0})$ for each $u \in C^n(\text{Gal}(K_0), A)$ and $\sigma_0, \dots, \sigma_n \in \text{Gal}(\hat{K}_{0,\mathfrak{p}})$.
- (c) The map Res is an abbreviation to the system of maps $(\text{res}_{\mathfrak{P}})_{\mathfrak{P}|\mathfrak{p}}$ where $\text{res}_{\mathfrak{P}}: H^n(\text{Gal}(K), A) \rightarrow H^n(\text{Gal}(\hat{K}_{\mathfrak{P}}), A)$ is the restriction map defined $\text{res}_{\mathfrak{P}}(h) = h_{\mathfrak{P}}$ where $h_{\mathfrak{P}}(\sigma_0, \dots, \sigma_n) = h(\sigma_0^{\lambda_{\mathfrak{P}}^{-1}}, \dots, \sigma_n^{\lambda_{\mathfrak{P}}^{-1}})$ for each $h \in C^n(\text{Gal}(K), A)$ and $\sigma_0, \dots, \sigma_n \in \text{Gal}(\hat{K}_{\mathfrak{P}})$.
- (d) The map Cor is the product of the corestriction maps $\text{cor}_{\mathfrak{P}}: H^n(\text{Gal}(\hat{K}_{\mathfrak{P}}), A) \rightarrow H^n(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ defined below, using that $\text{Gal}(\hat{K}_{\mathfrak{P}})$ is considered as an open subgroup of $\text{Gal}(\hat{K}_{0,\mathfrak{p}})$.

Set $d = [K : K_0]$ and $d_{\mathfrak{P}} = [\hat{K}_{\mathfrak{P}} : \hat{K}_{0,\mathfrak{P}}]$ for $\mathfrak{P}|\mathfrak{p}$. Then, we write

$$(3.2.11) \quad \text{Gal}(K_0) = \bigcup_{j=1}^d \text{Gal}(K)\varepsilon_j^{-1} \text{ and } \text{Gal}(\hat{K}_{0,\mathfrak{P}}) = \bigcup_{k=1}^{d_{\mathfrak{P}}} \text{Gal}(\hat{K}_{\mathfrak{P}})\varepsilon_{\mathfrak{P},k}^{-1}$$

Then, $f(X) = \prod_{j=1}^d (X - x^{\varepsilon_j^{-1}})$ and $f_{\mathfrak{P}}(X) = \prod_{k=1}^{d_{\mathfrak{P}}} (X - x_{\mathfrak{P}}^{\varepsilon_{\mathfrak{P},k}^{-1}})$ for $\mathfrak{P}|\mathfrak{p}$. It follows that there exists a bijection of sets $\beta: \bigcup_{\mathfrak{P}|\mathfrak{p}} \{(\mathfrak{P}, 1), \dots, (\mathfrak{P}, d_{\mathfrak{P}})\} \longrightarrow \{1, \dots, d\}$ such that

$$(3.2.12) \quad \varepsilon_{\mathfrak{P},k}^{-1}|_K = \varepsilon_{\beta(\mathfrak{P},k)}^{-1}|_K \text{ for } i = 1, \dots, m \text{ and } k = 1, \dots, d_i.$$

Hence, there exists $\eta_{\mathfrak{P},k} \in \text{Gal}(K)$ such that

$$(3.2.13) \quad \varepsilon_{\mathfrak{P},k}^{-1}|_{\hat{K}_0} = \eta_{\mathfrak{P},k} \varepsilon_{\beta(\mathfrak{P},k)}^{-1}$$

For each $\sigma \in \text{Gal}(K_0)$ we use (3.2.11) to choose $\tilde{\sigma} \in \{\varepsilon_1, \dots, \varepsilon_d\}$ with $\text{Gal}(K)\sigma^{-1} = \text{Gal}(K)\tilde{\sigma}^{-1}$. Then

$$\text{cor}: H^n(\text{Gal}(K), A) \longrightarrow H^n(\text{Gal}(K_0), A)$$

is defined for each homogeneous cochain $h: \text{Gal}(K)^{n+1} \longrightarrow A$ and for all $(\sigma_0, \dots, \sigma_n) \in \text{Gal}(K_0)^{n+1}$ by

$$(3.2.14) \quad \text{cor}(h)(\sigma_0, \dots, \sigma_n) = \prod_{j=1}^d h(\widetilde{\sigma_0 \varepsilon_j^{-1}} \sigma_0 \varepsilon_j, \dots, \widetilde{\sigma_n \varepsilon_j^{-1}} \sigma_n \varepsilon_j)^{\varepsilon_j^{-1}}.$$

Similarly for each i between 1 and m and every $\sigma \in \text{Gal}(\hat{K}_{0,\mathfrak{P}})$ there is a unique $\tilde{\sigma} \in \{\varepsilon_{\mathfrak{P},1}, \dots, \varepsilon_{\mathfrak{P},d_{\mathfrak{P}}}\}$ such that $\text{Gal}(\hat{K}_{\mathfrak{P}})\sigma^{-1} = \text{Gal}(\hat{K}_{\mathfrak{P}})\tilde{\sigma}^{-1}$. Again, we have for each homogeneous cochain $h: \text{Gal}(\hat{K}_{\mathfrak{P}})^{n+1} \longrightarrow A$ and every tuple $(\sigma_0, \dots, \sigma_n) \in \text{Gal}(\hat{K}_{0,\mathfrak{P}})^{n+1}$ that

$$\text{cor}_{\mathfrak{P}}(h)(\sigma_0, \dots, \sigma_n) = \prod_{k=1}^{d_{\mathfrak{P}}} h(\widetilde{\sigma_0 \varepsilon_{\mathfrak{P},k}^{-1}} \sigma_0 \varepsilon_{i,k}, \dots, \widetilde{\sigma_n \varepsilon_{i,k}^{-1}} \sigma_n \varepsilon_{\mathfrak{P},k})^{\varepsilon_{\mathfrak{P},k}^{-1}}.$$

Lemma 3.2.1. Diagram (3.2.10) commutes for $n = 0$

Proof. By (3.2.7),

$$H^0(\mathrm{Gal}(K), A) = A^{\mathrm{Gal}(K)} = \{a \in A \mid a^\sigma = a \text{ for all } \sigma \in \mathrm{Gal}(K)\}$$

and the map $\mathrm{cor}: H^0(\mathrm{Gal}(K), A) \rightarrow H^0(\mathrm{Gal}(K_0), A)$ is defined (in terms of inhomogeneous 0-cochains) for each $a \in A^{\mathrm{Gal}(K)}$ by $\mathrm{cor}(a) = \prod_{j=1}^d a^{\varepsilon_j^{-1}}$ (see (3.2.14)). Similarly, for each $\mathfrak{P}|\mathfrak{p}$ we have $H^0(\mathrm{Gal}(\hat{K}_{\mathfrak{P}}), A) = A^{\mathrm{Gal}(\hat{K}_{\mathfrak{P}})}$ and $\mathrm{cor} = \mathrm{cor}_{\mathfrak{P}}: H^0(\mathrm{Gal}(\hat{K}_{\mathfrak{P}}), A) \rightarrow H^0(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ is defined by $\mathrm{cor}(a) = \prod_{k=1}^{d_{\mathfrak{P}}} a^{\varepsilon_{\mathfrak{P},k}^{-1}}$. Furthermore, for each $a \in A^{\mathrm{Gal}(K)}$ and $\sigma \in \mathrm{Gal}(\hat{K}_{\mathfrak{P}})$, $a^\sigma = a^{\sigma^{\lambda_{\mathfrak{P}}^{-1}}} = a$, so $\mathrm{res}_{\mathfrak{P}}(a) = a$. Similarly, if $a \in A^{\mathrm{Gal}(K_0)}$ and $\sigma \in \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$, $a^\sigma = a^{\sigma^{\lambda_{K_0}}} = a$, so $\mathrm{res}(a) = a$.

Now, let $a \in A^{\mathrm{Gal}(K)}$. Then

$$\begin{aligned} \mathrm{Cor}(\mathrm{Res}(a)) &= \mathrm{Cor}(a, \dots, a) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{cor}_{\mathfrak{P}}(a) \\ &= \prod_{\mathfrak{P}|\mathfrak{p}} \prod_{k=1}^{d_{\mathfrak{P}}} a^{\varepsilon_{i,k}^{-1}|_{\hat{K}_0}} = \prod_{\mathfrak{P}|\mathfrak{p}} \prod_{k=1}^{d_{\mathfrak{P}}} a^{\eta_{\mathfrak{P},k} \varepsilon_{\beta(\mathfrak{P},k)}^{-1}} \end{aligned}$$

Since $\eta_{\mathfrak{P},k} \in \mathrm{Gal}(K)$ (see 3.2.13) and $a \in A^{\mathrm{Gal}(K)}$, $a^{\eta_{\mathfrak{P},k}} = a$, hence

$$\begin{aligned} \mathrm{Cor}(\mathrm{Res}(a)) &= \prod_{\mathfrak{P}|\mathfrak{p}} \prod_{k=1}^{d_{\mathfrak{P}}} a^{\varepsilon_{\beta(\mathfrak{P},k)}^{-1}} \\ &= \prod_{j=1}^d a^{\varepsilon_j} = \mathrm{cor}(a) = \mathrm{cor}(\mathrm{res}(a)). \end{aligned}$$

Thus, $\mathrm{Cor} \circ \mathrm{Res} = \mathrm{res} \circ \mathrm{cor}$ in dimension 0. \square

The special case of the following result for $n = 1$ is used in the proof of Theorem 1 of [Neu79] without a proof.

Proposition 3.2.2. The diagram (3.2.10) commutes for every integer $n \geq 0$.

Proof. Each of the four vertices in diagram (3.2.10) can be considered as a cohomological functor in the sense of [Rib70] (p. 120, Def. 5.1). Moreover,

res: $H^n(G, A) \longrightarrow H^n(H, A)$ commutes with the connecting homomorphism δ for every profinite group G , every closed subgroup H , and every finite G -module A ([Rib70], p. 135). The same holds for the maps induced by the conjugations with the $\lambda_{\mathfrak{P}}$'s ([NSW00], Prop. 1.5.4 and Prop. 1.6.2). Hence, both horizontal maps in digram (3.2.10) are morphisms of cohomological functors in the sense of [Rib70] (p. 121, Def. 5.2). The same holds for both corestriction maps in (3.2.10), with H now open in G ([Rib70], p. 136). By Lemma 3.2.1, $\text{Cor} \circ \text{Res} = \text{res} \circ \text{cor}$ in dimension 0. Hence, the method of dimension shifting of cohomology theory (in particular, [Rib70], p. 124, Cor. 5.6) implies that the latter relation holds for each integer $n \geq 0$, as claimed. \square

3.3 Bound on the Ramification of 1-Cocycles

This section contains the main result of this chapter.

Let K/K_0 be a finite Galois extension of number fields, let \mathfrak{p} be a prime of K_0 , and let \mathfrak{P} be a prime of K that lies over \mathfrak{p} . The case $n = 1$ of Proposition 3.2.2 supplies a commutative diagram

$$(3.3.1) \quad \begin{array}{ccc} H^1(\text{Gal}(K), A) & \xrightarrow{\text{Res}} & \prod_{\mathfrak{P}|\mathfrak{p}} H^1(\text{Gal}(K_{\mathfrak{P}}), A) \\ \text{cor} \downarrow & & \downarrow \text{Cor} \\ H^1(\text{Gal}(K_0), A) & \xrightarrow{\text{res}_{\mathfrak{p}}} & H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A) \end{array}$$

Now, suppose that $\text{Gal}(K)$ acts trivially on A , so $H^1(\text{Gal}(K), A) = \text{Hom}(\text{Gal}(K), A)$. Then, $\text{res}_{\mathfrak{P}}: H^1(\text{Gal}(K), A) \longrightarrow H^1(\text{Gal}(\hat{K}_{\mathfrak{P}}), A)$ is defined by $\text{res}_{\mathfrak{P}}(h)(\sigma) = h(\sigma^{\lambda_{\mathfrak{P}}^{-1}})$ for each homomorphism $h: \text{Gal}(K) \longrightarrow A$ and each $\sigma \in \text{Gal}(\hat{K}_{\mathfrak{P}})$. Recall that, as in Def. 1.2.4(b), the homomorphism $h: \text{Gal}(K) \longrightarrow A$ is unramified at \mathfrak{P} if $\text{res}_{\mathfrak{P}}(h)(\hat{I}_{\mathfrak{P}}) = 1$.

Let T be a system of representatives for the left cosets of $\text{Gal}(\hat{K}_{0,\mathfrak{p}})$ modulo $\text{Gal}(\hat{K}_{\mathfrak{P}})$. As before, for each $\sigma \in \text{Gal}(\hat{K}_{0,\mathfrak{p}})$, we let $\tilde{\sigma}$ be the unique element of T with $\tilde{\sigma}\text{Gal}(\hat{K}_{\mathfrak{P}}) = \sigma\text{Gal}(\hat{K}_{\mathfrak{P}})$. By (3.2.2), the map

$$\text{cor}_{\mathfrak{P}}: C^1(\text{Gal}(\hat{K}_{\mathfrak{P}}), A) \longrightarrow C^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$$

is defined for each $h_{\mathfrak{P}} \in C^1(\text{Gal}(\hat{K}_{\mathfrak{P}}), A)$ and for all $\sigma_0, \sigma_1 \in \text{Gal}(\hat{K}_{0,\mathfrak{p}})$ by

$$(3.3.2) \quad \text{cor}_{\mathfrak{P}}(h_{\mathfrak{P}})(\sigma_0, \sigma_1) = \prod_{\tau \in T} h_{\mathfrak{P}}(\widetilde{\sigma_0\tau}^{-1}\sigma_0\tau, \widetilde{\sigma_1\tau}^{-1}\sigma_1\tau)^{\tau^{-1}}.$$

Remark 3.3.1. If \mathfrak{p} totally splits in K , the map

$$\text{Cor}: \prod_{\mathfrak{P}|\mathfrak{p}} H^1(\text{Gal}(\hat{K}_{\mathfrak{P}}), A) \longrightarrow H^1(\text{Gal}(\hat{K}_{\mathfrak{p}}), A)$$

is surjective. Indeed, $\text{Gal}(\hat{K}_{\mathfrak{P}}) = \text{Gal}(\hat{K}_{0,\mathfrak{p}})$ for each $\mathfrak{P}|\mathfrak{p}$, so by (3.2.9), $\text{cor}_{\mathfrak{P}}: H^1(\text{Gal}(\hat{K}_{\mathfrak{P}}), A) \rightarrow H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ is the identity map. Let $h_{\mathfrak{p}} \in H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ and let $(h_{\mathfrak{P}})_{\mathfrak{P}|\mathfrak{p}} \in (H^1(\text{Gal}(\hat{K}_{\mathfrak{P}}), A))_{\mathfrak{P}|\mathfrak{p}}$ where $h_{\mathfrak{P}} = h_{\mathfrak{p}}$ for one $\mathfrak{P}|\mathfrak{p}$ and $h_{\mathfrak{P}'} = 1$ for each $\mathfrak{P}' \neq \mathfrak{P}$. Then $\text{Cor}((h_{\mathfrak{P}})_{\mathfrak{P}|\mathfrak{p}}) = \prod_{\mathfrak{P}|\mathfrak{p}} \text{cor}_{\mathfrak{P}}(h_{\mathfrak{P}}) = h_{\mathfrak{P}} \cdot 1 \cdots 1 = h_{\mathfrak{P}} = h_{\mathfrak{p}}$. \square

Lemma 3.3.2. Suppose $\mathfrak{p} \in \mathbb{P}(K_0)$ is unramified in K . For each $\mathfrak{P} \in \mathbb{P}(K)$ lying over \mathfrak{p} , let $h_{\mathfrak{P}} \in H^1(\text{Gal}(\hat{K}_{\mathfrak{P}}), A) = \text{Hom}(\text{Gal}(\hat{K}_{\mathfrak{P}}), A)$ such that $h_{\mathfrak{P}}(\hat{I}_{\mathfrak{P}}) = 1$. Let $u_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \text{cor}_{\mathfrak{P}}(h_{\mathfrak{P}})$. Then, $u_{\mathfrak{p}}|_{\hat{I}_{\mathfrak{p}}} = 1$.

Proof. For each $\mathfrak{P}|\mathfrak{p}$, we also denote by $h_{\mathfrak{P}} \in C^1(\text{Gal}(\hat{K}_{\mathfrak{P}}), A)$ the homogeneous cochain that corresponds to $h_{\mathfrak{P}}$ (see (1.4.4)). Then, $h_{\mathfrak{P}}|_{\hat{I}_{\mathfrak{P}} \times \hat{I}_{\mathfrak{P}}} = 1$. Similarly, we denote $u_{\mathfrak{p}}$ as well the homogeneous cochain corresponding to $u_{\mathfrak{p}}$. Since \mathfrak{p} is unramified in K , for each $\sigma \in \hat{I}_{\mathfrak{p}}$ we have $\sigma \in \hat{I}_{\mathfrak{P}}$ for each $\mathfrak{P}|\mathfrak{p}$, so $\hat{I}_{\mathfrak{P}}$ is a normal subgroup of $\text{Gal}(\hat{K}_{0,\mathfrak{p}})$. Let $\tau \in T_{\mathfrak{P}}$, where $T_{\mathfrak{P}}$ is a system of representatives of the left cosets of $\text{Gal}(\hat{K}_{\mathfrak{P}})$ modulo $\text{Gal}(\hat{K}_{\mathfrak{P}})$. Then, $\tau^{-1}\sigma\tau \in \hat{I}_{\mathfrak{P}}$. Moreover, $\widetilde{\sigma\tau}\text{Gal}(\hat{K}_{\mathfrak{P}}) = \sigma\tau\text{Gal}(\hat{K}_{\mathfrak{P}}) = \tau(\tau^{-1}\sigma\tau)\text{Gal}(\hat{K}_{\mathfrak{P}}) = \tau\text{Gal}(\hat{K}_{\mathfrak{P}})$. So

$\widetilde{\sigma}\tau = \tau$ and $\widetilde{\sigma}\tau^{-1}\sigma\tau = \tau^{-1}\sigma\tau \in \hat{I}_{\mathfrak{p}}$. Thus for each $\sigma_0, \sigma_1 \in \hat{I}_{\mathfrak{p}}$ we have by (3.2.2) that

$$\begin{aligned} \text{cor}_{\mathfrak{p}}(h_{\mathfrak{p}})(\sigma_0, \sigma_1) &= \prod_{\tau \in T_{\mathfrak{p}}} h_{\mathfrak{p}}(\widetilde{\sigma_0\tau}^{-1}\sigma_0\tau, \widetilde{\sigma_1\tau}^{-1}\sigma_1\tau)^{\tau^{-1}} \\ &= \prod_{\tau \in T_{\mathfrak{p}}} h_{\mathfrak{p}}(\tau^{-1}\sigma_0\tau, \tau^{-1}\sigma_1\tau)^{\tau^{-1}} \end{aligned}$$

Since $\tau^{-1}\sigma_i\tau \in \hat{I}_{\mathfrak{p}}$ for $i = 0, 1$, we have $h_{\mathfrak{p}}(\tau^{-1}\sigma_0\tau, \tau^{-1}\sigma_1\tau) = 1$. Hence $\text{cor}_{\mathfrak{p}}(h_{\mathfrak{p}})(\sigma_0, \sigma_1) = 1$. It follows that

$$(3.3.3) \quad u_{\mathfrak{p}}(\sigma_0, \sigma_1) = \prod_{\mathfrak{p}|\mathfrak{p}} \text{cor}_{\mathfrak{p}}(h_{\mathfrak{p}})(\sigma_0, \sigma_1) = 1 \text{ for } \sigma_0, \sigma_1 \in \hat{I}_{\mathfrak{p}}.$$

□

Corollary 3.3.3. If $A = C_{l,1} \times \cdots \times C_{l,r}$ where each $C_{l,j}$ is an isomorphic copy of C_l , we fix an $1 \leq i \leq r$ and consider the prime $\mathfrak{q}_i \in \mathbb{P}(K_0)$ and the homomorphism $h: \text{Gal}(K) \rightarrow A$ given by Proposition 2.4.1. Let $u = \text{cor}(h) \in H^1(\text{Gal}(K_0), A)$. Then $u_{\mathfrak{q}_i} = \text{res}_{\mathfrak{q}_i}(u) \in H^1(\text{Gal}(\hat{K}_{0,\mathfrak{q}_i}), A)$ is a cyclic (possibly trivial) homomorphism $u_{\mathfrak{q}_i}: \text{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \rightarrow C_l \leq A$.

Proof. By (a) of Proposition 2.4.1, \mathfrak{q}_i totally splits in K . Let $\mathfrak{Q}_{i,1}, \dots, \mathfrak{Q}_{i,k}$ be the primes of K lying over \mathfrak{q}_i and let $\mathfrak{Q}_i = \mathfrak{Q}_{i,1}$ the prime given by (c) of Proposition 2.4.1. For each $t = 1, \dots, k$, $\text{Gal}(\hat{K}_{\mathfrak{Q}_{i,t}}) = \text{Gal}(\hat{K}_{0,\mathfrak{q}_i})$, so $\text{Gal}(\hat{K}_{0,\mathfrak{q}_i})$ acts trivially on A . Therefore $u_{\mathfrak{q}_i}$ is a homomorphism. Let $h_{\mathfrak{Q}_{i,t}} = \text{res}_{\mathfrak{Q}_{i,t}}(h)$ for each $t = 1, \dots, k$. By the diagram (3.3.1), $u_{\mathfrak{q}_i} = \prod_{t=1}^k \text{cor}_{\mathfrak{Q}_{i,t}}(h_{\mathfrak{Q}_{i,t}})$. Since, $\text{Gal}(\hat{K}_{\mathfrak{Q}_{i,t}}) = \text{Gal}(\hat{K}_{0,\mathfrak{q}_i})$, the map $\text{cor}_{\mathfrak{Q}_{i,t}}$ is the identity map for each $t = 1, \dots, k$. It follows that $u_{\mathfrak{q}_i} = \prod_{t=1}^k h_{\mathfrak{Q}_{i,t}}$. By (c) and (d) of Proposition 2.4.1, $\text{Im}(h_{\mathfrak{Q}_{i,1}}) = 1 \times \cdots \times 1 \times C_{l,i} \times 1 \times \cdots \times 1$ and $\text{Im}(h_{\mathfrak{Q}_{i,t}}) \leq 1 \times \cdots \times 1 \times C_{l,i} \times 1 \times \cdots \times 1$ for each $t = 2, \dots, k$. It follows that $\text{Im}(\prod_{t=1}^k h_{\mathfrak{Q}_{i,t}}) \leq 1 \times \cdots \times 1 \times C_{l,i} \times 1 \times \cdots \times 1$. Therefore, $u_{\mathfrak{q}_i}$ is cyclic homomorphism. □

The following local-global result of Neukirch is an important tool for the construction of our desired element $x \in H^1(\text{Gal}(K_0), A)$ described in the introduction of this chapter.

Lemma 3.3.4 ([Neu79], Lem. 3). Let $A = C_l^r$ be a simple $\text{Gal}(K_0)$ -module on which $\text{Gal}(K)$ acts trivially. Suppose $\zeta_l \notin K$. Let T be a finite set of primes of K_0 and for each $\mathfrak{p} \in T$ consider an element $y_{\mathfrak{p}} \in H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$. Then there exists an element $z \in H^1(\text{Gal}(K_0), A)$ such that, if we denote $z_{\mathfrak{p}} = \text{res}_{\mathfrak{p}}(z)$, then

- (a) for each $\mathfrak{p} \in T$, $z_{\mathfrak{p}} = y_{\mathfrak{p}}$,
- (b) if $\mathfrak{p} \in \mathbb{P}(K_0) \setminus T$ and $z_{\mathfrak{p}}$ is ramified, then \mathfrak{p} totally splits in $K(\zeta_l)$.

We come now to the proof of the main result of this chapter. The first step in the construction of the element $x \in H^1(\text{Gal}(K_0), A)$ changes each given element $y_{\mathfrak{p}} \in H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ to an element $\eta_{\mathfrak{p}} \in H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ that belongs to the image of the corestriction map. After that, we shift the $\eta_{\mathfrak{p}}$'s to elements of $H^1(\text{Gal}(\hat{K}_{\mathfrak{p}}), A)$ and use Proposition 2.4.1 to find a homomorphism $h: \text{Gal}(K) \rightarrow A$ with a bound on its ramification. The corestriction map maps h onto an element $u \in H^1(\text{Gal}(K_0), A)$ which when multiplied by an element $z \in H^1(\text{Gal}(K_0), A)$ from Lemma 3.3.4 gives the desired element x .

Proposition 3.3.5. Let $K_0 \subseteq K \subseteq L$ a tower of finite Galois extension of number fields such that L/K is an abelian l -extension. Suppose $\zeta_l \notin K$. Let $A = C_l^r$ be a simple $\text{Gal}(K_0)$ -module on which $\text{Gal}(K)$ acts trivially. Let n be a multiple of l and let T be a finite set of primes of K_0 that contains all primes which are ramified in K . Let T_K be the set of primes of K that divide the primes in T . Suppose $S_0 \subseteq T_K$. For each $\mathfrak{p} \in T$, let $y_{\mathfrak{p}} \in H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$. Then there exist $\mathfrak{q}_1, \dots, \mathfrak{q}_r \in \mathbb{P}(K_0) \setminus T$ and there exists an element $x \in H^1(\text{Gal}(K_0), A)$ such that, if $x_{\mathfrak{p}} = \text{res}_{\mathfrak{p}}(x)$ then

- (a) for each $\mathfrak{p} \in T$, $x_{\mathfrak{p}} = y_{\mathfrak{p}}$,
- (b) for each $\mathfrak{p} \in \mathbb{P}(K_0) \setminus (T \cup \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\})$, the element $x_{\mathfrak{p}}$ is unramified, and
- (c) for $i = 1, \dots, r$, the prime \mathfrak{q}_i totally splits in $L(\zeta_n)$, and $x_{\mathfrak{q}_i}: \text{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \rightarrow C_l \leq A$ is a cyclic homomorphism.

- (d) Let G and \bar{G} be finite groups with $A \leq \bar{G}$, $\lambda: G \rightarrow \bar{G}$ an epimorphism. Suppose that $|\text{Ker}(\lambda)| \cdot l$ divides n . Then, for each $i = 1, \dots, r$ there exists a homomorphism $x'_{q_i}: \text{Gal}(\hat{K}_{0,q_i}) \rightarrow G$ such that $\lambda \circ x'_{q_i} = x_{q_i}$.

Proof. By Lemma 3.3.4, there exists an element $z \in H^1(\text{Gal}(K_0), A)$ such that

$$(3.3.4) \quad \text{for each } \mathfrak{p} \in T, z_{\mathfrak{p}} = y_{\mathfrak{p}},$$

$$(3.3.5) \quad \text{if } \mathfrak{p} \in \mathbb{P}(K_0) \setminus T \text{ and } z_{\mathfrak{p}} \text{ is ramified, then } \mathfrak{p} \text{ totally splits in } K(\zeta_l), \text{ in particular in } K.$$

We divide the rest of the proof in three parts.

Part A: *Definition of $\eta_{\mathfrak{p}}$.* Let $V = T \cup \{\mathfrak{p} \in \mathbb{P}(K_0) \mid z_{\mathfrak{p}} \text{ is ramified}\}$. For each $\mathfrak{p} \in V$ we define $\eta_{\mathfrak{p}} \in H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ by

$$(3.3.6) \quad \begin{aligned} \eta_{\mathfrak{p}} &= 1 \text{ for } \mathfrak{p} \in T \\ \eta_{\mathfrak{p}} &= z_{\mathfrak{p}}^{-1} \text{ for } \mathfrak{p} \in V \setminus T \end{aligned}$$

Claim: For each $\mathfrak{p} \in V$, the element $\eta_{\mathfrak{p}} \in H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ lies in the image of

$$(3.3.7) \quad \text{Cor: } \prod_{\mathfrak{q}|\mathfrak{p}} H^1(\text{Gal}(\hat{K}_{\mathfrak{q}}), A) \longrightarrow H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A).$$

Indeed, the statement holds for $\mathfrak{p} \in T$ since, by (3.3.6), $\eta_{\mathfrak{p}} = 1$ and since $\text{Cor} = \prod_{\mathfrak{q}|\mathfrak{p}} \text{cor}_{\mathfrak{q}}$ is a homomorphism of groups. If $\mathfrak{p} \in V \setminus T$, then $z_{\mathfrak{p}}$ is ramified, so by (3.3.5), \mathfrak{p} totally splits in K . It follows from Remark 3.3.1 that the map in (3.3.7) is surjective, so $\eta_{\mathfrak{p}}$ belongs to the image of Cor as claimed.

Part B: *Shifting the $\eta_{\mathfrak{p}}$'s.* For each $\mathfrak{p} \in V$ we choose a pre-image $(\tilde{\eta}_{\mathfrak{q}})_{\mathfrak{q}|\mathfrak{p}} \in \prod_{\mathfrak{q}|\mathfrak{p}} H^1(\text{Gal}(\hat{K}_{\mathfrak{q}}), A)$ of $\eta_{\mathfrak{p}} \in H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$, that is

$$(3.3.8) \quad \eta_{\mathfrak{p}} = \prod_{\mathfrak{q}|\mathfrak{p}} \text{cor}_{\mathfrak{q}}(\tilde{\eta}_{\mathfrak{q}}), \quad \mathfrak{p} \in V$$

Let $V_K = \{\mathfrak{P} \in \mathbb{P}(K) \mid \mathfrak{P}|\mathfrak{p} \text{ for a prime } \mathfrak{p} \in V\}$. Since $\text{Gal}(K)$ acts trivially on A , the map $\tilde{\eta}_{\mathfrak{P}}: \text{Gal}(\hat{K}_{\mathfrak{P}}) \rightarrow A$ is a homomorphism for each $\mathfrak{P} \in V_K$. Likewise,

$$(3.3.9) \quad z' = z|_{\text{Gal}(K)}: \text{Gal}(K) \rightarrow A$$

is a homomorphism. Let L' be the fixed field of $\text{Ker}(z')$ in \tilde{K} . Then L' is a finite abelian l -extension of K , hence so is LL' . Hence the Galois closure L'' of LL' over K_0 is a finite abelian l -extension of K . Considering the tower of number fields $K_0 \subseteq K \subseteq L''$, the set of primes V_K , and the system of homomorphisms $(\tilde{\eta}_{\mathfrak{P}})_{\mathfrak{P} \in V_K}$, Proposition 2.4.1, gives primes $\mathfrak{q}_1, \dots, \mathfrak{q}_r \in \mathbb{P}(K_0) \setminus V$ and a homomorphism $h: \text{Gal}(K) \rightarrow A$ such that, if we denote $h_{\mathfrak{P}} = \text{res}_{\mathfrak{P}}(h)$, then

$$(3.3.10) \quad \mathfrak{q}_i \text{ totally splits in } L''(\zeta_n) \text{ for } i = 1, \dots, r,$$

$$(3.3.11) \quad h_{\mathfrak{P}} = \tilde{\eta}_{\mathfrak{P}}, \text{ for each } \mathfrak{P} \in V_K,$$

$$(3.3.12) \quad \text{for } i = 1, \dots, r \text{ there exists } \mathfrak{Q}_i \in \mathbb{P}(K) \text{ with } \mathfrak{Q}_i|_{K_0} = \mathfrak{q}_i \text{ such that} \\ h(\text{Gal}(\hat{K}_{\mathfrak{Q}_i})) \cong C_i,$$

$$(3.3.13) \quad h_{\mathfrak{P}}(\hat{I}_{\mathfrak{P}}) = 1 \text{ for each } \mathfrak{P} \in \mathbb{P}(K) \setminus (V_K \cup \{\mathfrak{Q}_1, \dots, \mathfrak{Q}_r\}),$$

We consider $u = \text{cor}(h) \in H^1(\text{Gal}(K_0), A)$ and set $u_{\mathfrak{p}} = \text{res}_{\mathfrak{p}}(u)$ for each $\mathfrak{p} \in \mathbb{P}(K_0)$. By the commutativity of the diagram (3.3.1), by (3.3.11), and by (3.3.8) we have

$$(3.3.14) \quad u_{\mathfrak{p}} = \text{res}_{\mathfrak{p}}(\text{cor}(h)) = \text{Cor}(\text{Res}(h)) \\ = \prod_{\mathfrak{P}|\mathfrak{p}} \text{cor}_{\mathfrak{P}}(h_{\mathfrak{P}}) = \prod_{\mathfrak{P}|\mathfrak{p}} \text{cor}_{\mathfrak{P}}(\tilde{\eta}_{\mathfrak{P}}) = \eta_{\mathfrak{p}}, \quad \mathfrak{p} \in V.$$

Furthermore, by Corollary 3.3.3, for each $i = 1, \dots, r$

$$(3.3.15) \quad u_{\mathfrak{q}_i} = \prod_{\mathfrak{Q}|\mathfrak{q}_i} \text{cor}_{\mathfrak{Q}}(h_{\mathfrak{Q}}) \text{ is a cyclic (possibly trivial) homomorphism} \\ u_{\mathfrak{q}_i}: \text{Gal}(\hat{K}_{0, \mathfrak{q}_i}) \rightarrow C_i$$

Part C: *The element x .* We prove that the element $x = uz \in H^1(\text{Gal}(K_0), A)$ satisfies Conditions (a)-(d) of the Proposition.

Proof of (a): For each $\mathfrak{p} \in T$, we have from (3.3.13), (3.3.4), and (3.3.6) that

$$x_{\mathfrak{p}} = u_{\mathfrak{p}}z_{\mathfrak{p}} = \eta_{\mathfrak{p}}y_{\mathfrak{p}} = 1y_{\mathfrak{p}} = y_{\mathfrak{p}}.$$

Hence, x satisfies Condition (a).

Proof of (b): Let $\mathfrak{p} \in \mathbb{P}(K_0) \setminus (T \cup \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\})$. If $\mathfrak{p} \in V$, then, by (3.3.13) and (3.3.6)

$$x_{\mathfrak{p}} = u_{\mathfrak{p}}z_{\mathfrak{p}} = \eta_{\mathfrak{p}}z_{\mathfrak{p}} = z_{\mathfrak{p}}^{-1}z_{\mathfrak{p}} = 1.$$

Hence, $x_{\mathfrak{p}}$ is unramified (Def. 3.1.2(a)). If $\mathfrak{p} \notin V$, then by the definition of V in Part A, $z_{\mathfrak{p}}$ is unramified. Furthermore, since all ramified primes of K/K_0 are contained in $T \subseteq V$, \mathfrak{p} is unramified in K . Since, by (3.3.12), $h_{\mathfrak{P}}(\hat{I}_{\mathfrak{P}}) = 1$ for $\mathfrak{P}|\mathfrak{p}$, and since $u_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \text{cor}_{\mathfrak{P}}(h_{\mathfrak{P}})$ (by (3.3.13)), it follows from Lemma 3.3.2 that $u_{\mathfrak{p}}|_{\hat{I}_{\mathfrak{p}}} = 1$. Hence, $x_{\mathfrak{p}}|_{\hat{I}_{\mathfrak{p}}} = u_{\mathfrak{p}}|_{\hat{I}_{\mathfrak{p}}}z_{\mathfrak{p}}|_{\hat{I}_{\mathfrak{p}}} = 1$, so $x_{\mathfrak{p}}$ is unramified. Thus, x satisfies (b).

Proof of (c): Consider i between 1 and r . By (3.3.10), \mathfrak{q}_i totally splits K . On one hand,

$$u_{\mathfrak{q}_i} = \text{res}_{\mathfrak{q}_i}(\text{cor}(h)).$$

Hence by (3.3.14), $u_{\mathfrak{q}_i}: \text{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \rightarrow C_l \leq A$ is a cyclic homomorphism. On the other hand, since $\text{Gal}(\hat{K}_{0,\mathfrak{q}_i}) = \text{Gal}(\hat{K}_{\Omega_{i,j}})$ and since $\text{Gal}(K)$ acts trivially on A , the group $\text{Gal}(\hat{K}_{0,\mathfrak{q}_i})$ acts trivially on A , so $z_{\mathfrak{q}_i} \in H^1(\text{Gal}(\hat{K}_{0,\mathfrak{q}_i}), A)$ is a homomorphism and there exists $\Omega_{i,j}|\mathfrak{q}_i$ such that $z_{\mathfrak{q}_i} = \text{res}_{\Omega_{i,j}}(z'): \text{Gal}(\hat{K}_{\Omega_{i,j}}) \rightarrow A$ with z' as in (3.3.9). Again by (3.3.10), $\Omega_{i,j}$ totally splits in L' . Since L' is the fixed field of $\text{Ker}(z')$ (Part B), it follows that $z_{\mathfrak{q}_i}$ is the trivial homomorphism. Then $x_{\mathfrak{q}_i} = u_{\mathfrak{q}_i}$, so it is cyclic homomorphism $x_{\mathfrak{q}_i}: \text{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \rightarrow C_l$. Hence x satisfies (c), as desired.

Proof of (d): We fix i between 1 and r . By Condition (c), $x_{\mathfrak{q}_i}: \text{Gal}(K_{0,\mathfrak{q}_i}) \rightarrow C_l$

is a cyclic homomorphism. If $x_{\mathfrak{q}_i}$ is unramified, then by Lemma 1.2.6, there exists a homomorphism $x'_{\mathfrak{q}_i}: \text{Gal}(K_{0,\mathfrak{q}_i}) \longrightarrow G$ such that $\lambda \circ x'_{\mathfrak{q}_i} = x_{\mathfrak{q}_i}$. Suppose $x_{\mathfrak{q}_i}$ ramifies. Again by Condition (c), $\zeta_n \in \hat{K}_{0,\mathfrak{q}_i}$. Since $\mathfrak{q}_i \in \mathbb{P}(K_0) \setminus T$, $\mathfrak{q}_i \nmid l$, then the result follows from Lemma 1.2.7. \square

Chapter 4

Solving embedding problems with bounded ramification

This chapter contains the main results of this work. Given a finite Galois extension K/K_0 of number fields, an epimorphism $\alpha: G \rightarrow \text{Gal}(K/K_0)$ with a solvable kernel such that each of the corresponding local embedding problem is solvable, a finite subset T of $\mathbb{P}(K_0)$ that contains $\text{Ram}(K/K_0)$, and a local solution $\varphi_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \rightarrow G$ for each $\mathfrak{p} \in T$, there exist, under certain conditions on the roots of unity in K , a proper solution $\psi: \text{Gal}(K_0) \rightarrow G$ of the corresponding embedding problem and a set $R \subseteq \mathbb{P}(K_0) \setminus T$ such ψ coincides with $\varphi_{\mathfrak{p}}$ for each $\mathfrak{p} \in T$ (i.e. for $\mathfrak{p} \in T$, ψ defines the same local solution field as the solution field defined by $\varphi_{\mathfrak{p}}$) and $\text{Ram}(\psi) \subseteq T \cup R$, and $|R| = \Omega(|\text{Ker}(\alpha)|)$, where Ω is a well known arithmetical function (defined in (4.2.1)). We start with the solution of the first layer, i.e. an embedding problem whose kernel is a simple $\text{Gal}(K_0)$ -module. Then, we use induction on the order of $\text{Ker}(\alpha)$. In the last section of this chapter, we give some applications of the main result. We recall that every given homomorphism of a profinite group is assumed to be continuous.

For the rest of this chapter, as in Definition 1.2.1, if $\psi: \text{Gal}(K_0) \rightarrow G$ is a homomorphism, then we denote $\psi_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \rightarrow G$ the local restriction

defined by $\psi_{\mathfrak{p}}(\sigma) = \psi(\sigma|_{\tilde{K}_0})$.

4.1 The Principal Homogeneous Space over $H^1(\text{Gal}(K_0), A)$

As mentioned in the previous chapters, in order to carry out the induction step, the solution of the first layer must satisfy certain conditions. For that, we multiply the solution obtained by the local-global principle (Lemma 1.2.8) by a crossed homomorphism. This multiplication gives rise to an action of the first cohomology group $H^1(\text{Gal}(K_0), A)$ on the set of the solutions of the embedding problem up to equivalence class (Definition 1.2.3), where A is the kernel of the embedding problem which is abelian. In this section, we define this action and determine some of its properties for the special case $A = C_l^r$.

Let K/K_0 be a finite Galois extension of number fields with $\text{Gal}(K/K_0) = \Gamma$. Let \tilde{G} be a finite group, and let $\bar{\alpha}: \tilde{G} \rightarrow \Gamma$ be an epimorphism. Consider the following embedding problem

$$(4.1.1) \quad \begin{array}{ccccccc} & & & \text{Gal}(K_0) & & & \\ & & & \downarrow \rho & & & \\ 1 & \longrightarrow & A & \longrightarrow & \tilde{G} & \xrightarrow{\bar{\alpha}} & \Gamma & \longrightarrow & 1 \end{array},$$

(4.1.2) where $\rho = \text{res}_{\tilde{K}_0/K}$ and A is a simple Γ -module with $A = C_l^r$, and l is a prime number such that ζ_l is not fixed by $\text{Ker}(\rho)$ (i.e. $\zeta_l \notin K$).

(4.1.3) The action of Γ on A is defined by

$$\begin{aligned} \Gamma \times A &\longrightarrow A \\ (\bar{g}, a) &\longmapsto a^{\bar{g}} = g^{-1}ag, \end{aligned}$$

where $g \in \tilde{G}$ with $\bar{\alpha}(g) = \bar{g}$. The group A becomes a simple $\text{Gal}(K_0)$ -module via ρ . If $\sigma \in \text{Gal}(K_0)$ and $a \in A$, then $a^\sigma = a^{\rho(\sigma)}$. In particular, $\text{Gal}(K) = \text{Ker}(\rho)$ acts trivially on A .

We recall that $\mathcal{H}\text{om}_{\Gamma, \rho, \bar{\alpha}}(\text{Gal}(K_0), \bar{G})$ is the set of equivalence classes of the solutions of (4.1.1) and $\mathcal{H}\text{om}_{\Gamma, \rho, \bar{\alpha}}(\text{Gal}(K_0), \bar{G})_{\text{sur}}$ is the subset of equivalence classes of the proper solutions (i.e. surjective solutions).

Lemma 4.1.1. Let $\psi: \text{Gal}(K_0) \rightarrow \bar{G}$ be a homomorphism such that $\bar{\alpha} \circ \psi = \rho$, and $\chi: \text{Gal}(K_0) \rightarrow A$ is a crossed homomorphism. Then $\psi \cdot \chi: \text{Gal}(K_0) \rightarrow \bar{G}$, defined by $(\psi \cdot \chi)(\sigma) = \psi(\sigma) \cdot \chi(\sigma)$ for $\sigma \in \text{Gal}(K_0)$, is a homomorphism satisfying $\bar{\alpha} \circ (\psi \cdot \chi) = \rho$.

Proof. Denote $\psi' = \psi \cdot \chi$. For all $\sigma_1, \sigma_2 \in \text{Gal}(K_0)$, we have

$$\begin{aligned} \psi'(\sigma_1\sigma_2) &= \psi(\sigma_1\sigma_2)\chi(\sigma_1\sigma_2) \\ &= \psi(\sigma_1)\psi(\sigma_2)\chi(\sigma_1)^{\sigma_2}\chi(\sigma_2) \end{aligned}$$

Since $\bar{\alpha}(\psi(\sigma_2)) = \rho(\sigma_2)$, we have $\chi(\sigma_1)^{\sigma_2} = \chi(\sigma_1)^{\rho(\sigma_2)} = \psi(\sigma_2)^{-1}\chi(\sigma_1)\psi(\sigma_2)$. Hence,

$$\begin{aligned} \psi'(\sigma_1\sigma_2) &= \psi(\sigma_1)\psi(\sigma_2)\psi(\sigma_2)^{-1}\chi(\sigma_1)\psi(\sigma_2)\chi(\sigma_2) \\ &= \psi(\sigma_1)\chi(\sigma_1)\psi(\sigma_2)\chi(\sigma_2) \\ &= \psi'(\sigma_1)\psi'(\sigma_2). \end{aligned}$$

Moreover, for $\sigma \in \text{Gal}(K_0)$, $\bar{\alpha}(\psi'(\sigma)) = \bar{\alpha}(\psi(\sigma))\bar{\alpha}(\chi(\sigma))$. Since $\chi(\sigma) \in A = \text{Ker}(\bar{\alpha})$, we have $\bar{\alpha}(\psi'(\sigma)) = \bar{\alpha}(\psi(\sigma)) = \rho(\sigma)$, as desired. \square

The product defined in Lemma 4.1.1 gives rise to an action of $H^1(\text{Gal}(K_0), A)$ on $\mathcal{H}\text{om}_{\Gamma, \rho, \bar{\alpha}}(\text{Gal}(K_0), \bar{G})$. If $[\psi] \in \mathcal{H}\text{om}_{\Gamma, \rho, \bar{\alpha}}(\text{Gal}(K_0), \bar{G})$ and $x \in H^1(\text{Gal}(K_0), A)$, we define $[\psi'] = [\psi]^x$ such that if $\psi: \text{Gal}(K_0) \rightarrow \bar{G}$ (resp. $\chi: \text{Gal}(K_0) \rightarrow A$) is a representative of $[\psi]$ (resp. of x), then $\psi' = \psi \cdot \chi$ is a representative of $[\psi']$. In particular, $[\psi]^{x_1 x_2} = [\psi \chi_1 \chi_2] = ([\psi]^{x_1})^{x_2}$. This action does not depend on the choice of the representatives of $[\psi]$ and x . Indeed, let $\psi_1: \text{Gal}(K_0) \rightarrow \bar{G}$ be another representative of $[\psi]$. Then there exists $a \in A$ such that $\psi_1(\sigma) = a^{-1}\psi(\sigma)a$ for all $\sigma \in \text{Gal}(K_0)$. If $\chi_1: \text{Gal}(K_0) \rightarrow A$ is another representative of x , then there exists a coboundary $\gamma: \text{Gal}(K_0) \rightarrow A$ such that $\chi_1 = \gamma\chi$. Thus, there exists $b \in A$ with $\gamma(\sigma) = b^\sigma b^{-1}$ for all

$\sigma \in \text{Gal}(K_0)$. Now let $\psi'' = \psi_1 \cdot \chi_1$. For $\sigma \in \text{Gal}(K_0)$, we have, since A is abelian

$$\begin{aligned}\psi''(\sigma) &= \psi_1(\sigma) \cdot \chi_1(\sigma) = a^{-1}\psi(\sigma)a \cdot \gamma(\sigma)\chi(\sigma) \\ &= a^{-1}\psi(\sigma)a \cdot b^\sigma b^{-1}\chi(\sigma) \\ &= a^{-1}\psi(\sigma)b^\sigma ab^{-1}\chi(\sigma).\end{aligned}$$

Now, $b^\sigma = b^{\rho(\sigma)}$. Since $\bar{\alpha}(\psi(\sigma)) = \rho(\sigma)$, $b^{\rho(\sigma)} = \psi(\sigma)^{-1}b\psi(\sigma)$. Thus,

$$\begin{aligned}\psi''(\sigma) &= a^{-1}\psi(\sigma)\psi(\sigma)^{-1}b\psi(\sigma)ab^{-1}\chi(\sigma) \\ &= a^{-1}b\psi(\sigma)\chi(\sigma)ab^{-1} \\ &= (ab^{-1})^{-1}\psi'(\sigma)ab^{-1}\end{aligned}$$

Therefore, $[\psi''] = [\psi']$ as desired.

Now suppose $x = 1$, i.e. x is represented by $\chi = 1$. Hence $[\psi]^x = [\psi\chi] = [\psi]$. Thus $[\psi]^1 = [\psi]$.

In a similar way, for each $\mathfrak{p} \in \mathbb{P}(K_0)$, the cohomology group $H^1(\text{Gal}(K_{0,\mathfrak{p}}), A)$ acts on $\mathcal{H}\text{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\text{Gal}(K_{0,\mathfrak{p}}), \bar{G})$. These actions satisfy

$$[\psi]_{\mathfrak{p}}^x = [\psi_{\mathfrak{p}}]^{\text{resp}(x)},$$

for $[\psi] \in \mathcal{H}\text{om}_{\Gamma,\rho,\alpha}(\text{Gal}(K_0), \bar{G})$, $x \in H^1(\text{Gal}(K_0), A)$, and $\mathfrak{p} \in \mathbb{P}(K_0)$.

Recall that a **principal homogeneous space** X over a group H is a set X on which H acts freely and transitively (from the right). Thus, if $x \in X, \eta \in H$ and $x^\eta = x$, then $\eta = 1$. Moreover, for all $y \in X$ there exists $\tau \in H$ such that $x^\tau = y$.

Lemma 4.1.2. The set $\mathcal{H}\text{om}_{\Gamma,\rho,\bar{\alpha}}(\text{Gal}(K_0), \bar{G})$ (resp. $\mathcal{H}\text{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), \bar{G})$) is a principal homogeneous space over $H^1(\text{Gal}(K_0), A)$ (resp. $H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$), that is the action of $H^1(\text{Gal}(K_0), A)$ (resp. $H^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$) on $\mathcal{H}\text{om}_{\Gamma,\rho,\bar{\alpha}}(\text{Gal}(K_0), \bar{G})$ (resp. $\mathcal{H}\text{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), \bar{G})$) is transitive and free.

Proof. Let $[\psi], [\varphi] \in \mathcal{H}om_{\Gamma, \rho, \bar{\alpha}}(\text{Gal}(K_0), \bar{G})$ with representatives $\psi: \text{Gal}(K_0) \longrightarrow \bar{G}$ and $\varphi: \text{Gal}(K_0) \longrightarrow \bar{G}$ respectively. Let $\chi: \text{Gal}(K) \longrightarrow A$ be the map defined by $\chi(\sigma) = \varphi(\sigma)^{-1}\psi(\sigma)$ for each $\sigma \in \text{Gal}(K_0)$. Since $\bar{\alpha}(\varphi(\sigma)^{-1}\psi(\sigma)) = \bar{\alpha}(\varphi(\sigma)^{-1})\bar{\alpha}(\psi(\sigma)) = \rho(\sigma^{-1})\rho(\sigma) = 1$, we have $\varphi(\sigma)^{-1}\psi(\sigma) \in A$, so χ is well defined. Moreover, χ is a crossed homomorphism. Indeed, let $\sigma, \tau \in \text{Gal}(K_0)$. Since $\bar{\alpha}(\varphi(\tau)) = \rho(\tau)$, then

$$\begin{aligned} \chi(\sigma)^\tau \chi(\tau) &= (\varphi(\tau)^{-1}\varphi(\sigma)^{-1}\psi(\sigma)\varphi(\tau))(\varphi(\tau)^{-1}\psi(\tau)) \\ &= \varphi(\tau)^{-1}\varphi(\sigma)^{-1}\psi(\sigma)\psi(\tau) \\ &= \varphi(\sigma\tau)^{-1}\psi(\sigma\tau) \\ &= \chi(\sigma\tau). \end{aligned}$$

Let $x \in H^1(\text{Gal}(K_0), A)$ be the cohomology class of χ . Since $\psi(\sigma) = \varphi(\sigma)\chi(\sigma)$ for each $\sigma \in \text{Gal}(K_0)$, we have $[\psi] = [\varphi]^x$, so the action is transitive.

Now suppose that $[\varphi]^x = [\varphi]$ for some $x \in H^1(\text{Gal}(K_0), A)$. Let χ be a representative of x . Then, there exists $a \in A$ such that $\varphi(\sigma)\chi(\sigma) = a^{-1}\varphi(\sigma)a$, for each $\sigma \in \text{Gal}(K_0)$. Hence,

$$\begin{aligned} \chi(\sigma) &= \varphi(\sigma)^{-1}a^{-1}\varphi(\sigma)a \\ &= (a^{-1})^\sigma a. \end{aligned}$$

Hence χ is a coboundary, i.e. $x = 1$ in $H^1(\text{Gal}(K_0), A)$. Thus, the action of $H^1(\text{Gal}(K_0), A)$ on the set $\mathcal{H}om_{\Gamma, \rho, \bar{\alpha}}(\text{Gal}(K_0), \bar{G})$ is free. Similar methods hold to prove that the action of $H^1(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), A)$ on the set $\mathcal{H}om_{\Gamma, \rho_{\mathfrak{p}}, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), \bar{G})$ is transitive and free. \square

Lemma 4.1.3. Let $\mathfrak{p} \in \mathbb{P}(K_0)$. Let $[\psi] \in \mathcal{H}om_{\Gamma, \rho, \bar{\alpha}}(\text{Gal}(K_0), \bar{G})$. Suppose $[\psi]$ is unramified at \mathfrak{p} . Let $x \in H^1(\text{Gal}(K_0), A)$ such that $x_{\mathfrak{p}} = \text{res}_{\mathfrak{p}}(x) \in H^1(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), A)$ is unramified. Then $[\psi'] = [\psi]^x$ is unramified at \mathfrak{p} .

Proof. Let ψ and χ be representatives of $[\psi]$ and x respectively. Hence $\psi \cdot \chi$ is a representative of $[\psi']$. Let $\chi_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0, \mathfrak{p}}) \longrightarrow A$ be a representative

of $x_{\mathfrak{p}}$ in $\mathcal{Z}^1(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$. Since $x_{\mathfrak{p}}$ is unramified, there exists $a_{\mathfrak{p}} \in A$ such that for each $\sigma \in \hat{I}_{\mathfrak{p}}$, $\chi_{\mathfrak{p}}(\sigma) = a_{\mathfrak{p}}^{\sigma} a_{\mathfrak{p}}^{-1}$ (Definition 3.1.2(a)). Hence for each $\sigma \in \hat{I}_{\mathfrak{p}}$,

$$\begin{aligned} \psi'(\sigma) &= \psi(\sigma)\chi_{\mathfrak{p}}(\sigma) \\ &= \psi(\sigma)a_{\mathfrak{p}}^{\sigma}a_{\mathfrak{p}}^{-1} \\ &= a_{\mathfrak{p}}^{\sigma}a_{\mathfrak{p}}^{-1}, \end{aligned}$$

because $\psi(\sigma) = 1$. Now $a_{\mathfrak{p}}^{\sigma} = a_{\mathfrak{p}}^{\rho(\sigma)}$. Since $\bar{\alpha}(\psi(\sigma)) = \rho(\sigma)$, we have $a_{\mathfrak{p}}^{\sigma} = \psi(\sigma)^{-1}a_{\mathfrak{p}}\psi(\sigma) = a_{\mathfrak{p}}$. It follows that $\psi'(\sigma) = a_{\mathfrak{p}}a_{\mathfrak{p}}^{-1} = 1$, for all $\sigma \in \hat{I}_{\mathfrak{p}}$. Thus $[\psi']$ is unramified at \mathfrak{p} . \square

4.2 Embedding Problem whose Kernel is a Simple $\text{Gal}(K_0)$ -module

In this section we solve the first layer of our embedding problem. We construct an epimorphism $\bar{\psi}: \text{Gal}(K_0) \rightarrow \bar{G}$ in such a way that the induced second layer of the embedding problem is locally solvable, if \bar{N} is the solution field (fixed field of $\text{Ker}(\bar{\psi})$ in \tilde{K}_0) then $|\mu(\bar{N})|$ and the order of the kernel of the next layer are coprime, and we have a bound on $|\text{Ram}(\bar{\psi})|$.

Let K/K_0 be a finite Galois extension of number fields with $\text{Gal}(K/K_0) = \Gamma$, let $\bar{\alpha}: \bar{G} \rightarrow \Gamma$ be an epimorphism with kernel $A = C_l^r$ which is a simple Γ -module. Suppose that $\zeta_l \notin K$. We use the action of $\text{Gal}(K_0)$ on A defined in (4.1.3), to make A a simple $\text{Gal}(K_0)$ -module and $\text{Gal}(K)$ acts trivially on A .

We start with a Lemma that will assure the surjectivity of the solution $\bar{\psi}$ and handles the growth of the number of roots of unity in the solution field.

Lemma 4.2.1. Consider the embedding problem in (4.1.1). Let n be a positive integer. Let m be the minimal number of generators of $\text{Gal}(K(\zeta_n)/K)$.

Suppose that $\gcd(n, |\mu(K)|) = 1$. Let T be a finite set of primes of K_0 . There exist distinct primes $\mathfrak{p}_1, \dots, \mathfrak{p}_m, \mathfrak{q} \in \mathbb{P}(K_0) \setminus T$ which totally split in K and for each $\mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_m, \mathfrak{q}\}$ there exists an element $[\varphi_{\mathfrak{p}}] \in \mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), \bar{G})$ such that if an element $[\bar{\psi}] \in \mathcal{H}\text{om}_{\Gamma, \rho, \bar{\alpha}}(\text{Gal}(K_0), \bar{G})$, satisfies $[\bar{\psi}_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$ in $\mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), \bar{G})$ then

- (a) $[\bar{\psi}]$ is unramified at $\mathfrak{p}_1, \dots, \mathfrak{p}_m, \mathfrak{q}$,
- (b) if \bar{N} is the fixed field of $\text{Ker}(\bar{\psi})$ in \hat{K}_0 then $\gcd(n, |\mu(\bar{N})|) = 1$,
- (c) $[\bar{\psi}]$ is surjective.

Proof. We break up the proof into several parts.

Part A: *The choice of $\mathfrak{p}_1, \dots, \mathfrak{p}_m$.* Let $\text{Gal}(K(\zeta_n)/K) = \langle \sigma_1, \dots, \sigma_m \rangle$. Let $T_{K(\zeta_n)}$ be the finite set of primes of $K(\zeta_n)$ that divide the primes in T . We apply the Chebotarev density theorem and choose, by induction on m , primes $\mathfrak{Q}_1, \dots, \mathfrak{Q}_m \in \mathbb{P}(K(\zeta_n)) \setminus T_{K(\zeta_n)}$ in such a way that $\left[\frac{K(\zeta_n)/K}{\mathfrak{Q}_i} \right] = \sigma_i$ for $i = 1, \dots, m$ and the primes $\mathfrak{p}_1 = \mathfrak{Q}_1|_{K_0}, \dots, \mathfrak{p}_m = \mathfrak{Q}_m|_{K_0} \in \mathbb{P}(K_0) \setminus T$ are distinct. For each $i = 1, \dots, m$ set $\mathfrak{P}_i = \mathfrak{Q}_i|_K$. Then $\left[\frac{K/K_0}{\mathfrak{P}_i} \right] = \sigma_i|_K = 1$, so \mathfrak{p}_i totally splits in K (last paragraph of Section 1.2). Thus, $K \subset \hat{K}_{0, \mathfrak{p}_i}$. Since $\text{Gal}(K) = \text{Ker}(\rho)$, we have that $\rho_{\mathfrak{p}_i}: \text{Gal}(\hat{K}_{0, \mathfrak{p}_i}) \rightarrow \Gamma$ is trivial. Hence, the class $[\varphi_{\mathfrak{p}_i}]$ of the trivial homomorphism $\varphi_{\mathfrak{p}_i}: \text{Gal}(\hat{K}_{0, \mathfrak{p}_i}) \rightarrow \bar{G}$ is an element of $\mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}_i}, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}_i}), \bar{G})$ for each $i = 1, \dots, m$.

Part B: *The choice of the prime \mathfrak{q} .* By the Chebotarev density theorem, there exists $\mathfrak{q} \in \mathbb{P}(K_0) \setminus (T \cup \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\})$ which totally splits in K . Let $\hat{K}_{0, \mathfrak{q}, \text{ur}}$ be the maximal unramified extension of $\hat{K}_{0, \mathfrak{q}}$. Then $\text{Gal}(\hat{K}_{0, \mathfrak{q}, \text{ur}}/\hat{K}_{0, \mathfrak{q}}) \cong \hat{\mathbb{Z}}$. Let σ be the generator of $\text{Gal}(\hat{K}_{0, \mathfrak{q}, \text{ur}}/\hat{K}_{0, \mathfrak{q}})$ that corresponds under this isomorphism to 1 of $\hat{\mathbb{Z}}$. Let $a \in A$ with $a \neq 1$. Then there exists unique homomorphism $\bar{\varphi}_{\mathfrak{q}}: \text{Gal}(\hat{K}_{0, \mathfrak{q}, \text{ur}}/\hat{K}_{0, \mathfrak{q}}) \rightarrow \bar{G}$ that maps σ to a . Consider the homomorphism $\varphi_{\mathfrak{q}}: \text{Gal}(\hat{K}_{0, \mathfrak{q}}) \xrightarrow{\text{res}} \text{Gal}(\hat{K}_{0, \mathfrak{q}, \text{ur}}/\hat{K}_{0, \mathfrak{q}}) \xrightarrow{\bar{\varphi}_{\mathfrak{q}}} \bar{G}$. Since $\hat{I}_{\mathfrak{q}} = \text{Ker}(\text{Gal}(\hat{K}_{0, \mathfrak{q}}) \rightarrow \text{Gal}(\hat{K}_{0, \mathfrak{q}, \text{ur}}/\hat{K}_{0, \mathfrak{q}}))$, we have $\varphi_{\mathfrak{q}}(\hat{I}_{\mathfrak{q}}) = 1$, that is $\varphi_{\mathfrak{q}}$ is

unramified. On the other hand, since \mathfrak{q} totally splits in K , we have, as in Part A, that $\rho_{\mathfrak{q}}: \text{Gal}(\hat{K}_{0,\mathfrak{q}}) \rightarrow \Gamma$ is the trivial homomorphism. If $\tau \in \text{Gal}(\hat{K}_{0,\mathfrak{q}})$, there exists $s \in \mathbb{Z}$ such that $\varphi_{\mathfrak{q}}(\tau) = a^s$, hence $\bar{\alpha} \circ \varphi_{\mathfrak{q}}(\tau) = \bar{\alpha}(a^s) = 1 = \rho_{\mathfrak{q}}(\tau)$. It follows that $[\varphi_{\mathfrak{q}}] \in \mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{q}}, \bar{\alpha}}(\text{Gal}(\hat{K}_{0,\mathfrak{q}}), \bar{G})$.

Part C: *The conditions of the Lemma*. Now let $[\bar{\psi}] \in \mathcal{H}\text{om}_{\Gamma, \rho, \bar{\alpha}}(\text{Gal}(K_0), \bar{G})$ such that $[\bar{\psi}_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$ for $\mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_m, \mathfrak{q}\}$. Let $\bar{\psi}$ be a representative of $[\bar{\psi}]$, in particular $\bar{\alpha} \circ \bar{\psi} = \rho$.

Proof of (a). For each $\mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$, $[\varphi_{\mathfrak{p}}]$ is the class of the trivial homomorphism, so it is unramified. Hence $\bar{\psi}$ is unramified at $\mathfrak{p}_1, \dots, \mathfrak{p}_m$. Furthermore, by the definition of $[\varphi_{\mathfrak{q}}]$ in Part B to be unramified and since $[\bar{\psi}_{\mathfrak{q}}] = [\varphi_{\mathfrak{q}}]$ ($\text{Ker}(\bar{\psi}_{\mathfrak{q}}) = \text{Ker}(\varphi_{\mathfrak{q}})$), then $\bar{\psi}$ is unramified at \mathfrak{q} , as desired.

Proof of (b). Since $\bar{\alpha} \circ \bar{\psi} = \rho$, we have $\text{Ker}(\bar{\psi}) \leq \text{Ker}(\rho) = \text{Gal}(K)$. Hence, the fixed field \bar{N} of $\text{Ker}(\bar{\psi})$ contains K . Therefore, $K \subseteq \bar{N} \cap K(\zeta_n)$. In addition, $[\bar{\psi}_{\mathfrak{p}_i}] = [\varphi_{\mathfrak{p}_i}]$ and $\varphi_{\mathfrak{p}_i}$ is trivial, so $\bar{\psi}_{\mathfrak{p}_i}$ is trivial, that is $\bar{\psi}(\text{Gal}(\hat{K}_{0,\mathfrak{p}_i})) = 1$, so $\bar{N} \subset \hat{K}_{0,\mathfrak{p}_i}$ for each $i = 1, \dots, m$. Hence \mathfrak{p}_i totally splits in \bar{N} , so in $\bar{N} \cap K(\zeta_n)$. Therefore, the automorphisms $\bar{\sigma}_i = \left[\frac{\bar{N} \cap K(\zeta_n)/K}{\mathfrak{P}_i} \right]$, $i = 1, \dots, m$, which generate the Galois group $\text{Gal}(\bar{N} \cap K(\zeta_n)/K)$, are all identity. It follows that $\bar{N} \cap K(\zeta_n) \subseteq K$, hence $\bar{N} \cap K(\zeta_n) = K$. Let now $d = \text{gcd}(n, |\mu(\bar{N})|)$ and let ζ_d be a primitive d -th root of unity. Then $\zeta_d \in \bar{N} \cap K(\zeta_n) = K$. Thus $d | \text{gcd}(n, |\mu(K)|)$, so $d = 1$.

Proof of (c). Since $[\bar{\psi}_{\mathfrak{q}}] = [\varphi_{\mathfrak{q}}]$, there exists $b \in A$, with $\bar{\psi}_{\mathfrak{q}}(\tau) = b^{-1} \varphi_{\mathfrak{q}}(\tau) b$, for all $\tau \in \text{Gal}(\hat{K}_{0,\mathfrak{q}})$. Since $a \in \varphi_{\mathfrak{q}}(\text{Gal}(\hat{K}_{0,\mathfrak{q}}))$ (chosen in Part B), and A is abelian, $a \in \bar{\psi}(\text{Gal}(\hat{K}_{0,\mathfrak{q}})) \subseteq \bar{\psi}(\text{Gal}(K_0))$. Therefore $A \cap \bar{\psi}(\text{Gal}(K_0))$ is a non-trivial Γ -submodule of A . Since A is simple, $A \subseteq \bar{\psi}(\text{Gal}(K_0))$. Since $\rho: \text{Gal}(K_0) \rightarrow \Gamma$ is surjective, $\bar{\psi}(\text{Gal}(K_0)) = \bar{G}$. \square

(4.2.1) The arithmetical function $\Omega: \mathbb{N} \rightarrow \mathbb{N}$ is defined for $n = \prod_{i=1}^m l_i^{r_i}$,

where l_1, \dots, l_m are distinct prime divisors, by $\Omega(n) = \sum_{i=1}^m r_i$. Therefore, $\Omega(nm) = \Omega(n) + \Omega(m)$ (See [HaW62], p. 354, Sec. 22.10).

Now we prove the main result of this section. For the next layer, we consider an epimorphism of $\gamma: G \rightarrow \bar{G}$ of finite groups with solvable kernel.

$$(4.2.2) \quad \begin{array}{ccccccc} & & G & & \text{Gal}(K_0) & & \\ & & \downarrow \gamma & & \downarrow \rho & & \\ 1 & \longrightarrow & A & \longrightarrow & \bar{G} & \xrightarrow{\bar{\alpha}} & \Gamma & \longrightarrow & 1 \end{array},$$

Proposition 4.2.2. Consider the embedding problem in (4.2.2) with the properties as in (4.1.2), and an epimorphism $\gamma: G \rightarrow \bar{G}$ with solvable kernel from a finite group G . Let n be a positive integer multiple of $|\text{Ker}(\gamma)|l$. Let T be a finite set of primes of K_0 such that $\text{Ram}(K/K_0) \subseteq T$. Suppose $\gcd(n, |\mu(K)|) = 1$, and $\prod_{\mathfrak{p}} \mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), \bar{G}) \neq \emptyset$. For each $\mathfrak{p} \in T$, let $[\varphi_{\mathfrak{p}}] \in \mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), \bar{G})$. There exists a set $R \subset \mathbb{P}(K_0) \setminus T$ with $|R| = \Omega(|A|)$ and there exists an element $[\bar{\psi}] \in \mathcal{H}\text{om}_{\Gamma, \rho, \bar{\alpha}}(\text{Gal}(K_0), \bar{G})_{\text{sur}}$ such that

- (a) $[\bar{\psi}_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$ in $\mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), \bar{G})$ for each $\mathfrak{p} \in T$,
- (b) $[\bar{\psi}]$ is unramified at each $\mathfrak{p} \in \mathbb{P}(K_0) \setminus (T \cup R)$, that is if \bar{N} is the solution field (fixed field of $\text{Ker}(\bar{\psi})$) then $\text{Ram}(\bar{N}/K_0) \subset T \cup R$,
- (c) $[\bar{\psi}_{\mathfrak{p}}]$ can be lifted to an element $[\psi_{\mathfrak{p}}] \in \mathcal{H}\text{om}_{\bar{G}, \bar{\psi}_{\mathfrak{p}}, \gamma}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G)$ for each $\mathfrak{p} \in \mathbb{P}(K_0) \setminus T$, and
- (d) $\gcd(n, |\mu(\bar{N})|) = 1$.

Proof. Assume without loss that the basic set $S_0 \subseteq T_K$ where T_K is the set of primes of K that lie over the primes in T . We break up the proof into three parts.

Part A: *The surjectivity and the number of roots of unity.* Let m be the minimal number of generators of $\text{Gal}(K(\zeta_n)/K)$. We choose $\mathfrak{p}_1, \dots, \mathfrak{p}_m, \mathfrak{q} \in$

$\mathbb{P}(K_0) \setminus T$ and elements $[\varphi_{\mathfrak{p}}]$ in the set $\mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), \bar{G})$ for each $\mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_m, \mathfrak{q}\}$ that satisfy the conditions of Lemma 4.2.1. If $[\bar{\psi}] \in \mathcal{H}\text{om}_{\Gamma, \rho, \bar{\alpha}}(\text{Gal}(K_0), \bar{G})$ satisfies $[\bar{\psi}_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$ for each $\mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_m, \mathfrak{q}\}$, then by Lemma 4.2.1:

(4.2.3) $[\bar{\psi}]$ is unramified at $\mathfrak{q}, \mathfrak{p}_1, \dots, \mathfrak{p}_m$,

(4.2.4) the fixed field \bar{N} of $\text{Ker}(\bar{\psi})$ satisfies $\text{gcd}(n, |\mu(\bar{N})|) = 1$, and

(4.2.5) $[\bar{\psi}]$ is surjective.

Since $\prod_{\mathfrak{p}} \mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), \bar{G}) \neq \emptyset$, by Lemma 1.2.8, there exists an element $[\psi_0] \in \mathcal{H}\text{om}_{\Gamma, \rho, \bar{\alpha}}(\text{Gal}(K_0), \bar{G})$. Our aim is to change $[\psi_0]$ by the action of an element of $H^1(\text{Gal}(K_0), A)$ to an element $[\bar{\psi}]$ which satisfies the conclusion of the Proposition.

Let N_0 be the fixed field of the kernel of $\psi_0: \text{Gal}(K_0) \rightarrow \bar{G}$. Then, N_0 is a finite Galois extension of K_0 that contains K such that N_0/K is an abelian l -extension ($\text{Gal}(N_0/K) \leq A$).

Part B: *The sets T^* and T^{**} .* Let $T^* = T \cup \{\mathfrak{q}, \mathfrak{p}_1, \dots, \mathfrak{p}_m\}$. Let $\mathfrak{u}_1, \dots, \mathfrak{u}_v \in \mathbb{P}(K_0) \setminus T^*$ be the primes where ψ_0 ramifies. Then each \mathfrak{u}_i is unramified in K . It follows from Lemma 1.2.6 that the unramified homomorphism $\rho_{\mathfrak{u}_i}: \text{Gal}(\hat{K}_{0, \mathfrak{u}_i}) \rightarrow \Gamma$ can be lifted to an element $[\varphi_{\mathfrak{u}_i}] \in \mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{u}_i}, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{u}_i}), \bar{G})$ which is unramified for each $i = 1, \dots, v$. Hence, if $[\bar{\psi}] \in \mathcal{H}\text{om}_{\Gamma, \rho, \bar{\alpha}}(\text{Gal}(K_0), \bar{G})$ satisfies $[\bar{\psi}_{\mathfrak{u}_i}] = [\varphi_{\mathfrak{u}_i}]$ for each $i = 1, \dots, v$, then:

(4.2.6) $[\bar{\psi}]$ is unramified at $\mathfrak{u}_1, \dots, \mathfrak{u}_v$.

For each $\mathfrak{p} \in \mathbb{P}(K_0)$, let $\psi_{0\mathfrak{p}}: \text{Gal}(\hat{K}_{0, \mathfrak{p}}) \rightarrow G$ be the restriction of ψ_0 to $\text{Gal}(\hat{K}_{0, \mathfrak{p}})$. Let $T^{**} = T^* \cup \{\mathfrak{u}_1, \dots, \mathfrak{u}_v\}$. Then

(4.2.7) ψ_0 is unramified at each $\mathfrak{p} \in \mathbb{P}(K_0) \setminus T^{**}$.

Consider the system $([\varphi_{\mathfrak{p}}] \in \mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \alpha}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G))_{\mathfrak{p} \in T^{**}}$. For each $\mathfrak{p} \in T^{**}$, by Lemma 4.1.2, there exists a unique element $y_{\mathfrak{p}} \in H^1(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), A)$ that

satisfies:

$$(4.2.8) \quad [\psi_{0\mathfrak{p}}]^{y_{\mathfrak{p}}} = [\varphi_{\mathfrak{p}}]$$

The module A is a simple $\text{Gal}(K_0)$ -module and $\text{Gal}(K)$ acts trivially on A . Furthermore, the set S_0 is contained in the set T_K^{**} of all primes of K that lie over T^{**} . Since $\gcd(n, |\mu(K)|) = 1$, we have $\zeta_l \notin K$. Moreover, since N_0/K is an abelian l -extension, Proposition 3.3.5 gives an element $x \in H^1(\text{Gal}(K_0), A)$ and primes $\mathfrak{q}_1, \dots, \mathfrak{q}_r \in \mathbb{P}(K_0) \setminus T^{**}$ such that:

$$(4.2.9) \quad x_{\mathfrak{p}} = y_{\mathfrak{p}} \text{ for } \mathfrak{p} \in T^{**}$$

$$(4.2.10) \quad x_{\mathfrak{p}} \text{ is unramified for each } \mathfrak{p} \in \mathbb{P}(K_0) \setminus (T^{**} \cup \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}).$$

$$(4.2.11) \quad \text{for } i = 1, \dots, r, \mathfrak{q}_i \text{ totally splits in } N_0(\zeta_n), \text{ and } x_{\mathfrak{q}_i}: \text{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \longrightarrow C_l \text{ is a cyclic homomorphism,}$$

$$(4.2.12) \quad \text{for each } i = 1, \dots, r, x_{\mathfrak{q}_i} \text{ can be lifted to a } \bar{G}\text{-homomorphism } x'_{\mathfrak{q}_i}: \text{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \rightarrow G \text{ (i.e. } \gamma \circ x'_{\mathfrak{q}_i} = x_{\mathfrak{q}_i}).$$

Part C: *The solution $\bar{\psi}$.* We prove that the element $[\bar{\psi}] = [\psi_0]^x$ of $\mathcal{H}\text{om}_{\Gamma,\rho,\bar{\alpha}}(\text{Gal}(K_0), \bar{G})$ satisfies the conclusion of the Proposition.

For each $\mathfrak{p} \in T^{**}$, by (4.2.9) and (4.2.8):

$$(4.2.13) \quad [\bar{\psi}_{\mathfrak{p}}] = [\psi_{0\mathfrak{p}}]^{x_{\mathfrak{p}}} = [\psi_{0\mathfrak{p}}]^{y_{\mathfrak{p}}} = [\varphi_{\mathfrak{p}}] \text{ in } \mathcal{H}\text{om}_{\Gamma,\rho,\bar{\alpha}}(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), \bar{G})$$

Proof of (a): Since $T \subseteq T^{**}$, by (4.2.13), Condition (a) holds.

Proof of (b): Denote $R = \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$. Let $\mathfrak{p} \in \mathbb{P}(K_0) \setminus (T \cup R)$. If $\mathfrak{p} \in T^{**}$ (that is $\mathfrak{p} \in \{\mathfrak{q}, \mathfrak{p}_1, \dots, \mathfrak{p}_m, \mathfrak{u}_1, \dots, \mathfrak{u}_v\}$), then, by (4.2.3) and (4.2.6), $[\bar{\psi}]$ is unramified at \mathfrak{p} . If $\mathfrak{p} \in \mathbb{P}(K_0) \setminus (T^{**} \cup \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\})$, then by (4.2.7) and (4.2.10), $[\psi_{0\mathfrak{p}}]$ and $x_{\mathfrak{p}}$ are unramified. Hence, by Lemma 4.1.3, $[\bar{\psi}_{\mathfrak{p}}] = [\psi_{0\mathfrak{p}}]^{x_{\mathfrak{p}}}$ is unramified. So Condition (b) holds. Note that $|R| = \Omega(|A|)$.

Proof of (c): Let $\mathfrak{p} \in \mathbb{P}(K_0) \setminus T$. If $\mathfrak{p} \notin R$, then by (b), $[\bar{\psi}_{\mathfrak{p}}]$ is unramified. It follows from Lemma 1.2.6 that $\bar{\psi}_{\mathfrak{p}}$ can be lifted to an unramified element of $\mathcal{H}\text{om}_{\bar{G}, \bar{\psi}_{\mathfrak{p}}, \gamma}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G)$. If $\mathfrak{p} \in R$, then, by (4.2.11), \mathfrak{p} totally splits in $N_0(\zeta_n)$, in particular in N_0 . Hence $\psi_{0\mathfrak{p}}: \text{Gal}(\hat{K}_{0, \mathfrak{p}}) \rightarrow \bar{G}$ is the trivial homomorphism. Furthermore, by (4.2.11), the homomorphism $x_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0, \mathfrak{p}}) \rightarrow C_l$ satisfies

$$(4.2.14) \quad [\bar{\psi}_{\mathfrak{p}}] = [\psi_{0\mathfrak{p}}]^{x_{\mathfrak{p}}} = [\psi_{0\mathfrak{p}} \cdot x_{\mathfrak{p}}] = [x_{\mathfrak{p}}],$$

because $x_{\mathfrak{p}}$ represents its own class. By (4.2.12), $x_{\mathfrak{p}}$ can be lifted to a \bar{G} -homomorphism $x'_{\mathfrak{p}}$. Hence, also $\bar{\psi}_{\mathfrak{p}}$ has the same property. Therefore, $\mathcal{H}\text{om}_{\bar{G}, \bar{\psi}_{\mathfrak{p}}, \gamma}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G) \neq \emptyset$.

Proof of (d): From (4.2.4), the fixed field \bar{N} of $\bar{\psi}$ satisfies $\gcd(n, |\mu(\bar{N})|) = 1$. And by (4.2.5), $\bar{\psi}$ is surjective, and this completes the proof. \square

The epimorphism $\bar{\psi}: \text{Gal}(K_0) \rightarrow \bar{G}$ defined in Proposition 4.2.2 gives rise to an embedding problem

$$(4.2.15) \quad \begin{array}{ccccccc} & & & & \text{Gal}(K_0) & & \\ & & & & \downarrow \bar{\psi} & & \\ 1 & \longrightarrow & \text{Ker}(\gamma) & \longrightarrow & G & \xrightarrow{\gamma} & \bar{G} \longrightarrow 1, \end{array}$$

with solvable kernel which will be the next layer. The condition $\prod_{\mathfrak{p}} \mathcal{H}\text{om}_{\bar{G}, \bar{\psi}_{\mathfrak{p}}, \gamma}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G) \neq \emptyset$ is necessary in order that the global embedding problem has a solution. By (c) of that Proposition, for each $\mathfrak{p} \in \mathbb{P}(K_0) \setminus T$, $\mathcal{H}\text{om}_{\bar{G}, \bar{\psi}_{\mathfrak{p}}, \gamma}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G) \neq \emptyset$. For $\mathfrak{p} \in T$, in the next section, the properties of the epimorphism γ and the equality $[\bar{\psi}_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$ as in (a) of the Proposition will allow us to show the solvability of the corresponding local embedding problem.

4.3 Embedding Problem with Solvable Kernel

We are now ready to prove the main result of this work. Our approach is similar to that of [Neu79]. However we give an explicit bound on the ramification of our solution based on the bound given in the first layer (Proposition 4.2.2).

Construction 4.3.1. Consider the following finite embedding problem, where $H = \text{Ker}(\alpha)$ is solvable,

$$(4.3.1) \quad \begin{array}{ccccccc} & & & & \text{Gal}(K_0) & & \\ & & & & \downarrow \rho & & \\ 1 & \longrightarrow & H & \longrightarrow & G & \xrightarrow{\alpha} & \Gamma & \longrightarrow & 1 \end{array}$$

It suffices to solve the problem in the case where H is non-trivial. To simplify the notation, for each $a \in H$ and each Γ -homomorphism $\varphi: \text{Gal}(K_0) \rightarrow G$, let $\varphi^a: \text{Gal}(K_0) \rightarrow G$ be the homomorphism defined for each $\sigma \in \text{Gal}(K_0)$ by $\varphi^a(\sigma) = a^{-1}\varphi(\sigma)a$ (i.e. φ^a and φ are $\text{Ker}(\alpha)$ -conjugate).

Since H is solvable, it has a normal subgroup H_1 such that H/H_1 is a non-trivial abelian group. Note that for each $g \in G$, $H_1^g = g^{-1}H_1g$ is a normal subgroup of H with H/H_1^g is abelian. The subgroup $\bigcap_{g \in G} H_1^g$ is the kernel of the homomorphism $\theta: H \rightarrow \prod_{g \in G} H/H_1^g$ defined by $\theta(h) = (hH_1^g)_{g \in G}$ for each $h \in H$. It follows that $H/\bigcap_{g \in G} H_1^g$ can be embedded in $\prod_{g \in G} H/H_1^g$. Hence $H/\bigcap_{g \in G} H_1^g$ is abelian. Replacing H_1 by $\bigcap_{g \in G} H_1^g$, we may assume that H_1 is normal in G . Now, we replace H_1 , if necessary, by a larger subgroup of H to assume that H_1 is a maximal subgroup of H with the property that it is normal in G and H/H_1 is non-trivial abelian. Lifting elements of Γ via α followed by conjugation gives rise to an action of Γ on H/H_1 .

Hence H/H_1 becomes a simple Γ -module. Therefore H/H_1 becomes a simple $\text{Gal}(K_0)$ -module via ρ . Thus there exist a prime number l_1 and a positive integer r_1 such that $H/H_1 \cong C_{l_1}^{r_1}$.

Note that $|H| = |H/H_1| \cdot |H_1|$. Hence by (4.2.1), we have

$$(4.3.2) \quad \Omega(|H|) = \Omega(|H/H_1|) + \Omega(|H_1|).$$

Using Proposition 4.2.2, we first solve the step:

$$\begin{array}{ccccccc}
 & & G & & \text{Gal}(K_0) & & \\
 & & \downarrow \pi & \swarrow \psi^{(1)} & \downarrow \rho & & \\
 1 & \longrightarrow & H/H_1 & \longrightarrow & G/H_1 & \xrightarrow{\bar{\alpha}} & \Gamma \longrightarrow 1 .
 \end{array}$$

After that we apply induction on the order of H in the step

$$\begin{array}{ccccccc}
 & & & & \text{Gal}(K_0) & & \\
 & & & & \downarrow \psi^{(1)} & & \\
 1 & \longrightarrow & H_1 & \longrightarrow & G & \xrightarrow{\pi} & G/H_1 \longrightarrow 1 ,
 \end{array}$$

and show that the obtained solution in this step is the desired solution of the original embedding problem (4.3.1).

Theorem 4.3.2. *Let K/K_0 be a finite Galois extension of number fields and consider the finite embedding problem (4.3.1) with a solvable kernel H , where $\Gamma = \text{Gal}(K/K_0)$ and ρ being the restriction map. Let T be a finite set of primes of K_0 such that $\text{Ram}(K/K_0) \subseteq T$. Suppose $\gcd(|H|, |\mu(K)|) = 1$, and $\prod_{\mathfrak{p}} \mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \alpha}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G) \neq \emptyset$. For each $\mathfrak{p} \in T$, let $[\varphi_{\mathfrak{p}}] \in \mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \alpha}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G)$. Then there exists an element $[\psi] \in \mathcal{H}\text{om}_{\Gamma, \rho, \alpha}(\text{Gal}(K_0), G)_{\text{sur}}$ and there exists a set $R \subset \mathbb{P}(K_0) \setminus T$ with $|R| = \Omega(|H|)$ such that*

(a) $[\psi_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$ in $\mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \alpha}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G)$ for each $\mathfrak{p} \in T$,

(b) $[\psi]$ is unramified at each $\mathfrak{p} \in \mathbb{P}(K_0) \setminus (T \cup R)$, that is, if N is the fixed field of $\text{Ker}(\psi)$, then $\text{Ram}(N/K_0) \subseteq T \cup R$.

Proof. Let H_1 be the normal subgroup of G contained in H with H/H_1 being a simple G -module constructed in Construction 4.3.1. The proof breaks up into three parts.

Part A: *An embedding problem whose kernel is a simple $\text{Gal}(K_0)$ -module.* Let $\pi: G \rightarrow G/H_1$ be the quotient map. Then, there exists an epimorphism $\bar{\alpha}: G/H_1 \rightarrow \Gamma$ with $\bar{\alpha} \circ \pi = \alpha$. Consider the following embedding problem:

$$(4.3.3) \quad \begin{array}{ccccccc} & & G & & \text{Gal}(K_0) & & \\ & & \downarrow \pi & & \downarrow \rho & & \\ 1 & \longrightarrow & H/H_1 & \longrightarrow & G/H_1 & \xrightarrow{\bar{\alpha}} & \Gamma & \longrightarrow & 1 \end{array}$$

Let $\mathcal{H}\text{om}_{\Gamma, \rho_p, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G/H_1)$ be the set of the equivalence classes corresponding to the diagram

$$\begin{array}{ccc} & \text{Gal}(K_0) & \\ & \swarrow \text{---} & \downarrow \rho \\ G/H_1 & \xrightarrow{\bar{\alpha}} & \Gamma \end{array}$$

For each $\mathfrak{p} \in \mathbb{P}(K_0)$, if $[\eta_{\mathfrak{p}}] \in \mathcal{H}\text{om}_{\Gamma, \rho_p, \alpha}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G)$ and $\bar{\eta}_{\mathfrak{p}} = \pi \circ \eta_{\mathfrak{p}}$, then the following diagram commutes:

$$\begin{array}{ccccccc} & & & & \text{Gal}(\hat{K}_{0, \mathfrak{p}}) & & \\ & & & & \downarrow \eta_{\mathfrak{p}} & & \downarrow \rho_{\mathfrak{p}} \\ & & & & G & & \\ & & \swarrow \bar{\eta}_{\mathfrak{p}} & & \downarrow \pi & & \\ 1 & \longrightarrow & H/H_1 & \longrightarrow & G/H_1 & \xrightarrow{\bar{\alpha}} & \Gamma & \longrightarrow & 1 \\ & & & & \downarrow \alpha & & \end{array}$$

It follows that $[\bar{\eta}_{\mathfrak{p}}] \in \mathcal{H}\text{om}_{\Gamma, \rho_p, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G/H_1)$. Hence

$$\prod_{\mathfrak{p}} \mathcal{H}\text{om}_{\Gamma, \rho_p, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G/H_1) \neq \emptyset.$$

For each $\mathfrak{p} \in T$, consider the element $[\bar{\varphi}_{\mathfrak{p}}] \in \mathcal{H}\text{om}_{\Gamma, \rho_p, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G/H_1)$ with $\bar{\varphi}_{\mathfrak{p}} = \pi \circ \varphi_{\mathfrak{p}}$.

Since $|H|$ is a multiple of $l_1|H_1|$ and $\gcd(|H|, |\mu(K)|) = 1$, Proposition 4.2.2 (taking $n = |H|$) provides a set $T_1 \subseteq \mathbb{P}(K_0) \setminus T$ of order $\Omega(|H/H_1|)$ and an element $[\psi^{(1)}] \in \mathcal{H}om_{\Gamma, \rho, \bar{\alpha}}(\text{Gal}(K_0), G/H_1)_{\text{sur}}$ such that

$$(4.3.4) \quad [\psi_{\mathfrak{p}}^{(1)}] = [\bar{\varphi}_{\mathfrak{p}}] \text{ in } \mathcal{H}om_{\Gamma, \rho_{\mathfrak{p}}, \bar{\alpha}}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G/H_1) \text{ for each } \mathfrak{p} \in T,$$

$$(4.3.5) \quad [\psi^{(1)}] \text{ is unramified at each } \mathfrak{p} \in \mathbb{P}(K_0) \setminus (T \cup T_1), \text{ that is if } N^{(1)} \text{ is the fixed field of } \text{Ker}(\psi^{(1)}) \text{ then } \text{Ram}(N^{(1)}/K_0) \subseteq T \cup T_1,$$

$$(4.3.6) \quad \text{for each } \mathfrak{p} \in \mathbb{P}(K_0) \setminus T, \text{ we may lift } [\psi_{\mathfrak{p}}^{(1)}] \text{ to an element of } \mathcal{H}om_{G/H_1, \psi_{\mathfrak{p}}^{(1)}, \pi}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G), \text{ and}$$

$$(4.3.7) \quad \gcd(|H|, |\mu(N^{(1)})|) = 1.$$

Part B: *The induction step.* This gives rise to an embedding problem:

$$(4.3.8) \quad \begin{array}{ccccccc} & & & & \text{Gal}(K_0) & & \\ & & & & \downarrow \psi^{(1)} & & \\ 1 & \longrightarrow & H_1 & \longrightarrow & G & \xrightarrow{\pi} & G/H_1 \longrightarrow 1 \end{array}$$

with a finite solvable kernel. Consider the set $\mathcal{H}om_{G/H_1, \psi_{\mathfrak{p}}^{(1)}, \pi}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G)$ which corresponds to the diagram

$$\begin{array}{ccc} & \text{Gal}(\hat{K}_{0, \mathfrak{p}}) & \\ & \swarrow \text{---} & \downarrow \psi_{\mathfrak{p}}^{(1)} \\ G & \xrightarrow{\pi} & G/H_1 \end{array}$$

For each $\mathfrak{p} \in T$, by (4.3.4), there exists $a_{\mathfrak{p}} \in H$, such that for each $\sigma \in \text{Gal}(\hat{K}_{0, \mathfrak{p}})$

$$\psi_{\mathfrak{p}}^{(1)}(\sigma) = \pi(a_{\mathfrak{p}})^{-1} \bar{\varphi}(\sigma) \pi(a_{\mathfrak{p}}) = \pi(a_{\mathfrak{p}})^{-1} (\pi \circ \varphi_{\mathfrak{p}})(\sigma) \pi(a_{\mathfrak{p}}) = \pi(a_{\mathfrak{p}}^{-1} \varphi_{\mathfrak{p}}(\sigma) a_{\mathfrak{p}}) = \pi \circ \varphi_{\mathfrak{p}}^{a_{\mathfrak{p}}}(\sigma).$$

$$(4.3.9) \quad \text{So } [\varphi_{\mathfrak{p}}^{a_{\mathfrak{p}}}] \in \mathcal{H}om_{G/H_1, \psi_{\mathfrak{p}}^{(1)}, \pi}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G) \text{ for each } \mathfrak{p} \in T.$$

It follows from (4.3.6) and (4.3.9) that $\prod_{\mathfrak{p}} \mathcal{H}om_{G/H_1, \psi_{\mathfrak{p}}^{(1)}, \pi}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G) \neq \emptyset$. Moreover, (4.3.7) implies that $\gcd(|H_1|, |\mu(N^{(1)})|) = 1$.

Consider the system $([\varphi_{\mathfrak{p}}^{(1)}] \in \mathcal{H}\text{om}_{G/H_1, \psi_{\mathfrak{p}}^{(1)}, \pi}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G))_{\mathfrak{p} \in T \cup T_1}$, such that if $\mathfrak{p} \in T$ then $\varphi_{\mathfrak{p}}^{(1)} = \varphi_{\mathfrak{p}}^{a_{\mathfrak{p}}}$, and if $\mathfrak{p} \in T_1$ we use (4.3.6) to choose $[\varphi_{\mathfrak{p}}^{(1)}]$.

Since H_1 is solvable and $|H_1| < |H|$, our induction hypothesis provides a set $R_1 \subset \mathbb{P}(K_0) \setminus (T \cup T_1)$ with $|R_1| = \Omega(|H_1|)$, and an element $[\psi] \in \mathcal{H}\text{om}_{G/H_1, \psi^{(1)}, \pi}(\text{Gal}(K_0), G)_{\text{sur}}$ such that

$$(4.3.10) \text{ for each } \mathfrak{p} \in T \cup T_1, [\psi_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}^{(1)}] \text{ in } \mathcal{H}\text{om}_{G/H_1, \psi_{\mathfrak{p}}^{(1)}, \pi}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G),$$

$$(4.3.11) [\psi] \text{ is unramified at each } \mathfrak{p} \in \mathbb{P}(K_0) \setminus (T \cup T_1 \cup R_1), \text{ that is if } N \text{ is the solution field then } \text{Ram}(N/K_0) \subseteq T \cup T_1 \cup R_1.$$

We set $R = T_1 \cup R_1$. Then $|R| = |T_1| + |R_1| = \Omega(|H/H_1|) + \Omega(|H_1|) = \Omega(|H|)$ (See 4.3.2).

Part C: *Conclusion of the proof.* Let us prove that $[\psi]$ satisfies the conclusion of the Theorem. Indeed, $\pi \circ \psi = \psi^{(1)}$, so $\bar{\alpha} \circ \pi \circ \psi = \bar{\alpha} \circ \psi^{(1)}$. Since $\bar{\alpha} \circ \pi = \alpha$ and $\bar{\alpha} \circ \psi^{(1)} = \rho$, we have $\alpha \circ \psi = \rho$, that is $[\psi] \in \mathcal{H}\text{om}_{\Gamma, \rho, \alpha}(\text{Gal}(K_0), G)_{\text{sur}}$.

$$\begin{array}{ccccccc}
 & & & & 1 & & \\
 & & & & \downarrow & & \\
 & & & & H_1 & & \\
 & & & & \downarrow & & \\
 & & & & G & \xrightarrow{\psi} & \text{Gal}(K_0) \\
 1 & \longrightarrow & H & \longrightarrow & G & \xrightarrow{\psi^{(1)}} & \Gamma \\
 & & \downarrow & & \downarrow \pi & \searrow \alpha & \downarrow \rho \\
 1 & \longrightarrow & H/H_1 & \longrightarrow & G/H_1 & \xrightarrow{\bar{\alpha}} & \Gamma \longrightarrow 1 \\
 & & & & \downarrow & & \\
 & & & & 1 & &
 \end{array}$$

Furthermore, by (4.3.10), for each $\mathfrak{p} \in T$, there exists $b_{\mathfrak{p}} \in H_1$ such that for

each $\sigma \in \text{Gal}(\hat{K}_{0,\mathfrak{p}})$

$$\begin{aligned} \psi_{\mathfrak{p}}(\sigma) &= \left(\varphi_{\mathfrak{p}}^{(1)}\right)^{b_{\mathfrak{p}}}(\sigma) \\ &= b_{\mathfrak{p}}^{-1} a_{\mathfrak{p}}^{-1} \varphi_{\mathfrak{p}}(\sigma) a_{\mathfrak{p}} b_{\mathfrak{p}} \\ &= (a_{\mathfrak{p}} b_{\mathfrak{p}})^{-1} \varphi_{\mathfrak{p}}(\sigma) (a_{\mathfrak{p}} b_{\mathfrak{p}}) \\ &= \varphi_{\mathfrak{p}}^{a_{\mathfrak{p}} b_{\mathfrak{p}}}(\sigma) \end{aligned}$$

Since $a_{\mathfrak{p}} \in H$, $b_{\mathfrak{p}} \in H_1$, we have $a_{\mathfrak{p}} b_{\mathfrak{p}} \in H$. Therefore $[\psi_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$ in $\text{Hom}_{\Gamma, \rho_{\mathfrak{p}}, \alpha}(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), G)$ for each $\mathfrak{p} \in T$, as desired. \square

4.4 Solving Embedding Problems with Solvable Kernels in $K_{0,\text{tot},S}$

In this section we give some applications of the main theorem of this work. Let K_0 be a number field and S a finite set of primes of K_0 . Let $K_{0,\text{tot},S}$ be the maximal Galois extension of K_0 where each prime $\mathfrak{p} \in S$ totally splits. By definition

$$K_{0,\text{tot},S} = \bigcap_{\mathfrak{p} \in S} \bigcap_{\sigma \in \text{Gal}(K_0)} K_{0,\mathfrak{p}}^{\sigma},$$

where $K_{0,\mathfrak{p}}$ is a henselization of K_0 at \mathfrak{p} (the algebraic part of $\hat{K}_{0,\mathfrak{p}}$).

In particular, for a prime p we write $\mathbb{Q}_{\text{tot},p}$ rather than $\mathbb{Q}_{\text{tot},\{p\}}$. In this case the thesis [Rami13] conjectures that every finite group that can be realized over \mathbb{Q} can also be realized over \mathbb{Q} in $\mathbb{Q}_{\text{tot},p}$. We proved there that every abelian group, symmetric group, and alternating group can be realized over \mathbb{Q} in $\mathbb{Q}_{\text{tot},p}$. Starting from embedding problem (4.4.1), Theorem 4.3.2 allows us now to solve it with local data and bounded ramification in $K_{0,\text{tot},S}$ once the kernel H is solvable, $\gcd(|H|, |\mu(K)|) = 1$, $K \subset K_{0,\text{tot},S}$, and each of the corresponding local embedding problem is solvable. In particular, the latter result leads to the realization of every solvable group over K_0 in $K_{0,\text{tot},S}$ with bounded ramification, and to the solvability of each split embedding problem

in $K_{0,\text{tot},S}$ under the above necessary condition.

Let K/K_0 be a finite Galois extension of number fields with $\text{Gal}(K/K_0) = \Gamma$. Set $\rho = \text{res}_{\hat{K}_0/K}$. Consider the finite embedding problem

$$(4.4.1) \quad \begin{array}{ccccccc} & & & & \text{Gal}(K_0) & & \\ & & & & \downarrow \rho & & \\ 1 & \longrightarrow & H & \longrightarrow & G & \xrightarrow{\alpha} & \Gamma & \longrightarrow & 1 \end{array}$$

with H a solvable group. Under the conditions of Theorem 4.3.2, if $K \subset K_{0,\text{tot},S}$, then the embedding problem has a proper solution in $K_{0,\text{tot},S}$ with bounded ramification.

Theorem 4.4.1. *Let K/K_0 be a finite Galois extension of number fields, and let S be a finite set of primes of K_0 such that $K \subseteq K_{0,\text{tot},S}$. Consider embedding problem (4.4.1) with a solvable kernel H , where $\Gamma = \text{Gal}(K/K_0)$ and ρ being the restriction map. Suppose $\gcd(|H|, |\mu(K)|) = 1$, and $\prod_{\mathfrak{p}} \mathcal{H}\text{om}_{\Gamma, \rho, \alpha}(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), G) \neq \emptyset$. Let $T \subset \mathbb{P}(K_0) \setminus S$ be a finite set of primes such that $\text{Ram}(K/K_0) \subseteq T$. For each $\mathfrak{p} \in T$, let $[\varphi_{\mathfrak{p}}] \in \mathcal{H}\text{om}_{\Gamma, \rho, \alpha}(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), G)$. There exists an element $[\psi] \in \mathcal{H}\text{om}_{\Gamma, \rho, \alpha}(\text{Gal}(K_0), G)_{\text{sur}}$ and there exists a set $R \subseteq \mathbb{P}(K_0) \setminus (T \cup S)$ with $|R| = \Omega(|H|)$, such that if we denote $[\psi_{\mathfrak{p}}] = [\psi|_{\text{Gal}(\hat{K}_{0,\mathfrak{p}})}]$ then*

- (a) $[\psi_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$ for each $\mathfrak{p} \in T$,
- (b) the fixed field N of $\text{Ker}(\psi)$ satisfies $N \subset K_{0,\text{tot},S}$,
- (c) $\text{Ram}(N/K_0) \subseteq T \cup R$.

Proof. Since $K \subset K_{0,\text{tot},S}$, each $\mathfrak{p} \in S$ totally splits in K , hence \mathfrak{p} is unramified in K and $\rho_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \rightarrow \Gamma$ is the trivial homomorphism. Thus, the equivalence class of the trivial homomorphism $\varphi_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0,\mathfrak{p}}) \rightarrow G$ is an element of $\mathcal{H}\text{om}_{\Gamma, \rho, \alpha}(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), G)$. Let $T_1 = T \cup S$ and consider the system $([\varphi_{\mathfrak{p}}] \in \mathcal{H}\text{om}_{\Gamma, \rho, \alpha}(\text{Gal}(\hat{K}_{0,\mathfrak{p}}), G))_{\mathfrak{p} \in T_1}$.

By Theorem 4.3.2, there exists an element $[\psi] \in \mathcal{H}\text{om}_{\Gamma, \rho, \alpha}(\text{Gal}(K_0), G)_{\text{sur}}$ and there exists an set $R \subset \mathbb{P} \setminus T_1$ with $|R| = \Omega(|H|)$ such that

$$(4.4.2) \text{ for each } \mathfrak{p} \in T_1, [\psi_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}] \text{ in } \mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \alpha}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G),$$

$$(4.4.3) \text{ the solution field } N \text{ (fixed field of } \text{Ker}(\psi)) \text{ satisfies } \text{Ram}(N/K_0) \subseteq T_1 \cup R$$

Proof of (a). Since $T \subset T_1$, (a) follows from (4.4.2).

Proof of (b). For each $\mathfrak{p} \in S$, by (4.4.2), $[\psi_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$. Since $\varphi_{\mathfrak{p}}$ is the trivial homomorphism, so is $\psi_{\mathfrak{p}}$. It follows that each $\mathfrak{p} \in S$ totally splits in N . Thus $N \subseteq K_{0, \text{tot}, S}$.

Proof of (c). By (a), each prime $\mathfrak{p} \in S$ totally splits in N . Since $T_1 = T \cup S$, it follows from (4.4.3) that $\text{Ram}(N/K_0) \subseteq T \cup R$. \square

An immediate consequence of Theorem 4.4.1 is that every solvable group whose order is prime to $|\mu(K_0)|$ can be realized over K_0 in $K_{0, \text{tot}, S}$ with bounded ramification.

Corollary 4.4.2. Let K_0 be a number field and let S be a finite set of primes of K_0 . Let G be a finite solvable group with $\gcd(|G|, |\mu(K_0)|) = 1$. Then, there exists a Galois extension N/K_0 with $N \subseteq K_{0, \text{tot}, S}$ and $\text{Gal}(N/K_0) \cong G$ such that $|\text{Ram}(N/K_0)| \leq \Omega(|G|)$.

Proof. We set $\Gamma = 1$ the trivial group, and we consider the following embedding problem:

$$\begin{array}{ccccccc} & & & & \text{Gal}(K_0) & & \\ & & & & \downarrow \rho & & \\ 1 & \longrightarrow & G & \longrightarrow & G & \xrightarrow{\alpha} & \Gamma & \longrightarrow & 1 . \end{array}$$

with α the trivial epimorphism. Then, for each prime $\mathfrak{p} \in \mathbb{P}(K_0)$, the class of the trivial homomorphism $\varphi_{\mathfrak{p}}: \text{Gal}(\hat{K}_{0, \mathfrak{p}}) \rightarrow G$ is an element of

$\mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \alpha}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G)$, so

$$\prod_{\mathfrak{p}} \mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \alpha}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G) \neq \emptyset.$$

Considering $K = K_0$, $T = \{\mathfrak{p}\}$ for some $\mathfrak{p} \in \mathbb{P}(K_0)$, and $[\varphi_{\mathfrak{p}}] \in \mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \alpha}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G)$ the class of the trivial homomorphism, by Theorem 4.4.1, there exists a Galois extension N/K_0 with $N \subseteq K_{0, \text{tot}, S}$ such that $\text{Gal}(N/K_0) \cong G$ and $|\text{Ram}(N/K_0)| \leq \Omega(|G|)$. \square

The next application of Theorem 4.4.1 says that if embedding problem (4.4.1) has a solution in $K_{0, \text{tot}, S}$, then it has a proper solution in $K_{0, \text{tot}, S}$ with bounded ramification.

Corollary 4.4.3. Let K/K_0 be a finite Galois extension of number fields and let S be a finite set of primes of K_0 . Suppose $K \subset K_{0, \text{tot}, S}$. Consider the embedding problem (4.4.1) with a solvable kernel H , where $\Gamma = \text{Gal}(K/K_0)$ and ρ being the restriction map. Suppose $\gcd(|H|, |\mu(K)|) = 1$. If the embedding problem (4.4.1) has a solution ψ_0 (homomorphism) in $K_{0, \text{tot}, S}$ then it has a proper solution ψ (epimorphism) in $K_{0, \text{tot}, S}$ with $|\text{Ram}(\psi)| \leq |\text{Ram}(K/K_0)| + \Omega(|H|)$.

Proof. For each $\mathfrak{p} \in \mathbb{P}(K_0)$ the local restriction $\psi_{0, \mathfrak{p}}: \text{Gal}(\hat{K}_{0, \mathfrak{p}}) \rightarrow G$ is a solution of the corresponding local embedding problem. It follows that $\prod_{\mathfrak{p}} \mathcal{H}\text{om}_{\Gamma, \rho_{\mathfrak{p}}, \alpha}(\text{Gal}(\hat{K}_{0, \mathfrak{p}}), G) \neq \emptyset$. Therefore, by Theorem 4.4.1, considering $T = \text{Ram}(K/K_0)$, there exists a proper solution (epimorphism) $\psi: \text{Gal}(K_0) \rightarrow G$ in $K_{0, \text{tot}, S}$ with $|\text{Ram}(\psi)| \leq |\text{Ram}(K/K_0)| + \Omega(|H|)$. \square

Always assuming that $K \subset K_{0, \text{tot}, S}$, Corollary 4.4.3 implies that if the embedding problem (4.4.1) splits, i.e. α has a section, then it has a proper solution in $K_{0, \text{tot}, S}$ with bounded ramification.

Corollary 4.4.4. Let K/K_0 be a finite Galois extension of number fields and let S be a finite set of primes of K_0 . Suppose $K \subset K_{0, \text{tot}, S}$. Consider embedding problem (4.4.1) with a solvable kernel H , where $\Gamma = \text{Gal}(K/K_0)$

and ρ being the restriction map. Suppose $\gcd(|H|, |\mu(K)|) = 1$ and the epimorphism α splits. Then the embedding problem (4.4.1) has a proper solution ψ in $K_{0,\text{tot},S}$ with $|\text{Ram}(\psi)| \leq |\text{Ram}(K/K_0)| + \Omega(|H|)$.

Proof. Let $s: \Gamma \rightarrow G$ be a section of α , i.e. $\alpha \circ s = \text{id}_\Gamma$. Then, the homomorphism $\psi_0 = s \circ \rho: \text{Gal}(K_0) \rightarrow G$ is a solution of (4.4.1) in $K_{0,\text{tot},S}$. Therefore, our corollary is a special case of Corollary 4.4.3. \square

Bibliography

- [CaF67] J. W. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London (1967).
- [FrJ08] M. D. Fried and M. Jarden, *Field Arithmetic*, third edition, revised by M. Jarden, *Ergebnisse der Mathematik (3)* **11**, Springer, Heidelberg (2008).
- [GeJ98] W. Geyer and M. Jarden, *Bounded realization of l -groups over global fields*, *Nagoya Mathematical Journal* **150** (1998), pp. 13-62.
- [HaW62] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Fourth Edition, Oxford (1962)
- [Jan73] G. Janusz, *Algebraic Number Fields*, Academic Press, New York (1973).
- [Jar91] M. Jarden, *Intersection of local algebraic extensions of a Hilbertian field*, *NATO ASI Series C* **333** (1991), 343-405.
- [Lan70] S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading (1970).
- [Lan93] S. Lang, *Algebra*, third edition, Addison-Wesley, Reading (1993).
- [MaU11] N. Markin and S.-V. Ullom, *Minimal ramification in nilpotent extensions*, *Pacific Journal of Mathematics* **253** (2011), No. 1, pp. 125-143.

- [Neu79] J. Neukirch, *On solvable number fields*, *Inventiones mathematicae* **53** (1979), pp. 135-164.
- [Neu99] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Heidelberg (1999).
- [NSW00] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, *Grundlehren der mathematischen Wissenschaften* **323**, Springer-Verlag, Heidelberg (2000).
- [Rami13] C. Ramiharimanana, *Realization of finite groups as Galois groups over \mathbb{Q} in $\mathbb{Q}_{\text{tot},p}$* , Master Thesis, Stellenbosch University (2013).
- [Rei37] H. Reichardt, *Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung*, *Journal für die reine und angewandte Mathematik* **177** (1937), pp. 1-6.
- [Rib70] L. Ribes, *Introduction to Profinite Groups and Galois Cohomology*, *Queen's papers in Pure and Applied Mathematics* **24**, Queen's University, Kingston (1970).
- [Sch37] A. Scholz, *Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I.*, *Mathematische Zeitschrift* **42** (1937), pp. 161-188.
- [Se92] J.-P. Serre, *Topics in Galois Theory*, Jones and Barlett, Boston (1992).
- [Se79] J.-P. Serre, *Local Fields*, Springer-Verlag, New York (1979), Translation from French by M. J. Greenberg.
- [Sha54] I. R. Shafarevich, *On the construction of fields with a given Galois group of order l^a* , *Izv. Akad. Nauk* **18** (1954), pp. 261-296. In Russian. *AMS Translations, Ser. 2*, **4** (1956), pp. 107-142.
- [Sha89] I. R. Shafarevich, *Factors of descending central series*, *Mathematical Notes* **45** (1989), pp. 262-264.