THE UNIVERSITY OF CHICAGO

CONSTRUCTING MAXIMAL UNRAMIFIED EXTENSIONS AND MURPHY'S LAW FOR GALOIS DEFORMATION RINGS

A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

BY
ANDREEA IORGA

CHICAGO, ILLINOIS
JUNE 2024

Părinților mei, Denisa și Dumitru, și fratelui meu, Alex.

TABLE OF CONTENTS

ACKNOWLEDGMENTS v

ABSTRACT vii

1 INTRODUCTION 1
- 1.1 Main Results 2
- 1.2 Overview of the Argument 5
- 1.3 Conditionality and Further Work 8
- 1.4 Outline of the Thesis 8

2 BACKGROUND 10
- 2.1 Background on Modular Representations 10
- 2.2 Embedding Problem 12
- 2.3 Some technical lemmas 17
- 2.4 Background on universal unramified deformations 20

3 CONSTRUCTING MAXIMAL UNRAMIFIED EXTENSIONS 23
- 3.1 Proof of Theorem 3.0.1 25
- 3.2 Proof of Theorem 3.0.2 34

4 UNIVERSAL UNRAMIFIED DEFORMATION RINGS 51
- 4.1 Finding the Universal Unramified Deformation Ring 52
- 4.2 Existence of Residual Representations 57
- 4.3 Murphy's Law for Galois Deformation Rings 60

REFERENCES 61

ACKNOWLEDGMENTS

I would like to express my gratitude to my advisor, Frank Calegari, who introduced me to this research area and suggested the problem that became the focus of this thesis. I want to thank Frank for his patience, support and guidance throughout this process. I am grateful for everything he has taught me and for the freedom he has given me to pursue this project on my own terms and at my own pace.

I would like to thank Matt Emerton for acting as my secondary advisor and the second reader of this thesis. I would also like to thank Matt for his guidance and fruitful discussions during the application process.

I would like to thank Ravi Ramakrishna for reading a first draft of the paper that this thesis is based on and for his insightful comments. I am incredibly grateful for his availability and support over the last two years.

I want to thank my colleagues and friends at the University of Chicago for all the mathematical discussions, emotional support and general life and career advice: Chengyang, Jason, Mathilde, Nikiforos, Sam, Stephen and many others.

I am grateful to my middle school and high school math teachers, Dobrița Ilie and Iuliana Turcu, who have always encouraged me to follow my passion. I am also thankful for Glenn Stevens and the PROMYS program, which introduced me to number theory as a high school student. I would like to thank the professors I met as an undergraduate student at Oxford. I am particularly grateful to Minhyong Kim, who supervised my first research project and has always supported me in my mathematical career.

I would like to thank all my friends and family outside of Chicago who have been there for me throughout this journey. I am particularly grateful to Andreea, Eliza, Maria and Radhica for their support and encouragement, and for providing much-needed distractions. I would like to thank Maria for being my best friend for so many years and for being an important source of emotional support during challenging times.

I would like to thank Sam for his unwavering support, both mathematical and emotional. His encouragement and belief in me, even when I struggled to believe in myself, provided me with the strength to keep going. I am also grateful for all his useful comments, for his patience in reading countless drafts of my paper and for listening to my practice talks numerous times. Thank you for being such a significant part of this process.

Finally, I owe the greatest amount of gratitude to my family, for everything they have done for me. I would like to thank my parents, Denisa and Dumitru, for teaching me how to count and for helping me solve my first math problem (and many more after that) back in first grade. I am deeply thankful for their love, encouragement, support and faith in me. I would also like to thank my brother, Alex, for being the best sibling in the world. His belief in me has always been a source of strength, and his own achievements have inspired me to strive for more. Alex, mami, tati, vă mulțumesc pentru tot. Nu aș fi fost aici fără voi.

ABSTRACT

The structure of the $\mathrm{Gal}(L^{\mathrm{ur}}/L)$, the Galois group of the maximal unramified extension of a number field L, has been an object of interest for more than a century now. This thesis is partially motivated by the question of which finite groups can appear as quotients of $\mathrm{Gal}(L^{\mathrm{ur}}/L)$. We prove, under a technical assumption, that any semi-direct product of a p-group G with a group Φ of order prime to p can appear as the Galois group of a tower of extensions $M/L/K$ with the property that M is the maximal p-extension of L that is unramified everywhere, and $\mathrm{Gal}(M/L) = G$. A consequence of this result is that any local ring admitting a surjection to $\mathbb{Z}_5$ or $\mathbb{Z}_7$ with finite kernel can occur as a universal everywhere unramified deformation ring.

CHAPTER 1

INTRODUCTION

Let p be a prime, let L be a number field, and let L^{ur} be the maximal unramified extension of L. The structure of $\mathrm{Gal}(L^{\mathrm{ur}}/L)$ has been studied extensively by numerous mathematicians since the late 19th century. In 1964, Golod and Shafarevich [GS64] solved the long-standing class field tower problem by proving that the group $\mathrm{Gal}(L^{\mathrm{ur}}/L)$ can be infinite. This thesis is partially motivated by the question of which finite groups can occur as $\mathrm{Gal}(L^{\mathrm{ur}}/L)$. In this direction, Manabu Ozaki proved in [Oza11] that any p-group can be written as the Galois group of $L^{\mathrm{ur},p}/L$, for some totally complex number field L. Here $L^{\mathrm{ur},p}$ is the maximal unramified p-extension of L. A recent paper of Hajir, Maire and Ramakrishna [HMR24a] provides two extensions to Ozaki's result: the base field can have arbitrary signature, as long as its class number is prime to p, and the degree of the new field over $\mathbb{Q}$ can be controlled. In this thesis, we prove a different generalisation in the case of regular primes. This thesis is based on the author's preprint [Ior23].

Note that Ozaki's Theorem does not yield any information on the structure of the number field L. In particular, this number field need not be Galois over $\mathbb{Q}$. As such, it is natural to ask what p-groups G occur as Galois groups of maximal unramified p-extensions of number fields L, as one varies over Φ-extensions L (number fields L that are Galois over $\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) = \Phi$, for a fixed group Φ).

If we fix a Φ-extension L, we observe that $L^{\mathrm{ur},p}/\mathbb{Q}$ has to be Galois. If, for example, we consider odd primes p and $\mathbb{Z}/2\mathbb{Z}$-extensions L, then the Galois group of $L^{\mathrm{ur},p}/\mathbb{Q}$ will be a semidirect product. Therefore, one might ask the following question, which this thesis addresses:

Question 1. Fix a group Φ of order prime to p and let G be a p-group with an action of Φ. Let $\Gamma = G \rtimes \Phi$. Does there exist an extension L/K such that $\mathrm{Gal}(L^{\mathrm{ur},p}/K) = \Gamma$ and $\mathrm{Gal}(L^{\mathrm{ur},p}/L) = G$?

There is another motivating question for this thesis, coming from the field of Galois deformations. The topic of deformations of Galois representations was introduced by Barry Mazur in [Maz89] and represents an important tool in Wiles's work on the modularity conjecture and Fermat's Last Theorem. Let $\overline{\rho}\colon G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ be an absolutely irreducible residual representation, where K is a number field. If we consider the unramified lifts of this representation, a natural question that arises is the following:

Question 2. What possible rings R can occur as universal unramified deformation rings of such $\overline{\rho}$?

An unramified deformation $\rho\colon G_K \to GL_2(R)$ factors through some finite group, so we can consider the fixed field of the kernel of this map; denote it by $K(\rho)$. The extension $K(\rho)/K(\overline{\rho})$ is a finite p-extension that is unramified everywhere, so its Galois group is a quotient of the Galois group of the maximal pro-p extension of $K(\overline{\rho})$ unramified everywhere. We observe that Ozaki's Theorem provides help in answering a variant of Question 2 if we allow $\overline{\rho}\colon G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ to be trivial and R to be a universal unramified pseudodeformation ring. Therefore, in order to answer the actual question, we need an extension of Ozaki's Theorem that allows us to deal with absolutely irreducible residual representations. In particular, for representations $\overline{\rho}$ with image of order prime to p, the natural step is to consider an extension of Ozaki's Theorem for semidirect products.

1.1 Main Results

In this section, we present the statements of the main results. As previously mentioned, Ozaki's Theorem ([Oza11, Theorem 1]) states that any p-group can be written as the Galois group of $L^{\mathrm{ur},p}/L$, for some totally complex number field L. In this thesis, we prove the following:

Theorem 1. *Let p be a prime. Let Φ be a group of order prime to p. Assume there exists an extension of number fields F/E such that:*

- *F/E is Galois with Galois group Φ, and $[E\colon \mathbb{Q}] \geq 2d(\Phi)$, where $d(\Phi)$ is the number of generators of the group Φ,*
- *F has class number prime to p,*
- *The prime p splits completely in F/E and F/E satisfies property **P** below,*
- *E contains μ_p, and is totally imaginary if $p = 2$.*

Then, for any p-group G with an action of Φ, there exist extensions of number fields $M/L/K$ such that:

1. *M/L is the maximal p-extension of L that is unramified everywhere,*
2. *$\mathrm{Gal}(M/L) = G$,*
3. *$\mathrm{Gal}(M/K) = \Gamma$, where $\Gamma = G \rtimes \Phi$,*
4. *M/K satisfies property **P** below.*

Definition 1.1.1. We say that an extension of number fields M/K has property **P** if for all primes $\mathfrak{p}$ of K, and $\mathfrak{P} \mid \mathfrak{p}$, either $M_{\mathfrak{P}}/K_{\mathfrak{p}}$ is unramified or $M_{\mathfrak{P}}/K_{\mathfrak{p}}$ is a cyclic tamely ramified extension with ramification index e and $e \mid (q-1)$, where q is the cardinality of the residue field of $K_{\mathfrak{p}}$.

At first, Property **P** might seem very strong. However, this is not the case. To illustrate what this condition means, let M/K be an extension, let $\mathfrak{p}$ be any prime of K and let $\mathfrak{P}$ be a prime of M lying above $\mathfrak{p}$. Consider the following examples:

- If M/K is a $\mathbb{Z}/2\mathbb{Z}$-extension that is only ramified at primes $\mathfrak{p}$ lying above odd rational primes, then M/K satisfies property **P**. Note that this holds for all tamely ramified $\mathbb{Z}/2\mathbb{Z}$-extensions.

- If M/K is a $\mathbb{Z}/3\mathbb{Z}$-extension that is only ramified at primes $\mathfrak{p}$ such that $N(\mathfrak{p}) \equiv 1 \pmod 3$, then M/K satisfies property **P**. Note that this is true for all tamely ramified $\mathbb{Z}/3\mathbb{Z}$-extensions.

- If M/K is an extension such that $M_{\mathfrak{P}}/K_{\mathfrak{p}}$ is either unramified or totally tamely ramified, then M/K satisfies property **P**.

When Φ is trivial, we can recover Ozaki's result from Theorem 1 in the case when p is a prime such that $\mathbb{Q}(\zeta_p)$ has a finite extension with class number prime to p (note that this includes all regular primes); a similar hypothesis is present in the first version (arXiv:0705.2293) of Ozaki's paper [Oza11].

A motivating example and a consequence of Theorem 1 is Theorem 2 below. Consider a continuous absolutely irreducible residual Galois representation $\overline{\rho}\colon G_K \to \mathrm{GL}_2(\mathbb{F}_p)$. One can associate to $\overline{\rho}$ a number of deformation rings. Let A be a local Artinian ring and consider a deformation $\rho\colon G_K \to \mathrm{GL}_2(A)$ of $\overline{\rho}$. This deformation factors through some finite group, and the fixed field of the kernel is a finite extension; call it $K(\rho)$. We say that ρ is unramified if the extension $K(\rho)/K(\overline{\rho})$ is unramified everywhere. The functor which sends local Artinian rings A to unramified deformations $D(A)$ is pro-representable by a universal deformation ring. Therefore, it is natural to seek for an answer to Question 2.

Assume that the image of $\overline{\rho}$ has order prime to p, so its projective image is $\Phi = A_4,\ S_4,\ A_5$ or a dihedral group by [Ser72, Proposition 16]. The Unramified Fontaine-Mazur Conjecture ([FM95, Conjecture 5a]) predicts that all $\overline{\mathbb{Q}}_p$-points will have finite image. Moreover, the tangent space to any $\overline{\mathbb{Q}}_p$-point with finite image will be trivial by class field theory (proof of [AC14, Proposition 10]), and thus conjecturally such a ring has a unique map to $\overline{\mathbb{Q}}_p$. The expectation is then that R is a ring admitting a map $R \twoheadrightarrow \mathbb{Z}_p$ with finite kernel I. In this thesis, we prove the following:

Theorem 2. *Let R be any local ring admitting a surjection to $\mathbb{Z}_5$ or to $\mathbb{Z}_7$ with finite kernel. Then there exists an absolutely irreducible residual representation $\overline{\rho}$ such that R is isomorphic to the universal unramified deformation ring of $\overline{\rho}$.*

1.2 Overview of the Argument

The proof is done by induction (with the assumption of Theorem 1 acting as the base case), as follows: since G is a p-group with an action of Φ, the group Φ must preserve the p-torsion of the centre of G, and thus any such G will fit into an exact sequence of p-groups

$$1 \to V \to G' \to G \to 1,$$

where V is a group of exponent p on which Φ acts by an irreducible representation. Thus, our semidirect product Γ fits into an exact sequence

$$1 \to V \to \Gamma' \to \Gamma \to 1. \tag{1.1}$$

We construct the desired extensions inductively, combining Kummer extensions with carefully chosen solutions to the embedding problem. The inductive step is divided into two cases, depending on whether this short exact sequence splits or not. An outline of the proof for the split case is presented below; when the sequence is not split, the proof requires an extra step that involves constructing a wildly ramified solution to the embedding problem.

The proof is inspired by Ozaki's methods and techniques [Oza11]. In order to make certain intermediate extensions more explicit, we also build on some ideas present in an earlier preprint of Ozaki. While some elements of Ozaki's proof can be modified to work in our situation, there are several key steps which do not work. There are multiple reasons why these arguments cannot be replicated in our situation, including the following:

- The dimension of V can be greater than 1, which could potentially lead to having an unramified, but not maximal, extension;

- Instead of working with p-groups alone, we are now working with p-groups with an action of Φ.

The inductive step is represented by Theorem 3.0.2. This Theorem takes a Galois extension L/K with Galois group Φ such that $\mathrm{Gal}(L^{\mathrm{ur},p}/K) \cong \Gamma = G \rtimes \Phi$ and $L^{\mathrm{ur},p}/K$ satisfies certain properties, and constructs a new extension L'/K' such that $\mathrm{Gal}(L'/K') \cong \Phi$ and $\mathrm{Gal}((L')^{\mathrm{ur},p}/K') \cong \Gamma' = G' \rtimes \Phi$. When the above short exact sequence splits, the structure of the argument is as follows:

1. Construct a very large number of carefully chosen primes $\lambda_i \mathcal{O}_L$. The number of primes depends on p and $n = \dim_{\mathbb{F}_p} V$. In order to make sure that such a construction is possible, the base field K needs to be large enough over $\mathbb{Q}$ (in other words, K must have enough Minkowski units). This is not a priori true, but we can ensure this by performing a series of base changes that increase the degree of K over $\mathbb{Q}$, but preserve all the other properties (and thus avoid the obstructions imposed by the Golod-Shafarevich towers). This is done in Theorem 3.0.1, whose proof is presented in Section 3.1. The proof relies on the theory of modular representations of $\mathbb{F}_p[\Gamma]$.

2. Consider the decomposition of the $\mathbb{F}_p[\Phi]$-module $L^\times/L^{\times p}$ into a direct sum of isotypic components. Construct two more primes $\alpha\mathcal{O}_L$ and $\beta\mathcal{O}_L$ that satisfy certain congruence conditions modulo $\lambda_i\mathcal{O}_L$ and have specific forms in the different isotypic components of $L^\times/L^{\times p}$.

3. Use Kummer Theory to construct two extensions of L that are Galois over K with Galois groups isomorphic to $V \rtimes \Phi$ satisfying certain ramification conditions at the primes $\alpha\mathcal{O}_L, \beta\mathcal{O}_L, \lambda_i\mathcal{O}_L$. Now, consider the compositum of these two extensions with

the field $L^{\mathrm{ur},p}$; call this $\tilde{M}$. The extension $\tilde{M}/L^{\mathrm{ur},p}$ satisfies certain maximality properties, so we can use a homological argument (Lemma 3.1.1) to prove that $\tilde{M}$ has class number prime to p.

4. Once again, use Kummer Theory to construct a subextension L' of $\tilde{M}/L$ that absorbs all the ramification. By construction, $\mathrm{Gal}(\tilde{M}/L') \cong G'$ and $(L')^{\mathrm{ur},p} = \tilde{M}$. Using the Schur-Zassenhaus Theorem, we are able to view $\Phi = \mathrm{Gal}(L/K)$ as a subgroup of $\mathrm{Gal}(L'/K) = V \rtimes \Phi$, so we construct $K' = L'^{\Phi}$, which finishes the proof when (1.1) splits.

5. As previously mentioned, when (1.1) does not split, the proof requires an extra step: the construction of a wildly ramified solution to the embedding problem. We now combine this solution with a split solution with certain properties to get the desired extension.

Theorem 2 can be reduced to Theorem 1 as follows. Recall that R is a local ring that surjects onto $\mathbb{Z}_p$ with finite kernel (note that we do not need $p = 5$ or $p = 7$ for now). Suppose we can find an absolutely irreducible representation $\overline{\rho}\colon G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ with image Φ of order prime to p. This lifts to a representation $\Phi \subset \mathrm{GL}_2(\mathbb{Z}_p)$; let Γ be the inverse image of Φ inside $\mathrm{GL}_2(R)$. There is a natural representation $\Gamma \to \mathrm{GL}_2(\mathbb{F}_p)$. A ring theoretic argument shows that R is the universal deformation ring of this representation. Moreover, if the lift to $\mathrm{GL}_2(R)$ is unramified, then R is the universal unramified deformation ring. Note that Γ will fit into an exact sequence of the form

$$1 \to G \to \Gamma \to \Phi \to 1,$$

where G is a p-group. Finding $\overline{\rho}$ with image Φ that has an unramified lift to $\mathrm{GL}_2(R)$ requires using Theorem 1. The proof does not rely on p until now, where we need to find extensions F/E satisfying the assumptions of Theorem 1. For $p = 5$ and $p = 7$, we find explicit

extensions using Pari. For $p > 7$, the difficulty comes from the fact that computational tools like Pari and MAGMA have limitations when computing class numbers of high degree fields. As mentioned in Chapter 4, we believe that Conjecture 1 holds, making this result true for all $p \geq 5$.

1.3 Conditionality and Further Work

As previously mentioned, the assumptions of Theorem 1 act as a base case for the inductive procedure. The ramification assumption (F/E satisfies property $\mathbf{P}$) ensures that the embedding problem is solvable (for more details, see Section 2.2). In practice, this does not add any difficulty to the construction. There is no hope of removing the first two conditions, as the theorem statement without these conditions would resemble a variant of the Inverse Galois Problem.

There is hope to remove the roots of unity assumption. This work is inspired by [HMR24a] and [HMR24b]. As previously noted, the proof of Theorem 1 presented in this thesis constructs certain Galois extensions using Kummer Theory. This is possible, since the base field contains p-th roots of unity. When removing the roots of unity assumption, the strategy is to construct these extensions using Galois cohomology and a modified version of the Gras-Munnier Theorem [GM99, Théorème 1.1].

As most of the proof of Theorem 2 does not depend on the precise value of p, establishing Theorem 1 true with the roots of unity assumption removed would lead to proving Theorem 2 for all primes $p \geq 5$.

1.4 Outline of the Thesis

In Chapter 2, we introduce some results which will be used in our arguments: some facts on modular representations (Section 2.1), on the embedding problem (Section 2.2), some

useful lemmas (Section 2.3), and a brief introduction to the theory of deformations of Galois representations (Section 2.4). Most of the results in this chapter are already known or can be deduced from known results. We collect them here to make later arguments easier to follow.

Chapter 3 presents the proof of Theorem 1. This is the most involved part of this thesis. The chapter starts by introducing two key results, Theorem 3.0.1 and Theorem 3.0.2, and showing how these two results combine to prove Theorem 1. The rest of the chapter presents the proof of these two results. Theorem 3.0.1 allows us to perform $\mathbb{Z}/p\mathbb{Z}$-base changes that increase the degree of the base field over $\mathbb{Q}$, but preserve all the other properties. The proof of this result relies on the theory of modular representations. In particular, it uses the key facts that $\mathbb{F}_p[\Phi]$ is semisimple and that the indecomposable projective $\mathbb{F}_p[\Gamma]$-modules are in a one-to-one correspondence with the simple $\mathbb{F}_p[\Phi]$-modules. Section 3.2 presents the proof of Theorem 3.0.2. The first part of this section is done under the assumption that (1.1) splits. After dropping this assumption, we construct a wildly ramified solution to the embedding problem (Proposition 3.2.2) and combine this solution with a split extension to get the desired extension.

Chapter 4 deals with the proof of Theorem 2. In the first section of the chapter, we start with a local ring admitting a surjection onto $\mathbb{Z}_p$ with finite kernel. Then we prove that if we have an absolutely irreducible residual representation with certain properties, the universal unramified deformation ring of that representation is isomorphic to the ring we started with. This proof does not depend on the prime p. In Section 4.2, we explain how the existence of such a representation reduces to having the assumptions of Theorem 1 satisfied. We then proceed to use GP/Pari to find extensions satisfying Theorem 1 for $p = 5$ and $p = 7$. Finally, in Section 4.3, we explain how Theorem 2 can be seen as an example of "Murphy's Law" for Galois deformation rings.

CHAPTER 2

BACKGROUND

2.1 Background on Modular Representations

In this section, we collect some results on modular representations that will be used later in the proof. Everything in this section is known and can be found in [Web16]. Throughout this section, let p be a prime, let Φ be a group of order prime to p, and let G be a p-group with an action of Φ. Let $\Gamma = G \rtimes \Phi$ be the semidirect product between G and Φ.

Firstly, we note that $\mathbb{F}_p[\Gamma]$ is a symmetric Frobenious algebra, so finitely generated projective $\mathbb{F}_p[\Gamma]$-modules are the same as finitely generated injective $\mathbb{F}_p[\Gamma]$-modules by [Web16, Corollary 8.5.3]. We have the following result:

Lemma 2.1.1. *The set of simple $\mathbb{F}_p[\Phi]$-modules are in a one-to-one correspondence with the set of indecomposable projective $\mathbb{F}_p[\Gamma]$-modules.*

Proof. Let S be a simple $\mathbb{F}_p[\Phi]$-module. By [Web16, Proposition 8.3.2(c)], we know that S can be viewed as a simple $\mathbb{F}_p[\Gamma]$-module via the quotient $\Gamma \to \Phi$. Construct the projective cover P_S of S. According to [Web16, Proposition 7.3.8], this is an indecomposable projective $\mathbb{F}_p[\Gamma]$-module and $P_S/\operatorname{Rad}(P_S) \cong S$, as $\mathbb{F}_p[\Gamma]$-modules. Here $\operatorname{Rad}(P_S)$ is the radical of P_S. Thus, the simple $\mathbb{F}_p[\Phi]$-modules are in a one-to-one correspondence with the indecomposable projective $\mathbb{F}_p[\Gamma]$-modules. □

Now, we say that a finitely generated module M over a ring R is stably free if there exists some integer $m \geq 0$ such that $M \oplus R^m$ is a free R-module. Such a module is projective. Moreover, if $m = 0$, then M is a free module. We note that if $R = \mathbb{F}_p[\Gamma]$, then any stably free $\mathbb{F}_p[\Gamma]$-module is actually free. This follows from the fact that $\mathbb{F}_p[\Gamma]$ is a semilocal ring and [Lam06, Example I.4.7(3)].

For the remainder of this section, let M, N and P be $\mathbb{F}_p[\Gamma]$-modules. We say that a monomorphism $f\colon M \to N$ of $\mathbb{F}_p[\Gamma]$-modules is essential if whenever $g\colon N \to P$ is a map such that $g \circ f$ is a monomorphism, then g is also a monomorphism. Following the notation in [Web16], we define the injective hull of an $\mathbb{F}_p[\Gamma]$-module M to be an essential monomorphism $M \to I$, where I is an injective module. By [Web16, Section 8.5], we know that injective hulls always exist and are unique. Since I is an injective $\mathbb{F}_p[\Gamma]$-module, it is also a projective $\mathbb{F}_p[\Gamma]$-module, so it can be written as a direct sum of indecomposable projective modules.

For an $\mathbb{F}_p[\Gamma]$-module M, we define the socle of M, denoted by $\mathrm{Soc}(M)$, to be the largest semisimple submodule of M. Of course, $\mathrm{Soc}(M) \subset M$. We have the following result:

Lemma 2.1.2. *Let M be an $\mathbb{F}_p[\Gamma]$-module.*

(i) If N is the injective hull of M, then $\mathrm{Soc}(M) \cong \mathrm{Soc}(N)$.

(ii) If P is a submodule of M, then $\mathrm{Soc}(P) = P \cap \mathrm{Soc}(M)$.

Proof. (i) Firstly, if S is a simple submodule of M, then S is also a simple submodule of N, so $\mathrm{Soc}(M) \subset \mathrm{Soc}(N)$. Conversely, if S is a nonzero simple submodule of N, then $S \cap M = 0$ or $S \cap M = S$. If $S \cap M = 0$, then the map $M \to N \to N/S$ is injective, so by the fact that the map $M \to N$ is an essential monomorphism, we obtain that the map $N \to N/S$ must be injective. But this is true if and only if $S = 0$, which is a contradiction. It follows that $S = S \cap M \subset M$, so $\mathrm{Soc}(N) \subset \mathrm{Soc}(M)$. We conclude that $\mathrm{Soc}(M) \cong \mathrm{Soc}(N)$.

(ii) On the one hand, if S is a simple submodule of P, then S is also a simple submodule of M, so $\mathrm{Soc}(P) \subset P \cap \mathrm{Soc}(M)$. On the other hand, if S is a simple submodule of M such that $S \in P \cap \mathrm{Soc}(M)$, then S is a submodule of P; thus, since S is simple, $S \in \mathrm{Soc}(P)$. We conclude that $\mathrm{Soc}(P) = P \cap \mathrm{Soc}(M)$.

□

2.2 Embedding Problem

In this section we introduce some results on the embedding problem, which will be instrumental in proving Theorem 3.0.2. A detailed exposition of this can be found in [Neu73]. Following the presentation of these already known results, we proceed to explain how they apply in our specific scenario.

Let F be a number field and let G_F be the absolute Galois group of F. Let K/F be a finite Galois extension with Galois group G. For an extension of finite groups $(\varepsilon)\colon 1 \to A \to E \to G \to 1$, the embedding problem (G_F, ε) is defined by the diagram

$$\begin{array}{ccccccccc} & & & & & & G_F & & \\ & & & & & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{\pi} & G & \longrightarrow & 1, \end{array}$$

where φ is the canonical surjection. A continuous homomorphism $\psi\colon G_F \to E$ is called a solution of (G_F, ε) if it satisfies the condition $\pi \circ \psi = \varphi$. A solution ψ is called a proper solution if it is surjective. If (ε) is a nonsplit extension, then every solution of the embedding problem is a proper solution ([Hoe68, Satz 2.3]). In this thesis, we will only construct solutions to the embedding problem when the extension is nonsplit, so we can assume that if an embedding problem has a solution, then that solution is proper. This translates to finding an extension M/F containing K/F such that $\mathrm{Gal}(M/F) \cong E$ compatibly with $\mathrm{Gal}(K/F) = G$. When such a solution exists, we say that (G_F, ε) is solvable.

For each prime $\mathfrak{p}$ of F, we denote by $F_\mathfrak{p}$ (respectively $K_\mathfrak{p}$) the completion of F at $\mathfrak{p}$ (respectively of K at a prime above $\mathfrak{p}$). Let $G_{F_\mathfrak{p}}$ be the absolute Galois group of $F_\mathfrak{p}$, $G_\mathfrak{p} = \varphi(G_{F_\mathfrak{p}}) \subset G$ (which is isomorphic to the decomposition subgroup of $\mathfrak{p}$ in $\mathrm{Gal}(K/F)$) and $E_\mathfrak{p} = \pi^{-1}(G_\mathfrak{p}) \subset E$. Then the local embedding problem $(G_{F_\mathfrak{p}}, \varepsilon_\mathfrak{p})$ is defined by

$$\begin{array}{ccccccccc} & & & & & & G_{F_\mathfrak{p}} & & \\ & & & & & & \downarrow{\scriptstyle \varphi_\mathfrak{p}} & & \\ 1 & \longrightarrow & A & \longrightarrow & E_\mathfrak{p} & \xrightarrow{\pi_\mathfrak{p}} & G_\mathfrak{p} & \longrightarrow & 1. \end{array}$$

We have the following results from [Neu73] (Satz 2.2, Satz 4.7, Satz 5.1).

Theorem 2.2.1 (Neukirch)**.** *Let (G_F, ε) be an embedding problem with abelian kernel A. If the map*

$$H^2(G_F, A) \to \prod_{\mathfrak{p} \in P} H^2(G_{F_\mathfrak{p}}, A)$$

is injective, then the embedding problem (G_F, ε) has a solution if and only if the local embedding problems $(G_{F_\mathfrak{p}}, \varepsilon_\mathfrak{p})$ have solutions, for all $\mathfrak{p} \in P$. Here P is the set of primes of F.

Theorem 2.2.2 (Neukirch)**.** *If A is a trivial finite G-module (i.e. $A = \mathbb{Z}/n\mathbb{Z}$) or A is the dual of one (i.e. $A = \mu_n$), then all maps*

$$H^q(F, A) \to \prod_{\mathfrak{p}} H^q(F_\mathfrak{p}, A), \quad q \geq 0,$$

are injective. Here we have $H^q(F, A) = H^q(G_F, A)$.

Theorem 2.2.3 (Neukirch)**.** *If $K_\mathfrak{p}/F_\mathfrak{p}$ is a cyclic extension of local fields, then the following conditions are equivalent:*

(i) Every embedding problem corresponding to the extension $K_\mathfrak{p}/F_\mathfrak{p}$ with an arbitrary (not necessarily abelian) kernel A of exponent n is solvable.

(ii) Every n-th root of unity in $F_\mathfrak{p}$ is the norm of an element of $K_\mathfrak{p}$.

This is always true if $K_\mathfrak{p}/F_\mathfrak{p}$ is unramified.

If $K_\mathfrak{p}/F_\mathfrak{p}$ is tamely ramified with ramification index e, then (i) and (ii) are true if and only if $n'e \mid (q-1)$, where $n' = \prod_{p \mid e} p^{v_p(n)}$ and q is the number of elements of the residue field of $F_\mathfrak{p}$.

We now return to our setting. Let p be a prime, let Φ be a group of order prime to p, and let G be a p-group with an action of Φ. Assume that there exists an extension of number fields L/K with Galois group Φ such that $\mathrm{Gal}(L^{\mathrm{ur},p}/K) \cong G \rtimes \Phi$ and L/K satisfies Property **P**. We claim that $L^{\mathrm{ur},p}/K$ also satisfies Property **P**:

Lemma 2.2.4. *Let L/K be a Galois extension with Galois group Φ as above and assume that L/K satisfies property **P**. Then $L^{ur,p}/K$ also satisfies property **P**.*

Proof. Let $\mathfrak{p}$ be a prime of K, and let $\mathfrak{q}$ and $\mathfrak{r}$, respectively, be primes of L and $L^{\mathrm{ur},p}$, respectively, lying over $\mathfrak{p}$. Let $K_{\mathfrak{p}}$, $L_{\mathfrak{q}}$, and $(L^{\mathrm{ur},p})_{\mathfrak{r}}$ be the corresponding completions. Let e be the ramification index of $\mathfrak{p}$ in $L^{\mathrm{ur},p}/K$. Note that, since $L^{\mathrm{ur},p}/L$ is unramified, e is also equal to the ramification index of $\mathfrak{p}$ in L/K. Since L/K satisfies property **P**, it follows that either $L_{\mathfrak{q}}/K_{\mathfrak{p}}$ is unramified or $L_{\mathfrak{q}}/K_{\mathfrak{p}}$ is tamely ramified with $e \mid (q-1)$, where q is the cardinality of the residue field of $K_{\mathfrak{p}}$. This immediately implies that $(L^{\mathrm{ur},p})_{\mathfrak{r}}/K_{\mathfrak{p}}$ is either unramified or is tamely ramified with $e \mid (q-1)$.

It remains to show that $(L^{\mathrm{ur},p})_{\mathfrak{r}}/K_{\mathfrak{p}}$ is cyclic. If $(L^{\mathrm{ur},p})_{\mathfrak{r}}/K_{\mathfrak{p}}$ is unramified, there is nothing to prove, so assume that it is tamely ramified. Let f_1 be the inertia index of $\mathfrak{p}$ in L/K, and let f_2 be the inertia index of $\mathfrak{q}$ in $L^{\mathrm{ur},p}/L$. Then $f = f_1 f_2$ is equal to the inertia index of $\mathfrak{p}$ in $L^{\mathrm{ur},p}/K$. Consider the extension $(L^{\mathrm{ur},p})_{\mathfrak{r}}/K_{\mathfrak{p}}$. By construction, we have the following short exact sequence

$$1 \to \mathrm{Gal}((L^{\mathrm{ur},p})_{\mathfrak{r}}/L_{\mathfrak{q}}) \to \mathrm{Gal}((L^{\mathrm{ur},p})_{\mathfrak{r}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) \to 1,$$

where $\mathrm{Gal}((L^{\mathrm{ur},p})_{\mathfrak{r}}/L_{\mathfrak{q}}) \cong \mathbb{Z}/f_2\mathbb{Z}$, $\mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) \cong \mathbb{Z}/(ef_1)\mathbb{Z}$, and $\mathrm{Gal}((L^{\mathrm{ur},p})_{\mathfrak{r}}/K_{\mathfrak{p}}) \cong \mathbb{Z}/f_2\mathbb{Z} \rtimes \mathbb{Z}/(ef_1)\mathbb{Z}$. The first equality follows from the fact that $(L^{\mathrm{ur},p})_{\mathfrak{r}}/L_{\mathfrak{q}}$ is unramified, the second from the fact that $L_{\mathfrak{q}}/K_{\mathfrak{p}}$ is cyclic, and the third from the Schur-Zassenhaus Theorem (since ef_1 and f_2 are coprime).

Now, let L_1 be the fixed field of inertia inside $(L^{\mathrm{ur},p})_{\mathfrak{r}}/K_{\mathfrak{p}}$. Note that the extension $L_1/K_{\mathfrak{p}}$

is cyclic of degree $f = f_1 f_2$. Since $(f_1, f_2) = 1$, it follows that there exists a subextension K_1 of $L_1/K_\mathfrak{p}$ such that we have the following tower:

$$\begin{array}{c} (L^{\mathrm{ur},p})_\mathfrak{r} \\ \Big| \mathbb{Z}/e\mathbb{Z} \\ L_1 \\ \Big| \mathbb{Z}/f_1\mathbb{Z} \\ K_1 \\ \Big| \mathbb{Z}/f_2\mathbb{Z} \\ K_\mathfrak{p} \end{array}$$

Consider the compositum of K_1 with $L_\mathfrak{q}$. Naturally, $K_1.L_\mathfrak{q} \subset (L^{\mathrm{ur},p})_\mathfrak{r}$, so $[K_1.L_\mathfrak{q} \colon K_\mathfrak{p}] \leq [(L^{\mathrm{ur},p})_\mathfrak{r} \colon K_\mathfrak{p}]$. Since $K_1/K_\mathfrak{p}$ is a p-extension and $L_\mathfrak{q}/K_\mathfrak{p}$ is an extension of order prime to p, we must have that $K_1 \cap L_\mathfrak{q} = K_\mathfrak{p}$. Thus, $[K_1.L_\mathfrak{q} \colon K_\mathfrak{p}] = [K_1 \colon K_\mathfrak{p}][L_\mathfrak{q} \colon K_\mathfrak{p}] = f_2 \cdot ef_1 = [(L^{\mathrm{ur},p})_\mathfrak{r} \colon K_\mathfrak{p}]$; so $K_1.L_\mathfrak{q} = (L^{\mathrm{ur},p})_\mathfrak{r}$. It follows that $\mathrm{Gal}((L^{\mathrm{ur},p})_\mathfrak{r}/K_1) \cong \mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p}) = \mathbb{Z}/(ef_1)\mathbb{Z}$ is a normal subgroup of $\mathrm{Gal}((L^{\mathrm{ur},p})_\mathfrak{r}/K_\mathfrak{p})$, so the group $\mathrm{Gal}((L^{\mathrm{ur},p})_\mathfrak{r}/K_\mathfrak{p})$, which is a semidirect product, is actually a direct product:

$$\mathrm{Gal}((L^{\mathrm{ur},p})_\mathfrak{r}/K_\mathfrak{p}) = \mathbb{Z}/f_2\mathbb{Z} \times \mathbb{Z}/(ef_1)\mathbb{Z} \cong \mathbb{Z}/(ef_1f_2)\mathbb{Z}.$$

Here, the last equality follows from $(ef_1, f_2) = 1$. This proves that $(L^{\mathrm{ur},p})_\mathfrak{r}/K_\mathfrak{p}$ is cyclic, which is what we wanted. □

Now, consider the following embedding problem:

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \downarrow & & \\ 1 & \longrightarrow & V & \longrightarrow & \Gamma' & \longrightarrow & \Gamma & \longrightarrow & 1, \end{array}$$

where V is a group of exponent p on which Φ acts by an irreducible representation and $\Gamma' = G' \rtimes \Phi$, for a p-group G' with an action of Φ. Since $L^{\mathrm{ur},p}/K$ satisfies property **P**, by

Theorem 2.2.3 we know that all the local embedding problems have solutions. Now, in order to use Theorem 2.2.1, we need to prove that the map

$$H^2(G_K, V) \to \prod_{\mathfrak{p} \in P} H^2(G_{K_\mathfrak{p}}, V)$$

is injective. Note that V is not a trivial $\mathbb{F}_p[\Gamma]$-module, so we can't apply Theorem 2.2.2 directly. Consider the following commutative diagram:

$$\begin{array}{ccc} H^2(G_K, V) & \longrightarrow & \prod_{\mathfrak{p}} H^2(G_{K_\mathfrak{p}}, V) \\ \Big\downarrow \text{res} & & \Big\downarrow \text{res} \\ H^2(G_L, V) & \longrightarrow & \prod_{\mathfrak{p}} H^2(G_{L_\mathfrak{p}}, V) \end{array}$$

Using spectral sequences, we observe that $H^2(G_L, V)^\Phi \cong H^2(G_K, V)$, so the restriction map on the left is injective. Similarly, it can be proved that the map on the right is injective. Note that G_K acts on V by Φ. Since $\mathrm{Gal}(L/K) = \Phi$, it follows that G_L acts trivially on V, so

$$H^2(G_L, V) \cong H^2(G_L, \mathbb{F}_p^n) \quad \text{and} \quad H^2(G_{L_\mathfrak{p}}, V) \cong H^2(G_{L_\mathfrak{p}}, \mathbb{F}_p^n),$$

where $n = \dim_{\mathbb{F}_p} V$. So by Theorem 2.2.2, the map on the bottom is injective. It thus follows that the top map is injective, and so by Theorem 2.2.1, the embedding problem we started with has a solution.

On the one hand, if the group extension is split, then a solution to the embedding problem will be given by $M = L^{\mathrm{ur},p}(\sqrt[p]{a_1}, \ldots, \sqrt[p]{a_n})/K$, with $a_1, \ldots, a_n \in L$, and $\mathrm{Gal}(M/K) \cong \Gamma' \cong V \rtimes \Gamma$. On the other hand, any two solutions to the embedding problem will differ by a split extension. To summarize:

Proposition 2.2.5. *Let L/K be an extension with Galois group Φ that satisfies property **P**.*

Consider the extension $L^{ur,p}/K$ with Galois group Γ. The embedding problem

$$1 \to V \to \Gamma' \to \Gamma \to 1$$

always has a solution. Furthermore, if $L^{ur,p}(\sqrt[p]{\alpha_1}, \ldots, \sqrt[p]{\alpha_n})/K$ is a solution, with $\alpha_i \in (L^{ur,p})^\times/(L^{ur,p})^{\times p}$, then all the other solutions are given by $L^{ur,p}(\sqrt[p]{\alpha_1 a_1}, \ldots, \sqrt[p]{\alpha_n a_n})/K$, where $a_i \in L^\times/L^{\times p}$, $\alpha_i a_i \neq 0$ in $(L^{ur,p})^\times/(L^{ur,p})^{\times p}$, and $\mathrm{Gal}(L(\sqrt[p]{a_1}, \ldots, \sqrt[p]{a_n})/K) \cong V \rtimes \Phi$.

2.3 Some technical lemmas

In this section, we present some facts that will be used in the proof of our main result. Some of these results can either be found in [Oza11] or are generalisations of results from [Oza11]. We will follow Ozaki's notation.

Let F be a number field and let $\mathfrak{p}$ be a prime of $\mathcal{O}_F$ lying above a rational prime p. Let $F_\mathfrak{p}$ be the completion of F at $\mathfrak{p}$, and denote by $U_\mathfrak{p}(F)$ the pro-p part of the local unit group of $F_\mathfrak{p}$. Let $U(F) = \oplus_{\mathfrak{p}|p} U_\mathfrak{p}(F)$. Consider the localisation of $\mathcal{O}_F$ at p and embed it diagonally into $U(F)$. Let $U'_\mathfrak{p}(F)$ be the submodule of $U(F)$ consisting of all the elements u such that $F_\mathfrak{p}(\sqrt[p]{u})/F_\mathfrak{p}$ is unramified and let $U'(F) = \oplus_{\mathfrak{p}|p} U'_\mathfrak{p}(F)$. Since $U(F)^p \subset U'(F) \subset U(F)$, we can define $R(F) = U(F)/U(F)^p$ and $R'(F) = U(F)/U'(F)$.

Going back to our situation, let p be a prime, let Φ be a group of order p and let G be a p-group with an action of Φ. Let L/K be a Galois extension with Galois group Φ such that $\mathrm{Gal}(L^{\mathrm{ur},p}/K) \cong G \rtimes \Phi$. Let $\Gamma = G \rtimes \Phi$. Assume moreover that every prime of K lying over p splits completely in $L^{\mathrm{ur},p}/K$. With this notation, we can prove the following:

Lemma 2.3.1. *If L/K is a Galois extension with Galois group Φ as above, then*

1. *$R(L) \cong \mathbb{F}_p[\Phi]^{[K:\,\mathbb{Q}]+s}$ and $R'(L) \cong \mathbb{F}_p[\Phi]^{[K:\,\mathbb{Q}]}$,*
2. *$R(L^{ur,p}) \cong \mathbb{F}_p[\Gamma]^{[K:\,\mathbb{Q}]+s}$ and $R'(L^{ur,p}) \cong \mathbb{F}_p[\Gamma]^{[K:\,\mathbb{Q}]}$,*

where s is the number of primes of K lying over p.

Proof. By definition, $U(K) = \oplus_{\mathfrak{p}|p} U_{\mathfrak{p}}(K) = \oplus_{\mathfrak{p}|p} \mathcal{O}_{K_{\mathfrak{p}}}^{\times} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p$. Tensoring with $\mathbb{F}_p$, we obtain that $\left(\mathcal{O}_{K_{\mathfrak{p}}}^{\times} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p\right) / \left(\mathcal{O}_{K_{\mathfrak{p}}}^{\times} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p\right)^p \cong \mathbb{F}_p^{d_{\mathfrak{p}}+1}$, where $d_{\mathfrak{p}} = [K_{\mathfrak{p}} \colon \mathbb{Q}_p]$. Note that $\sum_{\mathfrak{p}|p} d_{\mathfrak{p}} = [K \colon \mathbb{Q}]$. It follows that $R(K) \cong \mathbb{F}_p^{[K \colon \mathbb{Q}]+s}$. Similarly, $R'(K) \cong \mathbb{F}_p^{[K \colon \mathbb{Q}]}$.

Because every prime of K lying over p splits completely in L/K, we have a natural isomorphism of Φ-modules $U(L) \cong \mathbb{Z}_p[\Phi] \otimes_{\mathbb{Z}_p} U(K)$ and $U'(L) \cong \mathbb{Z}_p[\Phi] \otimes_{\mathbb{Z}_p} U'(K)$, which shows that $R(L) \cong \mathbb{F}_p[\Phi]^{[K \colon \mathbb{Q}]+s}$ and $R'(L) \cong \mathbb{F}_p[\Phi]^{[K \colon \mathbb{Q}]}$.

Similarly, since every prime of K lying over p splits completely in $L^{\mathrm{ur},p}/K$, we obtain that $R(L^{\mathrm{ur},p}) \cong \mathbb{F}_p[\Gamma]^{[K \colon \mathbb{Q}]+s}$ and $R'(L^{\mathrm{ur},p}) \cong \mathbb{F}_p[\Gamma]^{[K \colon \mathbb{Q}]}$. □

The following result is a generalisation of [Oza11, Lemma 9]. Note that Ozaki's Lemma only applies to $M = L^{\mathrm{ur},p}$, while our modification works for both $M = L^{\mathrm{ur},p}$ and $M = L$. This lemma is a key tool used in the proof of Theorem 1. The following proof uses the Chebotarev density theorem to construct a number of primes in $\mathcal{O}_M$ satisfying certain properties in $R(M)$.

Lemma 2.3.2. *Let $L^{ur,p}/K$ be an extension as above. Let $M = L$ or $L^{ur,p}$, and let $\tilde{M}/M$ be any finite abelian extension linearly disjoint from the maximal abelian extension of M unramified outside p. Then for any $u \in R(M)$ and any $\tau \in \mathrm{Gal}(\tilde{M}/M)$, there exist infinitely many prime ideals $\Lambda\mathcal{O}_M$ of $\mathcal{O}_M$ such that $\Lambda\mathcal{O}_M$ is prime to p, $(\Lambda \mod U(M)^p) = u$ in $R(M)$, and $(\Lambda\mathcal{O}_M, \tilde{M}/M) = \tau$.*

Proof. Let T be the maximal elementary abelian p-extension of M which is unramified outside p, and let H be the maximal elementary abelian p-extension of M unramified everywhere. Then we have the following exact sequence

$$\mathcal{O}_M^{\times} \otimes \mathbb{F}_p \to R(M) \xrightarrow{\rho} \mathrm{Gal}(T/M) \xrightarrow{f} \mathrm{Gal}(H/M) \to 1,$$

where the map $\rho \colon R(M) \to \mathrm{Gal}(T/M)$ is the map induced by class field theory, and the third

map is the natural surjection $f\colon \mathrm{Gal}(T/M) \to \mathrm{Gal}(H/M)$. Let $\sigma = \rho(u) \in \mathrm{Gal}(T/M)$. Let N be the maximal unramified abelian extension of M. Note that T and N are linearly disjoint over H, and let $\tilde{T}$ be their compositum. Observe that $\tilde{T}$ and $\tilde{M}$ are linearly disjoint over M. Let $\tilde{\sigma} \in \mathrm{Gal}(\tilde{T}/M)$ be an element with the properties that $\mathrm{res}(\tilde{\sigma}) \mid_T = \sigma^{-1}$ and $\mathrm{res}(\tilde{\sigma}) \mid_N = 1$. Such an element exists because T and N are linearly disjoint over H, and the restrictions $\sigma^{-1} \in \mathrm{Gal}(T/M)$ and $1 \in \mathrm{Gal}(H/M)$ agree on H/M, since $\mathrm{res}(\sigma^{-1}) \mid_H = \mathrm{res}(1) \mid_H$ if and only if $\sigma^{-1} \in \ker(f) = \mathrm{Im}(\rho)$, which is true by construction.

By the Chebotarev density theorem, there are infinitely many degree one primes α of $\mathcal{O}_M$ not lying over p such that $(\alpha, \tilde{T}/M) = \tilde{\sigma}$ and $(\alpha, \tilde{M}/M) = \tau$. Here, for a prime $\mathfrak{p}$ and an extension F/E, the symbol $(\mathfrak{p}, F/E)$ represents the Artin symbol. The first condition implies that $(\alpha, T/M) = \sigma^{-1}$ and $(\alpha, N/M) = 1$. But $(\alpha, N/M) = 1$ implies that α is a principal ideal in $\mathcal{O}_M$, so there exists $\Lambda_0 \in M$ such that $\alpha = \Lambda_0 \mathcal{O}_M$. Combining this with $(\alpha, T/M) = \sigma^{-1}$, we obtain that $\Lambda_0 = \Lambda\varepsilon$, for some $\varepsilon \in \mathcal{O}_M^\times$ and some $\Lambda \in M$. The element Λ has the properties $(\Lambda \mod U(M)^p) = u$ in $R(M)$ and $(\Lambda\mathcal{O}_M, \tilde{M}/M) = \tau$, which is what we wanted. □

We finish this section by noting that constructing unramified extensions in general is not a very difficult task: having a ramified extension, one may perform a series of base changes that kill off the ramification. However, in this thesis we are interested in finding maximal unramified extensions, so we need to have control over the class group of our newly constructed extensions. The following lemma due to Ozaki [Oza11] is a great tool in this direction.

Lemma 2.3.3 (Ozaki)**.** *Let p be any prime number, F a number field with $F^{ur,p} = F$ and S a finite set of primes of F. We denote by F_S/F the maximal elementary abelian p-extension of F unramified outside S. For any prime v of F, denote by D_v the decomposition subgroup*

of $\mathrm{Gal}(F_S/F)$ *at the prime* v*. We assume that the map*

$$\bigoplus_v H_2(D_v, \mathbb{Z}) \to H_2(\mathrm{Gal}(F_S/F), \mathbb{Z})$$

induced by the natural inclusion $D_v \subset \mathrm{Gal}(F_S/F)$ *is surjective. Then* $(F_S)^{ur,p} = F_S$*.*

Proof. See [Oza11, Lemma 7]. □

Corollary 2.3.4 (Ozaki)**.** *Let* S *and* F_S *be as in Lemma 2.3.3. If* F_S/F *is a cyclic extension, then* $(F_S)^{ur,p} = F_S$*.*

2.4 Background on universal unramified deformations

In this section, we introduce some definitions and results on deformations of Galois representations. Everything in this section is already known; a more detailed exposition of this can be found in [Maz89].

Throughout this section, let p be a prime number, let K be a number field and let G_K be the absolute Galois group of K. Let $\mathcal{C}$ denote the category of complete Noetherian local rings with residue field $\mathbb{F}_p$.

Consider a continuous Galois representation $\overline{\rho}\colon G_K \to \mathrm{GL}_2(\mathbb{F}_p)$. We will call this a residual representation. If A is a ring in $\mathcal{C}$, we can consider the lifts of $\overline{\rho}$ to $\mathrm{GL}_2(A)$. Let $\pi\colon A \to \mathbb{F}_p$ be the projection map. We say that two such lifts ρ_1, ρ_2 are strictly equivalent if there exists $M \in \ker(\mathrm{GL}_2(A) \to \mathrm{GL}_2(\mathbb{F}_p))$ such that $\rho_1 = M^{-1}\rho_2 M$. Deformations of the residual representation $\overline{\rho}$, as introduced by Mazur in [Maz89], are strict equivalence classes of continuous lifts:

Definition 2.4.1. Let $\overline{\rho}\colon G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ be a residual representation and let A be a local ring in $\mathcal{C}$. A deformation of $\overline{\rho}$ to A is a strict equivalent class of continuous homomorphisms $\rho\colon G_K \to \mathrm{GL}_2(A)$ such that the following diagram commutes:

$$\begin{array}{ccc} G_K & \xrightarrow{\overline{\rho}} & \mathrm{GL}_2(\mathbb{F}_p) \\ & \searrow^{\rho} & \uparrow \pi \\ & & \mathrm{GL}_2(A) \end{array}$$

We can therefore define a functor $\mathbf{D}\colon \mathcal{C} \rightsquigarrow \underline{\mathrm{Sets}}$ with $\mathbf{D}(A) = \{\text{deformations of } \overline{\rho} \text{ to } A\}$. We would like to understand when this functor is representable by a universal deformation ring. By a universal deformation ring we mean a complete Noetherian local ring $R \in \mathcal{C}$ with residue field $\mathbb{F}_p$, together with a deformation $\rho\colon G_K \to \mathrm{GL}_2(R)$, such that if $\psi\colon G_K \to \mathrm{GL}_2(A)$ is another deformation of $\overline{\rho}$, there is a unique morphism $\phi : R \to A$ such that $\psi = \phi \circ \rho$. Mazur proved in [Maz89, Proposition 1] that if $\overline{\rho}$ is absolutely irreducible, then a universal deformation ring exists.

Note that we can impose certain ramification conditions on these lifts. In this thesis, we are interested in lifts that are everywhere unramified. Let $\rho\colon G_K \to \mathrm{GL}_2(A)$ be a deformation of $\overline{\rho}$ for some ring $A \in \mathcal{C}$. This lift factors through some finite group, and the fixed field of the kernel is a finite extension. Call it $K(\rho)$. Denote the corresponding extension of $\overline{\rho}$ by $K(\overline{\rho})$. We say that the deformation ρ is unramified if the extension $K(\rho)/K(\overline{\rho})$ is unramified everywhere. The functor on $\mathcal{C}$ which sends A to the unramified deformations $D(A)$ is pro-representable by a universal deformation ring. We are interested in the following question:

Question 3. What possible rings R can occur as universal unramified deformation rings of such $\overline{\rho}$?

This question can be split into several cases:

- The representation $\overline{\rho}$ is absolutely irreducible and has image with order prime to p.
- The representation $\overline{\rho}$ is absolutely irreducible and has image with order divisible by p.
- The representation $\overline{\rho}$ is reducible. In this case, the universal (unramified) deformation ring need not exist, so one could consider an alternative question: what possible rings R occur as universal unramified pseudodeformation rings?

This thesis provides an answer to the first case via Theorem 2 and Conjecture 1. The author is also interested in the other two cases. However, certain techniques used in this thesis only apply to the first case, so approaching the other two cases would require different tools. Dealing with the second case (where the representation is absolutely irreducible and has image of order divisible by p) would require a modified version of Theorem 1 applicable to groups that have a more general form than just semidirect products between p-groups with groups of order prime to p. On the other hand, the last case (that of a reducible representation) would require a completely different version of Theorem 2 that would be suitable for pseudodeformations.

CHAPTER 3

CONSTRUCTING MAXIMAL UNRAMIFIED EXTENSIONS

In this chapter, we prove Theorem 1. Before outlining the proof, let us introduce two results that are crucial to the argument. Throughout this chapter, let p be a prime, let Φ be a group of order prime to p, and let G be a p-group with an action of Φ.

The following result allows us to perform base changes that extend the degree of the base field over $\mathbb{Q}$, but preserve all the other properties.

Theorem 3.0.1. *With the above notation, let L/K be a Galois extension of number fields with Galois group Φ satisfying:*

- *The extension $L^{ur,p}/K$ is Galois and has Galois group isomorphic to $\Gamma = G \rtimes \Phi$,*
- *The field K contains the group μ_p, and is totally imaginary if $p = 2$,*
- *Every prime of K lying over p splits completely in $L^{ur,p}$,*
- *The extension $K/\mathbb{Q}$ satisfies $[K\colon \mathbb{Q}] \geq 2\,(2d(G) + r(G) + d(\Phi))$, where $d(\tilde{G})$ and $r(\tilde{G})$, respectively, are the minimal number of generators and relations of a group $\tilde{G}$.*

Then there exists a cyclic extension K'/K of degree p such that if $L' = K'.L$, then:

1. $K' \cap L^{ur,p} = K$,
2. $(L')^{ur,p} = K'.L^{ur,p}$,
3. $\mathrm{Gal}((L')^{ur,p}/K') \cong \Gamma$,
4. *If the initial extension L/K satisfies property $\boldsymbol{P}$, then the new extension L'/K' also satisfies property $\boldsymbol{P}$. Moreover, under this assumption, the extension $(L')^{ur,p}/K'$ also satisfies property $\boldsymbol{P}$.*

Recall that any p-group G with an action of Φ fits into an exact sequence of the form

$$1 \to V \to G' \to G \to 1,$$

where V, G' are p-groups with an action of Φ. Moreover, V is a group of exponent p and Φ acts on V by an irreducible representation. Let $\Gamma = G \rtimes \Phi$ and $\Gamma' = G' \rtimes \Phi$. We have the following result:

Theorem 3.0.2. *Let L/K be a Galois extension of number fields satisfying the four conditions of Theorem 3.0.1 and property **P**. Assume that Φ acts irreducibly on the p-group V. Then for any exact sequence of groups*

$$1 \to V \to \Gamma' \to \Gamma \to 1,$$

there exists a finite extension of fields L'/K' such that:

1. *$K \subset K'$ and $L \subset L'$,*
2. *The extension L'/K' is Galois and has Galois group isomorphic to Φ,*
3. *The extension $(L')^{ur,p}/K'$ is Galois and has Galois group isomorphic to Γ',*
4. *Every prime of K' lying over p splits completely in $(L')^{ur,p}$,*
5. *The extension $(L')^{ur,p}/K'$ satisfies property **P**.*

The proof of Theorem 1 follows from Theorems 3.0.1 and 3.0.2 by induction. Recall that for a p-group G with a Φ-action, we have an exact sequence of p-groups

$$G = G_n \to G_{n-1} \to \cdots \to G_0 = 1,$$

where each map is surjective and the kernel at each step is isomorphic to V. If $\Gamma_i = G_i \rtimes \Phi$, then we have a sequence of surjections

$$\Gamma = \Gamma_n \to \Gamma_{n-1} \to \cdots \to \Gamma_0 = \Phi,$$

with $\ker(\Gamma_i \to \Gamma_{i-1}) \cong V$, for $1 \leq i \leq n$. The assumption of Theorem 1 is the base case of our inductive proof. At step i, we can assume that we have a Galois extension L_i/K_i satisfying the conditions of Theorem 3.0.1 for G_i and Γ_i. Using Theorem 3.0.1 repeatedly, we can construct a finite extension K_i' of K_i such that if $L_i' = K_i'.L_i$, then $K_i' \cap (L_i)^{\mathrm{ur},p} = K_i$, $(L_i')^{\mathrm{ur},p} = K_i'.(L_i)^{\mathrm{ur},p}$, and $\mathrm{Gal}((L_i')^{\mathrm{ur},p}/K_i') \cong \Gamma_i$. Moreover, repeatedly constructing extensions using Theorem 3.0.1, we increase the degree $[K_i' \colon \mathbb{Q}]$, while keeping $2(2d(G_{i+1}) + r(G_{i+1}) + d(\Phi))$ unchanged. Thus, we can also assume that $[K_i' \colon \mathbb{Q}] \geq 2(2d(G_{i+1}) + r(G_{i+1}) + d(\Phi))$. Since this extension L_i'/K_i' satisfies the conditions of Theorem 3.0.2, there exists a finite extension L_{i+1}/K_{i+1} such that $K_i' \subset K_{i+1}$, $L_i' \subset L_{i+1}$, $\mathrm{Gal}(L_{i+1}/K_{i+1}) \cong \Phi$, $\mathrm{Gal}((L_{i+1})^{\mathrm{ur},p}/K_{i+1}) \cong \Gamma_{i+1}$, every prime of K_{i+1} lying over p splits completely in $(L_{i+1})^{\mathrm{ur},p}$ and $(L_{i+1})^{\mathrm{ur},p}/K_{i+1}$ satisfies property $\mathbf{P}$. Therefore, we have obtained fields $K = K_n$, $L = L_n$ and $M = (L_n)^{\mathrm{ur},p}$ with the desired properties.

3.1 Proof of Theorem 3.0.1

In this section, we provide a proof for Theorem 3.0.1, which is our version of Proposition 1 in the first version of [Oza11]. Given a finite extension L/K satisfying the conditions of Theorem 1, Theorem 3.0.1 allows us to perform a base change that preserves all the properties of the initial extension, but increases the degree of the base field K over $\mathbb{Q}$. This base change will be a useful tool in the proof of Theorem 3.0.2.

Our proof is inspired Ozaki's proof of Proposition 1 in the first version of [Oza11], but uses techniques applicable to our situation. More explicitly, in his proof, Ozaki uses the

theory of $\mathbb{F}_p$-representations of p-groups G, while we have to use the more complex theory of $\mathbb{F}_p$-representations of groups of the form $G \rtimes \Phi$, where Φ is a group of order prime to p and G is a p-group with an action of Φ. Throughout this section, assume that the conditions of Theorem 3.0.1 hold. More explicitly, let Φ and G be as above. Assume we have a Galois extension L/K with Galois group Φ satisfying:

- The extension $L^{\mathrm{ur},p}/K$ is Galois and $\mathrm{Gal}(L^{\mathrm{ur},p}/K) \cong \Gamma = G \rtimes \Phi$.
- The field K contains μ_p, and is totally imaginary if $p = 2$.
- Every prime of K lying over p splits completely in $L^{\mathrm{ur},p}$.
- The extension $K/\mathbb{Q}$ satisfies $[K\colon \mathbb{Q}] \geq 2(2d(G) + r(G) + d(\Phi))$.

We claim that proving Theorem 3.0.1 reduces to finding an element Λ of $L^{\mathrm{ur},p}$ with the following properties:

(1) The ideal $\Lambda\mathcal{O}_{L^{\mathrm{ur},p}}$ is a prime ideal of degree 1, not lying over p.

(2) If S denotes the set of primes of $L^{\mathrm{ur},p}$ dividing $\eta = N_{L^{\mathrm{ur},p}/K}(\Lambda)$, then $L^{\mathrm{ur},p}(\sqrt[p]{\eta})$ is the maximal elementary abelian p-extension of $L^{\mathrm{ur},p}$ unramified outside S.

Lemma 3.1.1. *Assume such an element Λ of $L^{ur,p}$ exists. Let $K' = K(\sqrt[p]{\eta})$, with η as above. Then K'/K is an extension that makes Theorem 3.0.1 true.*

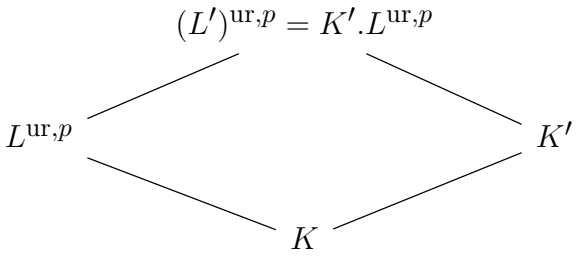
Proof. Since $\eta\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$, it follows that $\sqrt[p]{\eta} \notin K$, so K' is a degree p extension of K. Let $L' = L.K'$. The fields L and K' are linearly disjoint over K, so L'/L is a degree p extension. We want to prove that $K' \cap L^{\mathrm{ur},p} = K$, $(L')^{\mathrm{ur},p} = K'.L^{\mathrm{ur},p}$, and that the extension $(L')^{\mathrm{ur},p}/K'$ is Galois with Galois group isomorphic to Γ.

Consider $K' \cap L^{\mathrm{ur},p}$. This is equal to K' if $K' \subset L^{\mathrm{ur},p}$; otherwise, it is equal to K. Assume $K' \subset L^{\mathrm{ur},p}$. By construction, this implies that $L' \subset L^{\mathrm{ur},p}$. But $L^{\mathrm{ur},p}$ is the maximal unramified p-extension of L, and L' is a ramified p-extension of L, so they must

be linearly disjoint over L, and $L' \not\subset L^{\mathrm{ur},p}$. It follows that our assumption was false, and so $K' \cap L^{\mathrm{ur},p} = K$, which proves the first part.

Using the previous part, we observe that $K'.L^{\mathrm{ur},p} = L^{\mathrm{ur},p}(\sqrt[p]{\eta})$ and $L'.L^{\mathrm{ur},p} = L^{\mathrm{ur},p}(\sqrt[p]{\eta})$. By construction, $L^{\mathrm{ur},p}(\sqrt[p]{\eta})$ is the maximal elementary abelian p-extension of $L^{\mathrm{ur},p}$ unramified outside S, so Corollary 2.3.4 tells us that $(L^{\mathrm{ur},p}(\sqrt[p]{\eta}))^{\mathrm{ur},p} = L^{\mathrm{ur},p}(\sqrt[p]{\eta})$. On the one hand, since $K' \subset K'.L^{\mathrm{ur},p}$, we must have $(L')^{\mathrm{ur},p} \subset L_p(K'.L^{\mathrm{ur},p}) = K'.L^{\mathrm{ur},p}$. On the other hand, $L'.L^{\mathrm{ur},p}$ is an unramified p-extension of L', so $L'.L^{\mathrm{ur},p} \subset (L')^{\mathrm{ur},p}$. Combining these remarks, we obtain that $(L')^{\mathrm{ur},p} = L'.L^{\mathrm{ur},p} = K'.L^{\mathrm{ur},p}$, proving the second part.

To prove that the new extension has the right Galois group, consider the following diagram



Since the extension $L^{\mathrm{ur},p}/K$ is Galois and has Galois group isomorphic to Γ, it follows that $(L')^{\mathrm{ur},p}/K'$ is Galois and $\mathrm{Gal}((L')^{\mathrm{ur},p}/K') = \mathrm{Gal}(K'.L^{\mathrm{ur},p}/K') \cong \mathrm{Gal}(L^{\mathrm{ur},p}/K) \cong \Gamma$, which is what we wanted.

To conclude the proof, we need to check that if the initial extension has property **P**, then the new extensions also have property **P**. To this end, assume that L/K has property **P**. Firstly, let us prove that L'/K' satisfies property **P**. Let $\mathfrak{p}$ be a prime of K, and take primes $\mathfrak{q}$, $\mathfrak{p}'$, and $\mathfrak{q}'$, respectively, of L, K', and L', respectively, lying above it. Let $K_{\mathfrak{p}}$, $K'_{\mathfrak{p}'}$, $L_{\mathfrak{q}}$, and $L'_{\mathfrak{q}'}$ be the corresponding completions. Let e and e' be the ramification indices of $\mathfrak{p}$ in L/K and of $\mathfrak{p}'$ in L'/K', respectively. Let q and q' be the number of elements of the residue fields of $K_{\mathfrak{p}}$ and $K'_{\mathfrak{p}'}$, respectively. Since the order of Φ is prime to p, we must have that $e = e'$, and $q' = q$ or $q' = q^p$. Since L/K has property **P**, then either $e = 1$ or $L_{\mathfrak{q}}/K_{\mathfrak{p}}$ is tamely ramified with $e \mid (q-1)$. It follows that either $e' = e = 1$ or $L'_{\mathfrak{q}'}/K'_{\mathfrak{p}'}$ is tamely

ramified with $e' \mid (q-1) \mid (q'-1)$. Finally, if $L_{\mathfrak{q}}/K_{\mathfrak{p}}$ is cyclic of order prime to p, then by construction, $L'_{\mathfrak{q}'}/K'_{\mathfrak{p}'}$ is also cyclic of order prime to p, so the new extension L'/K' has property **P**. Finally, we need to show that if L/K satisfies property **P**, then $(L')^{\mathrm{ur},p}/K'$ also satisfies property **P**, but this follows from Lemma 2.2.4. □

Now, we would like to find an element Λ satisfying (1) and (2). To this end, assume that we already have an element Λ satisfying only the first property. Let S be the set of primes of $L^{\mathrm{ur},p}$ dividing η. If $L^{\mathrm{ur},p}(\sqrt[p]{\alpha})/L^{\mathrm{ur},p}$ is unramified outside S, for some $\alpha \in L^{\mathrm{ur},p}$, then

$$\alpha \mod (L^{\mathrm{ur},p})^{\times p} \equiv (\varepsilon \mod (L^{\mathrm{ur},p})^{\times p}) + \sum_{\sigma\in\Gamma} a_\sigma(\sigma\Lambda \mod (L^{\mathrm{ur},p})^{\times p}),$$

for some $a_\sigma \in \mathbb{F}_p$, $\varepsilon \in \mathcal{O}^{\times}_{L^{\mathrm{ur},p}}$. Since $L^{\mathrm{ur},p}(\sqrt[p]{\alpha})/L^{\mathrm{ur},p}$ is unramified at the primes above p, it must be true that

$$(\varepsilon \mod U'(L^{\mathrm{ur},p})) + \sum_{\sigma\in\Gamma} a_\sigma(\sigma\Lambda \mod U'(L^{\mathrm{ur},p})) \equiv 0.$$

If this equation only holds when $\varepsilon \in (\mathcal{O}^{\times}_{L^{\mathrm{ur},p}})^p$ and $a_\sigma = a$, $\forall \sigma \in \Gamma$, for some $a \in \mathbb{F}_p$, then

$$\alpha \mod U(L^{\mathrm{ur},p})^p \equiv a\sum_{\sigma\in\Gamma} \sigma(\Lambda \mod U(L^{\mathrm{ur},p})^p) = a(\eta \mod U(L^{\mathrm{ur},p})^p).$$

Thus, $\sqrt[p]{\alpha} \in L^{\mathrm{ur},p}(\sqrt[p]{\eta})$, so condition (2) also holds.

Let $E = E(L^{\mathrm{ur},p})$ be the image of the map $\mathcal{O}^{\times}_{L^{\mathrm{ur},p}} \otimes \mathbb{F}_p \to R'(L^{\mathrm{ur},p})$. If ε is an element in $\mathcal{O}^{\times}_{L^{\mathrm{ur},p}} \setminus (\mathcal{O}^{\times}_{L^{\mathrm{ur},p}})^p$, then the field extension $L^{\mathrm{ur},p}(\sqrt[p]{\varepsilon})/L^{\mathrm{ur},p}$ must be ramified at some prime lying over p. Thus, the map $\mathcal{O}^{\times}_{L^{\mathrm{ur},p}} \otimes \mathbb{F}_p \to R'(L^{\mathrm{ur},p})$ must be injective, and so $E \cong \mathcal{O}^{\times}_{L^{\mathrm{ur},p}} \otimes \mathbb{F}_p$. It follows that the map $\mathcal{O}^{\times}_{L^{\mathrm{ur},p}} \otimes \mathbb{F}_p \to R(L^{\mathrm{ur},p})$ is also injective, and by abuse of notation we denote its image by E.

The following result represents a key step in the proof of Theorem 3.0.1. It is a variation of Lemma 8 in [Oza11] and it is inspired by Lemma 2 in the first version of the same

paper. The main difference between Ozaki's proof and our proof comes from the fact that in [Oza11], $\mathbb{F}_p[G]$ is a projective indecomposable $\mathbb{F}_p[G]$-module, and this doesn't remain true if we replace G by $\Gamma = G \rtimes \Phi$ (for G a p-group and Φ a group of order prime to p). To deal with this, we turn to the theory of modular representations for groups of the form $G \rtimes \Phi$. For a more detailed treatment of this, see [Web16]. We will also make use of some of the ideas appearing in Section 6 of [HM17].

Proposition 3.1.2. *Let N be the kernel of the projection $R(L^{ur,p}) \to R'(L^{ur,p})$. Then N is a free $\mathbb{F}_p[\Gamma]$-module. Moreover, there exist free $\mathbb{F}_p[\Gamma]$-modules M and Q of $R(L^{ur,p})$ such that:*

- $R(L^{ur,p}) = M \oplus N \oplus Q$ *and* $R'(L^{ur,p}) \cong M \oplus Q$.
- $E \subset M$.
- $\operatorname{rank}_{\mathbb{F}_p[\Gamma]} Q \geq \frac{1}{2}[K\colon \mathbb{Q}] - d(G) - r(G)$.

Proof. Note that $\mathbb{F}_p[\Gamma]$ is a Frobenius algebra, so injective $\mathbb{F}_p[\Gamma]$-modules are the same as projective $\mathbb{F}_p[\Gamma]$-modules. In particular, any free $\mathbb{F}_p[\Gamma]$-module is injective.

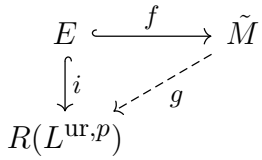
By Lemma 2.1.1, the indecomposable projective $\mathbb{F}_p[\Gamma]$-modules P_S are in a one-to-one correspondence with the simple $\mathbb{F}_p[\Phi]$-modules S. It follows that $\mathbb{F}_p[\Gamma]$ can be decomposed as a sum of indecomposable projective modules

$$\mathbb{F}_p[\Gamma] = \bigoplus_{S \text{ simple}} P_S^{n_s},$$

where $n_s = \dim_D(S)$, $D = \operatorname{End}_{\mathbb{F}_p[\Phi]} S$. Here, the sum is over the simple $\mathbb{F}_p[\Phi]$-modules S.

From Section 2.1, we know that any $\mathbb{F}_p[\Gamma]$-module has a unique injective hull (for more details of this, see [Web16, Section 8.5]). Let $\tilde{M} = \oplus P_S^{\alpha_S}$ be the injective hull of the

$\mathbb{F}_p[\Gamma]$-module E. Consider the following diagram:



The $\mathbb{F}_p[\Gamma]$-module $R(L^{\mathrm{ur},p})$ is free by Lemma 2.3.1, so it is injective. The map i is the usual inclusion map from E to $R(L^{\mathrm{ur},p})$. The map f is the essential monomorphism $E \to \tilde{M}$. Since $R(L^{\mathrm{ur},p})$ is an injective $\mathbb{F}_p[\Gamma]$-module, there exists a map $g\colon \tilde{M} \to R(L^{\mathrm{ur},p})$ such that $g \circ f = i$. Moreover, since f is an essential monomorphism, the map g is injective. Let $M_1 = \mathrm{Im}(g) \subset R(L^{\mathrm{ur},p})$; the module E can be seen as a submodule of M_1.

By definition of N, we have a short exact sequence of $\mathbb{F}_p[\Gamma]$-modules:

$$1 \to N \to R(L^{\mathrm{ur},p}) \to R'(L^{\mathrm{ur},p}) \to 1.$$

Since $R'(L^{\mathrm{ur},p})$ is a free module (Lemma 2.3.1), this sequence splits. It follows that N is a stably free $\mathbb{F}_p[\Gamma]$-module, which implies that N is a free $\mathbb{F}_p[\Gamma]$-module of rank s.

Consider the intersection $M_1 \cap N \subset M_1$. Let $\mathrm{Soc}(M_1 \cap N)$ be the socle of $M_1 \cap N$. For details about this notion, see Section 2.1 and [Web16, Section 6.3]. Since $\mathbb{F}_p[\Gamma]$ is an Artinian ring, every nonzero module has a simple submodule. It follows that if $M_1 \cap N$ is nonzero, then $\mathrm{Soc}(M_1 \cap N)$ must be nonzero. Using Lemma 2.1.2, we obtain

$$\begin{aligned}
\mathrm{Soc}(M_1 \cap N) &= (M_1 \cap N) \cap \mathrm{Soc}\, M_1 \\
&= N \cap \mathrm{Soc}\, M_1 \\
&\cong N \cap \mathrm{Soc}\, E \\
&\subset N \cap E \\
&= 0.
\end{aligned}$$

Here, the first and the third equalities follow from Lemma 2.1.2; the last equality follows from the fact that E and N are disjoint. It follows that $M_1 \cap N = 0$, so $M_1 + N$ is a direct sum in $R(L^{\mathrm{ur},p})$. Since $M_1 \oplus N$ is a projective $\mathbb{F}_p[\Gamma]$-module, it must also be injective, so the following exact sequence splits:

$$1 \to M_1 \oplus N \to R(L^{\mathrm{ur},p}) \to R(L^{\mathrm{ur},p})/(M_1 \oplus N) \to 1.$$

Let $Q_1 = R(L^{\mathrm{ur},p})/(M_1 \oplus N)$. This is a projective $\mathbb{F}_p[\Gamma]$-module, so it can be written as $Q_1 = \oplus P_S^{\beta_S}$ with the property that $\alpha_S + \beta_S = [K\colon \mathbb{Q}] \cdot n_S$.

We would like to estimate β_S. Let $r = \mathrm{rank}_{\mathbb{F}_p[\Phi]} E^G = \mathrm{rank}_{\mathbb{F}_p[\Phi]} (E^G)^* = \mathrm{rank}_{\mathbb{F}_p[\Phi]} (E^*)_G$. Thus, $\mathbb{F}_p[\Phi]^r \twoheadrightarrow (E^*)_G$. By Nakayama's Lemma, $\mathbb{F}_p[\Gamma]^r \twoheadrightarrow E^*$. Taking duals and using the fact that $\mathbb{F}_p[\Gamma]$ is self-dual, we obtain that $E \cong E^{**} \hookrightarrow \mathbb{F}_p[\Gamma]^r$. Since $\tilde{M}$ is the injective hull of E and $\mathbb{F}_p[\Gamma]$ is an injective module, we obtain that $\tilde{M} \hookrightarrow \mathbb{F}_p[\Gamma]^r$, which implies that $\alpha_S \leq n_S \cdot r$, so it is enough to estimate r. To compute this rank r, we follow the idea in Section 6 of [HM17].

On the one hand, from the exact sequence

$$0 \to \mathcal{O}^\times_{L^{\mathrm{ur},p}}/\mu_p \xrightarrow{p} \mathcal{O}^\times_{L^{\mathrm{ur},p}} \to \mathcal{O}^\times_{L^{\mathrm{ur},p}}/p \to 0,$$

we derive the sequence:

$$(\mathcal{O}^\times_{L^{\mathrm{ur},p}}/\mu_p)^G \to (\mathcal{O}^\times_{L^{\mathrm{ur},p}})^G \to (\mathcal{O}^\times_{L^{\mathrm{ur},p}}/p)^G \to H^1(G, \mathcal{O}^\times_{L^{\mathrm{ur},p}}/\mu_p).$$

We observe that

- $(\mathcal{O}^\times_{L^{\mathrm{ur},p}}/p)^G = E^G$,
- $(\mathcal{O}^\times_{L^{\mathrm{ur},p}})^G/(\mathcal{O}^\times_{L^{\mathrm{ur},p}}/\mu_p)^G \cong (\mathcal{O}^\times_L)/(\mathcal{O}^\times_L/\mu_p) \cong \mathcal{O}^\times_L/\mathcal{O}^{\times p}_L$,

so the sequence becomes:

$$\mathcal{O}_L^\times/\mathcal{O}_L^{\times p} \to E^G \to H^1(G, \mathcal{O}_{L^{\mathrm{ur},p}}^\times/\mu_p). \tag{3.1}$$

On the other hand, from the exact sequence

$$0 \to \mu_p \to \mathcal{O}_{L^{\mathrm{ur},p}}^\times \to \mathcal{O}_{L^{\mathrm{ur},p}}^\times/\mu_p \to 0,$$

we get the exact sequence:

$$H^1(G, \mathcal{O}_{L^{\mathrm{ur},p}}^\times) \to H^1(G, \mathcal{O}_{L^{\mathrm{ur},p}}^\times/\mu_p) \to H^2(G, \mu_p). \tag{3.2}$$

The p-group G acts trivially on μ_p, so for $i = 1, 2$, the groups $H^i(G, \mu_p)$ describe the generators and relations of G.

Before we continue the proof, let us introduce some notation. For a p-group H, let d_pH be the p-rank of H, $d(H)$ be the number of generators of H, and $r(H)$ be the number of relations of H.

Consider the inclusion $L \hookrightarrow L^{\mathrm{ur},p}$. It induces a map on class groups $\mathrm{Cl}_L \to \mathrm{Cl}_{L^{\mathrm{ur},p}}$ whose kernel is isomorphic to $H^1(G, \mathcal{O}_{L^{\mathrm{ur},p}}^\times)$ (see 2 in [Iwa56]). On the other hand, this kernel is also isomorphic to the p-primary part of Cl_L. By class field theory, we know that the p-primary part of Cl_L is isomorphic to the abelianisation of $\mathrm{Gal}(L^{\mathrm{ur},p}/L) = G$, so $H^1(G, \mathcal{O}_{L^{\mathrm{ur},p}}^\times) \cong G^{\mathrm{ab}}$. It follows that

$$d_pH^1(G, \mathcal{O}_{L^{\mathrm{ur},p}}^\times) = d(G^{\mathrm{ab}}) \leq d(G),$$

From the semisimple version of Dirichlet's unit theorem ([HM17, Theorem 6.1]; for a proof, see [Gra98, Theorem 6.1]) and the fact that K is totally imaginary, we obtain that

$$\mathrm{rank}_{\mathbb{F}_p[\Phi]}(\mathcal{O}_L^\times/\mathcal{O}_L^{\times p}) \leq \frac{1}{2}[K\colon \mathbb{Q}]. \tag{3.3}$$

From (3.1), (3.2) and (3.3) it follows that

$$\begin{aligned} r = \operatorname{rank}_{\mathbb{F}_p[\Phi]}\left(E^G\right) &\leq \operatorname{rank}_{\mathbb{F}_p[\Phi]}(\mathcal{O}_L^\times/\mathcal{O}_L^{\times p}) + d_p H^1(G, \mathcal{O}_{L^{\mathrm{ur},p}}^\times/\mu_p) \\ &\leq \operatorname{rank}_{\mathbb{F}_p[\Phi]}(\mathcal{O}_L^\times/\mathcal{O}_L^{\times p}) + d_p H^1(G, \mathcal{O}_{L^{\mathrm{ur},p}}^\times) + d_p H^2(G, \mu_p) \\ &\leq \frac{1}{2}[K\colon \mathbb{Q}] + d(G) + r(G), \end{aligned}$$

Therefore:

$$\begin{aligned} \beta_S &= [K\colon \mathbb{Q}] \cdot n_S - \alpha_S \\ &\geq [K\colon \mathbb{Q}] \cdot n_S - n_S \cdot r \\ &\geq [K\colon \mathbb{Q}] \cdot n_S - n_S \cdot \left(\frac{1}{2}[K\colon \mathbb{Q}] + d(G) + r(G)\right) \\ &\geq n_S \left(\frac{1}{2}[K\colon \mathbb{Q}] - d(G) - r(G)\right). \end{aligned}$$

We can thus choose $t \geq (\frac{1}{2}[K\colon \mathbb{Q}] - d(G) - r(G))$ such that $Q := \oplus P_S^{n_S \cdot t}$ is isomorphic to a submodule of Q_1. This new module Q is a free $\mathbb{F}_p[\Gamma]$-module of rank t. Moreover, it is injective, so $P = Q_1/Q$ is a projective $\mathbb{F}_p[\Gamma]$-module with $Q_1 = Q \oplus P$. Let $M = M_1 \oplus P$. Then

$$R(L^{\mathrm{ur},p}) = M_1 \oplus N \oplus Q_1 \cong M_1 \oplus N \oplus Q \oplus P \cong M \oplus N \oplus Q,$$

with $E \subset M$ and $\operatorname{rank}_{\mathbb{F}_p[\Gamma]} Q \geq \frac{1}{2}[K\colon \mathbb{Q}] - d(G) - r(G)$.

Since M is a stably free $\mathbb{F}_p[\Gamma]$-module, we can conclude that it is a free $\mathbb{F}_p[\Gamma]$-module, so the proof is complete. □

The only thing left to show is the existence of an element Λ of $L^{\mathrm{ur},p}$ with properties (1) and (2). The proof is similar to the proof of Proposition 1 in the first version of [Oza11]. Let M and $Q = \bigoplus_{i=1}^t \mathbb{F}_p[\Gamma] q_i$ be the $\mathbb{F}_p[\Gamma]$-submodules of $R(L^{\mathrm{ur},p})$ given by Proposition 3.1.2.

Then, by assumption of Theorem 3.0.1,

$$t \geq \frac{1}{2}[K\colon \mathbb{Q}] - d(G) - r(G) \geq d(G) + d(\Phi) \geq d(\Gamma).$$

Let $\{\sigma_1, \ldots, \sigma_d\}$ be a system of minimal generators for Γ, $d = d(\Gamma)$. Let $u = \sum_{i=1}^{d}(\sigma_i - 1)q_i \in Q \subset R(L^{\mathrm{ur},p})$. By Lemma 2.3.2 applied to $M = L^{\mathrm{ur},p}$, there exists $\Lambda\mathcal{O}_{L^{\mathrm{ur},p}}$ a prime of degree 1, not lying over p, such that $u = (\Lambda \mod U(L^{\mathrm{ur},p})^p)$. Assume that there exist $\varepsilon \in \mathcal{O}_{L^{\mathrm{ur},p}}^{\times}$ and $a_\sigma \in \mathbb{F}_p$ such that $(\varepsilon \mod U'(L^{\mathrm{ur},p})) + \sum_{\sigma\in\Gamma} a_\sigma(\sigma\Lambda \mod U'(L^{\mathrm{ur},p})) = 0$. Observe that:

- $\varepsilon \mod U(L^{\mathrm{ur},p})^p + \sum_{\sigma\in\Gamma} a_\sigma(\sigma\Lambda \mod U(L^{\mathrm{ur},p})^p) \in N$;
- $\sum_{\sigma\in\Gamma} a_\sigma(\sigma\Lambda \mod U(L^{\mathrm{ur},p})^p) = \sum_{\sigma\in\Gamma} a_\sigma(\sigma u) \in Q$;
- $\varepsilon \mod U(L^{\mathrm{ur},p})^p \in E \subset M$.

By Proposition 3.1.2, it follows that $\varepsilon \mod U(L^{\mathrm{ur},p})^p = \sum_{\sigma\in\Gamma} a_\sigma(\sigma\Lambda \mod U(L^{\mathrm{ur},p})^p) = 0$. On the one hand, since $U(L^{\mathrm{ur},p})^p \cap \mathcal{O}_{L^{\mathrm{ur},p}}^{\times} = \mathcal{O}_{L^{\mathrm{ur},p}}^{\times p}$, it follows that $\varepsilon \in \mathcal{O}_{L^{\mathrm{ur},p}}^{\times p}$. On the other hand, $\sum_{\sigma\in\Gamma} a_\sigma(\sigma\Lambda \mod U(L^{\mathrm{ur},p})^p) = 0$ implies $\sum_{\sigma\in\Gamma} a_\sigma\sigma[\sum_{i=1}^{d}(\sigma_i - 1)q_i] = \sum_{\sigma\in\Gamma} a_\sigma(\sigma u) = 0$. This implies $\sum_{\sigma\in\Gamma} a_\sigma\sigma(\sigma_i - 1) = 0$, for all $1 \leq i \leq d$, so $\sum_{\sigma\in\Gamma} a_\sigma\sigma(\tau - 1) = 0$, for all $\tau \in \Gamma$, meaning that a_σ must be constant for all $\sigma \in \Gamma$, i.e. $a_\sigma = a \in \mathbb{F}_p$, for some $a \in \mathbb{F}_p$. We have thus shown that Λ has properties (1) and (2), so the proof is complete.

3.2 Proof of Theorem 3.0.2

In this section, we will provide a proof for Theorem 3.0.2. This theorem represents the inductive step in the proof of Theorem 1. The proof can be split into two cases: when the following sequence splits or when it doesn't split:

$$1 \to V \to \Gamma' \to \Gamma \to 1.$$

The case when the extension does not split will use the embedding problem combined with the case when the extension splits, and will be treated at the end of this section. Assume first that the sequence splits. In this case, $\Gamma' \cong V \rtimes \Gamma$, and we can work over L.

Let $n = \dim_{\mathbb{F}_p} V$ and let $m = |\Phi|$. Let $g_1, \ldots, g_n$ be generators of the action of Φ on V. Let $T = \frac{(p^{2n}-1)(p^{2n}-p)}{(p^2-1)(p^2-p)}$. We can assume that $[K\colon \mathbb{Q}] \geq 2d(T+2)$, where $d = d(\Phi)$ is the number of generators of Φ, by replacing K with some finite extension of K given by Theorem 3.0.1. Recall that Theorem 3.0.1 constructs a new extension that satisfies property **P** if the initial extension satisfies this property. Note that $R(L^{\mathrm{ur},p})^G \cong R(L)$ and $R'(L^{\mathrm{ur},p})^G \cong R'(L)$ as $\mathbb{F}_p[\Phi]$-modules, $N^G \cong \ker(R(L) \to R'(L))$, and $(\mathcal{O}_L^\times \otimes \mathbb{F}_p) \cap Q^G = 0$, where Q is the $\mathbb{F}_p[\Gamma]$-module obtained in Proposition 3.1.2. Let $\{\sigma_1, \ldots, \sigma_d\}$ be a generator system of Φ. The free $\mathbb{F}_p[\Phi]$-module Q^G can be written as $Q^G = \bigoplus_{i=1}^t \mathbb{F}_p[\Phi] q_i$, with $t \geq d(T+2)$.

Using Lemma 2.3.2 applied to $M = L$, we obtain primes $\lambda_i \mathcal{O}_L$ that are completely split in $L^{\mathrm{ur},p}/L$, and satisfy $N(\lambda_i) \equiv 1 \pmod{p}$ and

$$\lambda_i \mod U(L)^p = \sum_{j=1}^{d} (1+\sigma_j) q_{(i-1)d+j}$$

in $R(L)$, for $1 \leq i \leq T$. Moreover, we can also assume that the primes of K below λ_i split completely in L/K.

Since Φ has order prime to p, the $\mathbb{F}_p[\Phi]$-module $R(L)$ can be decomposed as a direct sum of isotypic components:

$$R(L) = \bigoplus_W W^{n_W},$$

where each W is a simple $\mathbb{F}_p[\Phi]$-representation. Each $a \in R(L)$ may therefore be written as $a = \sum a_W$, where $a_W \in W^{n_W}$. The isotypic projection P_W of $R(L)$ onto W^{n_W} is given by

the formula

$$P_W = \frac{\dim W}{\mid \Phi \mid \cdot \dim_{\mathbb{F}_p} \operatorname{End} W} \sum_{g \in \Phi} \chi_W(g^{-1}) g,$$

where χ_W is the character of W. This is a modified version of [Ser77, Theorem 8] that applies to (not necessarily algebraically closed) finite fields. Note that $P_W(P_U(a)) = a_W$ if $U \cong W$ and $P_W(P_U(a)) = 0$ if $U \ncong W$. To ease notation, we will write $n_{g,W} = \frac{\dim W \cdot \chi_W(g^{-1})}{|\Phi| \cdot \dim_{\mathbb{F}_p} \operatorname{End} W}$. We can then write $P_W(a) = \sum_{g \in \Phi} n_{g,W} g(a)$. Note that since V is an absolutely irreducible $\mathbb{F}_p[\Phi]$-representation, $n_{g,V}$ is well-defined and nonzero in $\mathbb{F}_p$.

Consider the group $(\mathbb{Z}/p\mathbb{Z})^{2n}$. Let $(a_1, \ldots, a_n, b_1, \ldots, b_n)$ and $(x_1, \ldots, x_n, y_1, \ldots, y_n)$ be two nonzero elements of $(\mathbb{Z}/p\mathbb{Z})^{2n}$ that are not multiples of each other. This pair generates a $(\mathbb{Z}/p\mathbb{Z})^2$-subgroup of $(\mathbb{Z}/p\mathbb{Z})^{2n}$. There are $\frac{(p^{2n}-p)(p^{2n}-1)}{(p^2-p)(p^2-1)}$ subspaces spanned by such a pair, i.e. $(\mathbb{Z}/p\mathbb{Z})^2$-subgroups; label them from 1 to $\frac{(p^{2n}-p)(p^{2n}-1)}{(p^2-p)(p^2-1)}$. For each such subgroup, choose a prime λ_ℓ from the ones constructed above (we can do this since $T = \frac{(p^{2n}-p)(p^{2n}-1)}{(p^2-p)(p^2-1)}$) and define ν_1 and ν_2 to be products of conjugates of λ_ℓ, with $1 \leq \ell \leq T$, with the properties that the exponents of $g_1^{-1}(\lambda_\ell), g_2^{-1}(\lambda_\ell), \ldots g_n^{-1}(\lambda_\ell)$ in ν_1 are $a_1, \ldots, a_n$, and the exponents of $g_1^{-1}(\lambda_\ell), g_2^{-1}(\lambda_\ell), \ldots g_n^{-1}(\lambda_\ell)$ in ν_2 are $b_1, \ldots, b_n$, respectively. Write $a_{i,\ell} = a_i$, $b_{i,\ell} = b_i$, $x_{i,\ell} = x_i$, and $y_{i,\ell} = y_i$. Let $\nu_1 = \prod_{i=1}^{T} \prod_{g \in \Phi} g(\lambda_i)^{s_{g,i}}$ and $\nu_2 = \prod_{i=1}^{T} \prod_{g \in \Phi} g(\lambda_i)^{t_{g,i}}$. Write $g_i(\nu_1) = \lambda_\ell^{a_{i,\ell}} \omega_{i,\ell}$ and $g_i(\nu_2) = \lambda_\ell^{b_{i,\ell}} \xi_{i,\ell}$, for all $1 \leq i \leq n$, with $\omega_{i,\ell}$ and $\xi_{i,\ell}$ not divisible by λ_ℓ. For each ℓ, let $\overline{r_\ell}$ be a non p-power modulo $\lambda_\ell \mathcal{O}_L$. Lift this $\overline{r_\ell}$ to a principal ideal $r_\ell \mathcal{O}_L$ in $\mathcal{O}_L$. We distinguish two cases, each containing two subcases:

1. If $a_{i,\ell} \neq 0$, for some i, let

$$c_{j,\ell} = \begin{cases} x_{j,\ell} a_{i,\ell} - x_{i,\ell} a_{j,\ell}, & \text{if } j \neq i, \\ 0, & \text{if } j = i. \end{cases}$$

$$d_{j,\ell} = y_{j,\ell} a_{i,\ell} - x_{i,\ell} b_{j,\ell}, \text{ for all } j.$$

Since $(a_{1,\ell},\ldots,a_{n,\ell},b_{1,\ell},\ldots,b_{n,\ell})$ and $(x_{1,\ell},\ldots,x_{n,\ell},y_{1,\ell},\ldots,y_{n,\ell})$ are not multiples of each other, at least one of $c_{j,\ell}$ and $d_{j,\ell}$ is nonzero.

(a) If $c_{j,\ell}\neq 0$, for some $j\neq i$, let

$$A_{k,\ell}=\begin{cases}\omega_{k,\ell}^{-1} & \text{if } k=i,\\ r_\ell\cdot\omega_{k,\ell}^{-1} & \text{if } k=j,\\ r_\ell^{c_{k,\ell}c_{j,\ell}^{-1}}\cdot\omega_{k,\ell}^{-1} & \text{otherwise.}\end{cases}$$

$$B_{k,\ell}=r_\ell^{d_{k,\ell}c_{j,\ell}^{-1}}\cdot\xi_{k,\ell}^{-1},\ \text{for all } k.$$

(b) If $d_{j,\ell}\neq 0$, for some j (possibly $j=i$), let

$$A_{k,\ell}=\begin{cases}\omega_{k,\ell}^{-1} & \text{if } k=i,\\ r_\ell^{c_{k,\ell}d_{j,\ell}^{-1}}\cdot\omega_{k,\ell}^{-1} & \text{otherwise.}\end{cases}$$

$$B_{k,\ell}=\begin{cases}r_\ell\cdot\xi_{k,\ell}^{-1} & \text{if } k=j,\\ r_\ell^{d_{k,\ell}d_{j,\ell}^{-1}}\cdot\xi_{k,\ell}^{-1} & \text{otherwise.}\end{cases}$$

2. If $b_{i,\ell}\neq 0$, for some i, let

$$c_{j,\ell}=x_{j,\ell}b_{i,\ell}-y_{i,\ell}a_{j,\ell},\ \text{for all } j.$$

$$d_{j,\ell}=\begin{cases}y_{j,\ell}b_{i,\ell}-y_{i,\ell}b_{j,\ell}, & \text{for } j\neq i,\\ 0, & \text{if } j=i.\end{cases}$$

Since $(a_{1,\ell},\ldots,a_{n,\ell},b_{1,\ell},\ldots,b_{n,\ell})$ and $(x_{1,\ell},\ldots,x_{n,\ell},y_{1,\ell},\ldots,y_{n,\ell})$ are not multiples of each other, at least one of $c_{j,\ell}$ and $d_{j,\ell}$ is nonzero.

(a) If $d_{j,\ell} \neq 0$, for some $j \neq i$, let

$$A_{k,\ell} = r_\ell^{c_{k,\ell} d_{j,\ell}^{-1}} \cdot \omega_{k,\ell}^{-1}, \text{ for all } k.$$

$$B_{k,\ell} = \begin{cases} \xi_{k,\ell}^{-1} & \text{if } k = i, \\ r_\ell \cdot \xi_{k,\ell}^{-1} & \text{if } k = j, \\ r_\ell^{d_{k,\ell} d_{j,\ell}^{-1}} \cdot \xi_{k,\ell}^{-1} & \text{otherwise.} \end{cases}$$

(b) If $c_{j,\ell} \neq 0$, for some j (possibly $j = i$), let

$$A_{k,\ell} = \begin{cases} r_\ell \cdot \omega_{k,\ell}^{-1} & \text{if } k = j, \\ r_\ell^{c_{k,\ell} c_{j,\ell}^{-1}} \cdot \omega_{k,\ell}^{-1} & \text{otherwise.} \end{cases}$$

$$B_{k,\ell} = \begin{cases} \xi_{k,\ell}^{-1} & \text{if } k = i, \\ r_\ell^{d_{k,\ell} c_{j,\ell}^{-1}} \cdot \xi_{k,\ell}^{-1} & \text{otherwise.} \end{cases}$$

Let $R = \prod_{i,\ell} g_i^{-1}(\lambda_\ell)$. We would like to construct a prime $\alpha\mathcal{O}_L$ of $\mathcal{O}_L$ with $\alpha \equiv g_i^{-1}(A_{i,\ell})$ (mod $g_i^{-1}(\lambda_\ell)$), for all i and ℓ. Since the ideals $g_i^{-1}(\lambda_\ell)\mathcal{O}_L$ are pairwise coprime, the Chinese remainder theorem tells us that constructing such an element α is equivalent to constructing an element that satisfies a specific congruence modulo $R\mathcal{O}_L$, say $\alpha \equiv r_1 \pmod{R}$, compatible with $\alpha \equiv g_i^{-1}(A_{i,\ell}) \pmod{g_i^{-1}(\lambda_\ell)}$. Similarly, to construct a prime $\beta\mathcal{O}_L$ of $\mathcal{O}_L$ with $\beta \equiv g_i^{-1}(B_{i,\ell}) \pmod{g_i^{-1}(\lambda_\ell)}$, it is enough to construct a prime $\beta\mathcal{O}_L$ with a specific compatible congruence modulo $R\mathcal{O}_L$, say $\beta \equiv r_2 \pmod{R}$. Use the existence theorem of class field theory to construct an abelian extension whose Galois group is in a natural correspondence with the ray classes modulo $R\mathcal{O}_L$. Use Lemma 2.3.2 with $M = L$ again to find two primes

$\alpha\mathcal{O}_L$ and $\beta\mathcal{O}_L$ of $\mathcal{O}_L$ that split completely in $L^{\mathrm{ur},p}/L$, are prime to p, and satisfy:

$$\alpha \mod U(L)^p = -P_V(\nu_1) + \sum_{W\neq V} P_W\left(\sum_{j=1}^{d}(1+\sigma_j)q_{Td+j}\right)$$

and

$$\beta \mod U(L)^p = -P_V(\nu_2) + \sum_{W\neq V} P_W\left(\sum_{j=1}^{d}(1+\sigma_j)q_{(T+1)d+j}\right)$$

in $R(L)$, and

$$\alpha \equiv r_1 \pmod{R},$$
$$\beta \equiv r_2 \pmod{R}.$$

Observe that while taking projections $P_V(\nu_1)$ and $P_V(\nu_2)$ modifies the exponents of the primes $g(\lambda_\ell)$ in ν_1 and ν_2, those exponents still appear as the exponents of some other primes. In other words, if $(a_1,\ldots,a_n,b_1,\ldots,b_n)$ generates a $\mathbb{Z}/p\mathbb{Z}$ subgroup of $(\mathbb{Z}/p\mathbb{Z})^{2n}$, then there is a prime $g_i(\lambda_\ell)$ such that the the exponents of $g_1^{-1}(g_i(\lambda_\ell)), g_2^{-1}(g_i(\lambda_\ell)),\ldots,g_n^{-1}(g_i(\lambda_\ell))$ in ν_1 are $a_1,\ldots,a_n$ and the exponents of $g_1^{-1}(g_i(\lambda_\ell)), g_2^{-1}(g_i(\lambda_\ell)),\ldots,g_n^{-1}(g_i(\lambda_\ell))$ in ν_2 are $b_1,\ldots,b_n$.

Note that $L^\times/L^{\times p}$ is an $\mathbb{F}_p[\Phi]$-module, so we can consider the projections of $\nu_1\alpha$ and $\nu_2\beta$ to the V-eigenspace. Construct L_1 to be the Galois closure of $L(\sqrt[p]{P_V(\nu_1\alpha)})$ over K, and L_2 to be the Galois closure of $L(\sqrt[p]{P_V(\nu_2\beta)})$ over K. Then $\mathrm{Gal}(L_1/K)\cong\mathrm{Gal}(L_2/K)\cong V\rtimes\Phi$. Moreover, since $P_V(\nu_1\alpha)=0$ in $R(L)$, every prime lying over p in L splits completely in L_1/L. The same holds true for L_2/L. Consider their compositum $\tilde{L}=L_1.L_2$ and let $\tilde{M}=\tilde{L}.L^{\mathrm{ur},p}$. We claim that:

(i) The extension $\tilde{M}/L^{\mathrm{ur},p}$ is unramified at p.

(ii) Recall that $g(\alpha)$, $g(\beta)$, $g(\lambda_i)$ split completely in $L^{\mathrm{ur},p}/L$ by construction, for all $g\in\Phi$

and $1 \leq i \leq T$. Let $\tilde{S}$ be the set of primes of $L^{\mathrm{ur},p}$ lying above these primes. Then $\tilde{M}/L^{\mathrm{ur},p}$ is the maximal elementary abelian p-extension of $L^{\mathrm{ur},p}$ which is unramified outside $\tilde{S}$.

(iii) All the $(\mathbb{Z}/p\mathbb{Z})^2$-subgroups of $\mathrm{Gal}(\tilde{M}/L^{\mathrm{ur},p})$ appear as decomposition groups of some prime in $L^{\mathrm{ur},p}$ lying over $g(\lambda_i)$, for $g \in \Phi$ and $1 \leq i \leq T$.

Consider $P_V(\nu_1\alpha)$ in $R(L)$. By construction, $P_V(\nu_1\alpha) = 0$ in $R(L)$, so it must remain trivial in $R'(L)$. Similarly, $P_V(\nu_2\beta) = 0$ in $R'(L)$. It implies that L_1/L and L_2/L are unramified at p, and thus $\tilde{L}/L$ is unramified at p. Combine this with the fact that $L^{\mathrm{ur},p}/L$ is unramified everywhere to conclude that $\tilde{M} = \tilde{L}.L^{\mathrm{ur},p}/L^{\mathrm{ur},p}$ is unramified at p, proving (i).

Now, let $S = \{g(\alpha), g(\beta), g(\lambda_i) \mid g \in \Phi, 1 \leq i \leq T\}$. We claim that in order to prove (ii), it is enough to prove that $\tilde{L}/L$ is the maximal elementary abelian p-extension of L unramified outside S. To this end, assume that $\tilde{L}/L$ is such an extension. By construction, it follows that $\tilde{M}/L^{\mathrm{ur},p}$ is an elementary abelian p-extension unramified outside the primes of $L^{\mathrm{ur},p}$ that lie above S, i.e. $\tilde{M}/L^{\mathrm{ur},p}$ is unramified outside $\tilde{S}$. Moreover, since all the primes of S split completely in $L^{\mathrm{ur},p}/L$ and $\tilde{L}/L$ is maximal, the extension $\tilde{M}/L^{\mathrm{ur},p}$ must also be maximal.

We claim that $\tilde{L}/L$ is the maximal elementary abelian p-extension of L that is unramified outside S. To this end, consider an elementary abelian p-extension of L unramified outside S, $L(\sqrt[p]{\gamma})/L$, for some $\gamma \in L^\times/L^{\times p}$. We would like to prove that $L(\sqrt[p]{\gamma}) \subset \tilde{L}$. By definition of $L(\sqrt[p]{\gamma})$, it follows that:

$$\gamma \equiv \eta \cdot \prod_{i=1}^{T} \prod_{g \in \Phi} g(\lambda_i)^{c_{g,i}} \prod_{g \in \Phi} g(\alpha)^{a_g} \prod_{g \in \Phi} g(\beta)^{b_g} \mod L^{\times p},$$

for some $\eta \in \mathcal{O}_L^\times$ and $a_g, b_g, c_{g,i} \in \mathbb{F}_p$, for $1 \leq i \leq T$ and $g \in \Phi$. Since $L(\sqrt[p]{\gamma})/L$ is unramified at p, it follows that $\gamma = 0$ in $R'(L)$, so $\gamma \in N^G$. Thus $P_W(\gamma) = 0 \in R(L)$, for all W, which in turn means that $P_W(\gamma) = 0 \in R'(L)$. From construction, $g(\lambda_i), g(\alpha), g(\beta) \in Q^G \subset R'(L)$.

Moreover, since $\eta \in \mathcal{O}_L^\times \otimes \mathbb{F}_p$, and $\mathcal{O}_L^\times \otimes \mathbb{F}_p$ intersects Q^G and N^G trivially, it follows that $\eta = 0$ in $R'(L)$, so $\eta \in \mathcal{O}_L^{\times p}$, since η is a global unit.

On the one hand, consider $P_W(\gamma)$ in $R(L)$, for $W \neq V$ (note the switch from multiplicative notation to additive notation) :

$$\begin{aligned} 0 = P_W(\gamma) = &\sum_{i=1}^{T} \sum_{g \in \Phi} \left(\sum_{h \in \Phi} c_{gh^{-1},i} \cdot n_{h,W} g(\lambda_i) \right) \\ &+ \sum_{g \in \Phi} \left(\sum_{h \in \Phi} a_{gh^{-1}} \cdot n_{h,W} g(\alpha) \right) \\ &+ \sum_{g \in \Phi} \left(\sum_{h \in \Phi} b_{gh^{-1}} \cdot n_{h,W} g(\beta) \right) \end{aligned}$$

By construction, λ_i, α, β and their conjugates are all linearly independent in Q^G, so it follows that their coefficients have to be 0:

$$\begin{aligned} \sum_{h \in \Phi} n_{h,W} \cdot c_{gh^{-1},i} &= 0, \\ \sum_{h \in \Phi} n_{h,W} \cdot a_{gh^{-1}} &= 0, \\ \sum_{h \in \Phi} n_{h,W} \cdot b_{gh^{-1}} &= 0, \end{aligned}$$

for all $1 \leq i \leq T$ and $g \in \Phi$.

On the other hand, recall that $P_V(\nu_1 \alpha) = 0$ and $P_V(\nu_2 \beta) = 0$ in $R(L)$. Moreover, recall that

$$\nu_1 = \prod_{i=1}^{T} \prod_{g \in \Phi} g(\lambda_i)^{s_{g,i}} \quad \text{and} \quad \nu_2 = \prod_{i=1}^{T} \prod_{g \in \Phi} g(\lambda_i)^{t_{g,i}}.$$

Consider $P_V(\gamma)$ in $R(L)$:

$$\begin{aligned} 0 = P_V(\gamma) &= \sum_{i=1}^{T} \sum_{g\in\Phi} c_{g,i} P_V(g(\lambda_i)) + \sum_{g\in\Phi} a_g P_V(g(\alpha)) + \sum_{g\in\Phi} b_g P_V(g(\beta)) \\ &= \sum_{i=1}^{T} \sum_{g\in\Phi} c_{g,i} P_V(g(\lambda_i)) - \sum_{g\in\Phi} a_g P_V(g(\nu_1)) - \sum_{g\in\Phi} b_g P_V(g(\nu_2)) \\ &= \sum_{i=1}^{T} \sum_{g\in\Phi} \left(\sum_{h\in\Phi} n_{h,V} \left(c_{gh^{-1},i} - \sum_{\tau\in\Phi} (b_{g\tau^{-1}} t_{h^{-1}\tau,i} + a_{g\tau^{-1}} s_{h^{-1}\tau,i}) \right) \right) g(\lambda_i). \end{aligned}$$

Using the same argument as above, we must have that:

$$\sum_{h\in\Phi} n_{h,V} (c_{gh^{-1},i} - \sum_{\tau\in\Phi} (b_{g\tau^{-1}} t_{h^{-1}\tau,i} + a_{g\tau^{-1}} s_{h^{-1}\tau,i})) = 0,$$

for all $1 \leq i \leq T$ and all $g \in \Phi$.

Finally, putting these things together, we obtain that:

$$\gamma \equiv \prod_{g\in\Phi} g(P_V(\nu_1\alpha))^{a_g} \prod_{g\in\Phi} g(P_V(\nu_2\beta))^{b_g} \mod L^{\times p},$$

meaning that $L(\sqrt[p]{\gamma}) \subset \tilde{L}$, which proves the maximality of $\tilde{L}$, and concludes the proof of (ii).

Finally, in order to prove (iii) for $\tilde{M}/L^{\mathrm{ur},p}$, we observe that it is enough to prove it for $\tilde{L}/L$. This is true since all the elements $g(\lambda_i)$ split completely in $L^{\mathrm{ur},p}/L$, for all $g \in \Phi$ and $1 \leq i \leq T$, and $\mathrm{Gal}(\tilde{M}/L^{\mathrm{ur},p}) \cong \mathrm{Gal}(\tilde{L}/L)$. The following short lemma proves this statement for $\tilde{L}/L$.

Lemma 3.2.1. *All the $(\mathbb{Z}/p\mathbb{Z})^2$-subgroups of $\mathrm{Gal}(\tilde{L}/L)$ appear as decomposition subgroups of some $g_i(\lambda_\ell)$, for $1 \leq \ell \leq T$ and $i = i(\ell)$.*

Proof. Take a $(\mathbb{Z}/p\mathbb{Z})^2$-subgroup H of $\mathrm{Gal}(\tilde{L}/L) \cong (\mathbb{Z}/p\mathbb{Z})^{2n}$; note that there are $T = \frac{(p^{2n}-1)(p^{2n}-p)}{(p^2-1)(p^2-p)}$ of them. Choose generators $(a_1, \ldots, a_n, b_1, \ldots, b_n)$ and $(x_1, \ldots, x_n, y_1, \ldots, y_n)$

of H with $(a_1, \ldots, a_n, b_1, \ldots, b_n) \neq 0$, $(x_1, \ldots, x_n, y_1, \ldots, y_n) \neq 0$, and $(a_1, \ldots, a_n, b_1, \ldots, b_n)$ and $(x_1, \ldots, x_n, y_1, \ldots, y_n)$ are not multiples of each other. Moreover, from the above discussion, we can choose these generators in such a way that there exists a prime $\lambda = g_i(\lambda_\ell)$ (for some $g_i \in \Phi$ and $1 \leq \ell \leq T$) such that the exponents of $g_1^{-1}(\lambda), g_2^{-1}(\lambda), \ldots, g_n^{-1}(\lambda)$ are $a_1, \ldots, a_n$ in ν_1, and $b_1, \ldots, b_n$ in ν_2, respectively.

Let L_λ be the completion of L at the prime λ. Consider any prime of $\tilde{L}$ above λ and take the completion of $\tilde{L}$ at that prime. By abuse of notation, denote this completion by $\tilde{L}_\lambda$. Let π be a uniformizer of L_λ. After relabelling, if necessary, we can assume that $\tilde{L}_\lambda = L_\lambda(\sqrt[p]{\pi^{a_1}\omega_1 g_1(\alpha)}, \ldots, \sqrt[p]{\pi^{a_n}\omega_n g_n(\alpha)}, \sqrt[p]{\pi^{b_1}\xi_1 g_1(\beta)}, \ldots, \sqrt[p]{\pi^{b_n}\xi_n g_n(\beta)})$, where ω_i and ξ_i are defined above. We know that the inertia subgroup is generated by $(a_1, \ldots, a_n, b_1, \ldots, b_n)$. Consider the fixed field of inertia. If $a_i \neq 0$ for some i, then $\sqrt[p]{\frac{\omega_j^{a_i} g_j(\alpha)^{a_i}}{\omega_i^{a_j} g_i(\alpha)^{a_j}}}$ is an element inside the fixed field of inertia, for all $j \neq i$. If, on the other hand, $b_i \neq 0$ for some i, then $\sqrt[p]{\frac{\xi_j^{b_i} g_j(\beta)^{b_i}}{\xi_i^{b_j} g_i(\beta)^{b_j}}}$ is an element inside the fixed field of inertia, for all $j \neq i$. Let c_j, d_j, and A_k, B_k be the quantities constructed earlier in this section. Using this construction and the fact that that the prime λ satisfies

$$\alpha \equiv g_j^{-1}(A_j) \pmod{g_j^{-1}(\lambda)},$$
$$\beta \equiv g_j^{-1}(B_j) \pmod{g_j^{-1}(\lambda)},$$

for all $1 \leq j \leq n$, we observe that at least one of the quantities $\frac{\omega_j^{a_i} g_j(\alpha)^{a_i}}{\omega_i^{a_j} g_i(\alpha)^{a_j}}$ and $\frac{\xi_j^{b_i} g_j(\beta)^{b_i}}{\xi_i^{b_j} g_i(\beta)^{b_j}}$ is not a p-power modulo $\lambda\mathcal{O}_L$ (by construction of the element $r = r_\ell$). It follows that the fixed field of inertia is nontrivial.

Now, consider the fixed field of H. Again, using the definitions of the primes λ, α, β, the fixed field of this will be trivial.

Since the fixed field of $(a_1, \ldots, a_n, b_1, \ldots, b_n) \subset H$ is nontrivial and the fixed field of H is trivial, it follows that H is isomorphic to the decomposition subgroup of λ. Since H was

chosen arbitrarily, the conclusion follows. □

We claim that the extension $\tilde{M}/L^{\mathrm{ur},p}$ satisfies the conditions of Lemma 2.3.3, with $\tilde{S}$ instead of S. We know that $(L^{\mathrm{ur},p})^{\mathrm{ur},p} = L^{\mathrm{ur},p}$ and we have just proved that $\tilde{M}$ is the maximal elementary abelian p-extension of $L^{\mathrm{ur},p}$ unramified outside $\tilde{S}$, so the only thing left to prove is that the following map is surjective:

$$\bigoplus_v H_2(D_v, \mathbb{Z}) \to H_2(\mathrm{Gal}(\tilde{M}/L^{\mathrm{ur},p}), \mathbb{Z}),$$

where the sum is over all the primes of $L^{\mathrm{ur},p}$. The key fact used here is that if G is a finite abelian group, then the homology group $H_2(G, \mathbb{Z})$ is isomorphic to the second exterior power of G, $\bigwedge^2(G)$ ([Raz77, Lemma 5]). Recall that $\mathrm{Gal}(\tilde{M}/L^{\mathrm{ur},p}) \cong \mathrm{Gal}(\tilde{L}/L) \cong (\mathbb{Z}/p\mathbb{Z})^{2n}$; assume that $\mathrm{Gal}(\tilde{M}/L^{\mathrm{ur},p})$ is generated by $\{\tau_1, \tau_2, \ldots, \tau_{2n}\}$. Consider the $(\mathbb{Z}/p\mathbb{Z})^2$-subgroups of $\mathrm{Gal}(\tilde{M}/L^{\mathrm{ur},p})$ generated by pairs of two elements in $\{\tau_1, \ldots, \tau_{2n}\}$. There are $n(2n-1)$ of them; call them $A_1, A_2, \ldots, A_{n(2n-1)}$. In particular, $A_{k+j} = \langle \tau_i, \tau_{i+j} \rangle$, where i ranges from 1 to $2n-1$, $k = 2n(i-1) - \frac{(i-1)i}{2}$, and $1 \leq j \leq 2n-i$.

Note that $T = \frac{(p^{2n}-1)(p^{2n}-p)}{(p^2-1)(p^2-p)} \geq n(2n-1)$, for all primes p. From the fact that the decomposition subgroups D_v exhaust the $(\mathbb{Z}/p\mathbb{Z})^2$-subgroups of $\mathrm{Gal}(\tilde{M}/L^{\mathrm{ur},p})$, as v ranges over all the primes in $\tilde{S}$, it follows that there are primes $v_i \in \tilde{S}$ such that $D_{v_i} \cong A_i$, for all $1 \leq i \leq n(2n-1)$. Note that these primes are primes above $g(\lambda_j)$. Consider the following intersections:

$$\begin{aligned}
B_1 &= D_{v_1} \cap D_{v_2} \cap \cdots \cap D_{v_{2n-1}} \cong \langle \tau_1 \rangle \cong \mathbb{Z}/p\mathbb{Z} \\
B_2 &= D_{v_1} \cap D_{v_{2n}} \cap \cdots \cap D_{v_{4n-3}} \cong \langle \tau_2 \rangle \cong \mathbb{Z}/p\mathbb{Z} \\
&\cdots \\
B_{2n} &= D_{v_{2n-1}} \cap D_{v_{4n-3}} \cap \cdots \cap D_{v_{n(2n-1)}} \cong \langle \tau_{2n} \rangle \cong \mathbb{Z}/p\mathbb{Z}.
\end{aligned}$$

The groups B_i span the group $\mathrm{Gal}(\tilde{M}/L^{\mathrm{ur},p})$, so there exists a basis $\{x_1, \dots x_{2n}\}$ of $\mathrm{Gal}(\tilde{M}/L^{\mathrm{ur},p})$ such that $x_i \in B_i$. Now,

$$x_1, x_2 \in D_{v_1} \Rightarrow x_1 \wedge x_2 \in \bigwedge^2 D_{v_1}$$
$$x_1, x_3 \in D_{v_2} \Rightarrow x_1 \wedge x_3 \in \bigwedge^2 D_{v_2}$$
$$\dots$$
$$x_{2n-1}, x_{2n} \in D_{v_{n(2n-1)}} \Rightarrow x_{2n-1} \wedge x_{2n} \in \bigwedge^2 D_{v_{n(2n-1)}},$$

which implies that $\langle x_i \wedge x_j \mid i < j \rangle \subset \bigoplus \bigwedge^2 D_{v_i}$, where the sum is over all v_i with $D_{v_i} \cong A_i$, for $1 \leq i \leq n(2n-1)$. On the other hand, $\langle x_i \wedge x_j \mid i < j \rangle$ spans $\bigwedge^2 \mathrm{Gal}(\tilde{M}/L^{\mathrm{ur},p})$, which implies that $\bigwedge^2 \mathrm{Gal}(\tilde{M}/L^{\mathrm{ur},p}) \subset \bigoplus \bigwedge^2 D_{v_i} \subset \bigoplus \bigwedge^2 D_v$, so we must have equality. Thus, the map in Lemma 2.3.3 is surjective, proving that $(\tilde{M})^{\mathrm{ur},p} = \tilde{M}$.

Recall that L_1 is the Galois closure of $L(\sqrt[p]{P_V(\nu_1\alpha)})$ over K and L_2 is the Galois closure of $L(\sqrt[p]{P_V(\nu_2\beta)})$ over K. Let $M_1 = L_1.L^{\mathrm{ur},p}$ and $M_2 = L_2.L^{\mathrm{ur},p}$. Then $\tilde{M} = M_1.M_2$. Note that $\mathrm{Gal}(M_1/K) \cong \mathrm{Gal}(M_2/K) \cong V \rtimes \Gamma \cong \Gamma'$, by the discussion preceding Proposition 2.2.5. Let L' be the Galois closure of $L(\sqrt[p]{P_V(\nu_1\alpha)P_V(\nu_2\beta)^{-1}})$ over K. We would like to show the existence of an extension K'/K satisfying Theorem 3.0.2. Since $\mathrm{Gal}(L'/L) \cong V$ and $\mathrm{Gal}(L'/K) \cong V \rtimes \Phi$ by construction, we have the following exact sequence:

$$1 \to \mathrm{Gal}(L'/L) \to \mathrm{Gal}(L'/K) \to \mathrm{Gal}(L/K) \to 1.$$

Recall that V is a p-group and Φ is a group of order prime to p, so by the Schur-Zassenhaus Theorem this sequence splits, and we can view $\mathrm{Gal}(L/K) = \Phi$ as a subgroup of $\mathrm{Gal}(L'/K)$. Let $K' = L'^{\Phi}$. The extension L'/K' is Galois and has Galois group Φ. Moreover, $L \subset L'$ and $K \subset K'$. By construction, K'/K and M_1/K are linearly disjoint, and $M_1.K' = M_1.L' = \tilde{M}$,

so $\mathrm{Gal}(\tilde{M}/K') \cong \mathrm{Gal}(M_1/K) \cong \Gamma'$. We claim that $(L')^{\mathrm{ur},p} = \tilde{M}$. Since $\tilde{M}$ is an unramified p-extension of $L^{\mathrm{ur},p}.L'$ and $L^{\mathrm{ur},p}.L'$ is an unramified p-extension of L', it follows that $\tilde{M} \subset (L')^{\mathrm{ur},p}$. Combining this with the fact that $(\tilde{M})^{\mathrm{ur},p} = \tilde{M}$, we conclude that $\tilde{M} = (L')^{\mathrm{ur},p}$. Moreover, every prime of K' lying over p splits completely in $\tilde{M}$. To finish the proof in the case of a split extension, we have to prove that $(L')^{\mathrm{ur},p}/K'$ satisfies property **P**. Firstly, we claim that L'/K' satisfies property **P**. Since $\mathrm{Gal}(L'/K') \cong \mathrm{Gal}(L/K) \cong \Phi$ has order prime to p, and K'/K is a p-extension, this argument follows in the same manner as the one at the end of the proof of Lemma 3.1.1, and will be omitted. Now, from Lemma 2.2.4, it follows that $(L')^{\mathrm{ur},p}/K'$ satisfies property **P**, finishing the proof.

If the extension

$$1 \to V \to \Gamma' \to \Gamma \to 1$$

is not split, we cannot work over L anymore. However, the proof is similar. We begin by proving the following lemma, which is a variation of Lemma 6 in [Oza11]. In fact, we can recover Ozaki's Lemma for regular primes from the following result by taking $\Phi = 1$ and $V = \mathbb{Z}/p\mathbb{Z}$. While the proof is similar to the proof of Lemma 4 in the first version of [Oza11], our proof requires several extra steps. The difficulty of the proof in our case comes from the $\mathbb{F}_p$-dimension of V (which in Ozaki's case is taken to be 1) and the action of Φ on V (which in Ozaki's case is trivial). This result allows us to construct a wildly ramified solution to the embedding problem. We will then use this solution, combined with a split extension, to construct an unramified solution to the embedding problem. Let $\Phi, G, G', \Gamma, \Gamma', V$ be the groups defined in Theorem 3.0.2.

Proposition 3.2.2. *Let L/K be a Galois extension with Galois group Φ. Assume that the Galois group $\mathrm{Gal}(L^{ur,p}/K) \cong \Gamma = G \rtimes \Phi$. Then, for any group extension*

$$1 \to V \to \Gamma' \to \Gamma \to 1,$$

there exists a finite extension K'/K such that if $L' = L.K'$, then

1. *$(L')^{ur,p} = L^{ur,p}.L'$ and $(L')^{ur,p} = L^{ur,p}.K'$; hence $\mathrm{Gal}((L')^{ur,p}/K') \cong \mathrm{Gal}(L^{ur,p}/K)$ and every prime of K' lying over p splits completely in $(L')^{ur,p}$.*

2. *There exist global units $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \mathcal{O}^{\times}_{(L')^{ur,p}}$ ($n = \dim_{\mathbb{F}_p} V$) such that the field extension $(L')^{ur,p}(\sqrt[p]{\varepsilon_1}, \ldots, \sqrt[p]{\varepsilon_n})/K'$ is Galois with Galois group isomorphic to Γ'.*

Proof. By Proposition 2.2.5, there exists a Galois extension M/K containing $L^{\mathrm{ur},p}$ such that $\mathrm{Gal}(M/K) \cong \Gamma'$. Note that this extension M is just a solution to the embedding problem; in particular, it is not an unramified extension. Let $\alpha_1, \ldots, \alpha_n$ be the Kummer generators of $M/L^{\mathrm{ur},p}$, so $M = L^{\mathrm{ur},p}(\sqrt[p]{\alpha_1}, \ldots, \sqrt[p]{\alpha_n})$. Since $L \subset L^{\mathrm{ur},p} \subset M$ and L/K is Galois, the extension M/L must be Galois, so $(\alpha_i \mod (L^{\mathrm{ur},p})^{\times p}) \in ((L^{\mathrm{ur},p})^{\times}/(L^{\mathrm{ur},p})^{\times p})^G$, where $G = \mathrm{Gal}(L^{\mathrm{ur},p}/L)$. It follows that there are ideals $\mathfrak{A}_i$ of $\mathcal{O}_{L^{\mathrm{ur},p}}$ and $\mathfrak{a}_i$ of $\mathcal{O}_L$ such that $\alpha_i \mathcal{O}_{L^{\mathrm{ur},p}} = \mathfrak{A}_i^p \mathfrak{a}_i$. Let h be the class number of $L^{\mathrm{ur},p}$ and note that $(h, p) = 1$. Let A_i be an element of $L^{\mathrm{ur},p}$ such that $\mathfrak{A}_i^h = A_i \mathcal{O}_{L^{\mathrm{ur},p}}$. Then $\alpha_i^h \mathcal{O}_{L^{\mathrm{ur},p}} = \mathfrak{A}_i^{ph} \mathfrak{a}_i^h = A_i^p \mathfrak{a}_i^h$. Let $\mathfrak{a}_i' = \mathfrak{a}_i^h$ and $\alpha_i' = \alpha_i^h A_i^{-p}$. Then $\mathfrak{a}_i' = \alpha_i' \mathcal{O}_{L^{\mathrm{ur},p}}$ is an ideal of $\mathcal{O}_L$, and $M = L^{\mathrm{ur},p}(\sqrt[p]{\alpha_1}, \ldots, \sqrt[p]{\alpha_n}) = L^{\mathrm{ur},p}(\sqrt[p]{\alpha_1'}, \ldots, \sqrt[p]{\alpha_n'})$.

Let p^{e_i} be the exact power of p dividing the order of the ideal class $[\alpha_i']_L$. Then $[\alpha_i']_L^{p^{e_i}}$ has order prime to p. Let $e = \max e_i$, and note that $[\alpha_i']_L^{p^e}$ has order prime to p. By using Theorem 3.0.1 repeatedly we obtain an extension K'/K of degree p^e such that if $L' = L.K'$, then:

- $L' \cap L^{\mathrm{ur},p} = L$ and $K' \cap L^{\mathrm{ur},p} = K$,
- $(L')^{\mathrm{ur},p} = L^{\mathrm{ur},p}.L'$ and $(L')^{\mathrm{ur},p} = L^{\mathrm{ur},p}.K'$,
- $\mathrm{Gal}((L')^{\mathrm{ur},p}/K') \cong \Gamma$.

Consider the inclusion $L \subset L'$. Denote by $j\colon \mathrm{Cl}_L \to \mathrm{Cl}_{L'}$ the map induced on class groups, and by $N\colon \mathrm{Cl}_{L'} \to \mathrm{Cl}_L$ the norm map. Note that, by construction, we have an

isomorphism $\mathrm{Gal}((L')^{\mathrm{ur},p}/L')^{\mathrm{ab}} \cong G^{\mathrm{ab}}$. It follows that the order of the kernel of the norm map is prime to p. Observe that $N \circ j([\mathfrak{a}_i']_L) = [\mathfrak{a}_i']_L^{p^e}$. Combining these two facts, we conclude that the order of $j([\mathfrak{a}_i']_L)$ is prime to p in $\mathrm{Cl}_{L'}$. Let m_i be the order of $j([\mathfrak{a}_i']_L)$ in $\mathrm{Cl}_{L'}$, and let $m = \mathrm{lcm}(m_i)$; so m is prime to p. Let $\mathfrak{a}_i'^m = a_i'\mathcal{O}_{L'}$, for some $a_i' \in L'^{\times}$. Then $a_i'\mathcal{O}_{L'} = \alpha_i'^m\mathcal{O}_{(L')^{\mathrm{ur},p}}$. Thus, there exists $\varepsilon_i \in \mathcal{O}^{\times}_{(L')^{\mathrm{ur},p}}$ such that $\alpha_i'^m = a_i'\varepsilon_i$. Note that $(L')^{\mathrm{ur},p}(\sqrt[p]{\alpha_1'}, \ldots, \sqrt[p]{\alpha_n'}) = (L')^{\mathrm{ur},p}(\sqrt[p]{\alpha_1'^m}, \ldots, \sqrt[p]{\alpha_n'^m})$, so we can replace α_i' by $\alpha_i'^m$.

Recall that $\langle \alpha_i' \mod ((L')^{\mathrm{ur},p})^{\times p}\rangle \subset (((L')^{\mathrm{ur},p})^{\times}/((L')^{\mathrm{ur},p})^{\times p})^G$, as a subgroup. Since the extension $(L')^{\mathrm{ur},p}(\sqrt[p]{\alpha_1'}, \ldots, \sqrt[p]{\alpha_n'})/K'$ has Galois group Γ', it follows that the group Γ acts on $\langle \alpha_i' \mod ((L')^{\mathrm{ur},p})^{\times p}\rangle$. Then, as an $\mathbb{F}_p[\Gamma]$-representation, $\langle \alpha_i' \mod ((L')^{\mathrm{ur},p})^{\times p}\rangle$ is isomorphic to a copy of the projective cover of V. Let $\tilde{V}$ be the projective cover of V. Hence, the Galois group $\mathrm{Gal}((L')^{\mathrm{ur},p}(\sqrt[p]{\alpha_1'}, \ldots, \sqrt[p]{\alpha_n'})/K')$ is isomorphic to the Galois group $\mathrm{Gal}\left((L')^{\mathrm{ur},p}\left(\sqrt[p]{P_{\tilde{V}}(\alpha_1')}, \ldots, \sqrt[p]{P_{\tilde{V}}(\alpha_n')}\right)/K'\right)$, so we can replace α_i' by $P_{\tilde{V}}(\alpha_i') = P_{\tilde{V}}(a_i\varepsilon_i) = P_{\tilde{V}}(a_i) \cdot P_{\tilde{V}}(\varepsilon_i)$. Note that $P_{\tilde{V}}(a_i') = P_V(a_i')^{|G|}$, since $a_i' \in L'^{\times}$. Since $\langle P_V(a_i')\rangle$ is isomorphic to a subrepresentation of V in $L'^{\times}/L'^{\times p}$, and V is an irreducible $\mathbb{F}_p[\Phi]$-representation, either $\langle P_V(a_i')\rangle \cong V$ or $\langle P_V(a_i')\rangle = 1$. The latter implies that $P_V(a_i') = 1$, for all i, which in turn implies that $P_{\tilde{V}}(\alpha_i') = P_{\tilde{V}}(\varepsilon_i)$, which finishes the proof: the extension $(L')^{\mathrm{ur},p}(\sqrt[p]{P_V(\alpha_1')}, \ldots, \sqrt[p]{P_V(\alpha_n')})/K'$ is the desired one. On the other hand, the former implies that $\langle P_V(a_i')\rangle \cong V$, so $\mathrm{Gal}(L'(\sqrt[p]{P_V(a_1')}, \ldots \sqrt[p]{P_V(a_n')})/K') \cong V \rtimes \Phi$. Then, by Proposition 2.2.5, the Galois group of $(L')^{\mathrm{ur},p}(\sqrt[p]{P_V(a_1')}, \ldots \sqrt[p]{P_V(a_n')})/K'$ is isomorphic to $V \rtimes \Gamma$, which means that $\mathrm{Gal}((L')^{\mathrm{ur},p}(\sqrt[p]{P_V(\varepsilon_1)}, \ldots \sqrt[p]{P_V(\varepsilon_n)})/K') \cong \Gamma'$, which is what we wanted. □

We are finally ready to prove Theorem 3.0.2 in the case when the group extension $1 \to V \to \Gamma' \to \Gamma \to 1$ is not split. Assume that L/K is an extension with the usual properties. Use Proposition 3.2.2 to construct a wildly ramified solution $(L')^{\mathrm{ur},p}(\sqrt[p]{\varepsilon_1}, \ldots, \sqrt[p]{\varepsilon_n})/K'$ to the embedding problem. Note that from construction, it follows that $\langle \varepsilon_1, \ldots, \varepsilon_n\rangle \cong \langle \sigma(\varepsilon_1) \mid \sigma \in \Gamma\rangle$, as representations. Moreover, the new extension $(L')^{\mathrm{ur},p}(\sqrt[p]{\varepsilon_1}, \ldots, \sqrt[p]{\varepsilon_n})/K'$ satisfies

property **P** except possibly at the primes above p.

Just as before, construct T primes $\lambda_i\mathcal{O}_{L'}$ in L', where $T = \frac{(p^n-1)(p^n-p)}{(p^2-1)(p^2-p)}$, satisfying:

- $\lambda_i\mathcal{O}_{L'}$ splits completely in $(L')^{\mathrm{ur},p}/L'$,
- $N(\lambda_i) \equiv 1 \pmod{p}$,
- the primes of K' below λ_i split completely in L'/K',
- $\lambda_i \mod U(L')^p = \sum_{j=1}^{d}(1+\sigma_j)q_{(i-1)d+j}$ in $R(L')$.

Construct the quantities ν_1, ν_2, and the elements $A_{k,\ell}$ and $B_{k,\ell}$ (and r_1, r_2) in the same manner as above (here $1 \leq k \leq n$ and $1 \leq \ell \leq T$). Let $R = \prod_{i,\ell} g_i^{-1}(\lambda_\ell)$ as above. Construct two new primes $\alpha\mathcal{O}_{L'}$ and $\beta\mathcal{O}_{L'}$ that split completely in $(L')^{\mathrm{ur},p}/L'$, are prime to p and satisfy:

- $\alpha \equiv r_1 \pmod{R}$ and $\beta \equiv r_2 \pmod{R}$,
- $\alpha \mod U(L')^p = -\varepsilon_1 - P_V(\nu_1) + \sum_{W\neq V} P_W\left(\sum_{j=1}^{d}(1+\sigma_j)q_{Td+j}\right)$ in $R(L')$,
- $\beta \mod U(L')^p = -\varepsilon_1 - P_V(\nu_2) + \sum_{W\neq V} P_W\left(\sum_{j=1}^{d}(1+\sigma_j)q_{(T+1)d+j}\right)$ in $R(L')$.

Let L_1 be the Galois closure of $L'(\sqrt[p]{P_V(\nu_1\alpha)})$ over K'. Then $\mathrm{Gal}(L_1/K') = V \rtimes \Phi$. Define the field $M_1 = (L')^{\mathrm{ur},p}(\sqrt[p]{\varepsilon_1 P_V(\nu_1\alpha)}, \ldots, \sqrt[p]{\varepsilon_n g_n(P_V(\nu_1\alpha))})$, and use Proposition 2.2.5 and Proposition 3.2.2 to observe that the Galois group of M_1/K' is Γ'. Construct L_2 and M_2 in a similar manner. Let $\tilde{L}$ be the Galois closure of $L'(\sqrt[p]{P_V(\nu_1\alpha)P_V(\nu_2\beta)^{-1}})$ over K' and let $\tilde{M} = M_1.M_2$. Note that, by an argument identical to the one above, the extension $\tilde{M}$ is the maximal unramified p-extension of $\tilde{L}$. Just as in the previous case, we are in the following situation:

$$1 \to \mathrm{Gal}(\tilde{L}/L') \to \mathrm{Gal}(\tilde{L}/K') \to \mathrm{Gal}(L'/K') \to 1.$$

Using the Schur-Zassenhaus Theorem again, we can construct a field $\tilde{K} = \tilde{L}^{\Phi}$. Then, by construction, this new extension $\tilde{M}/\tilde{K}$ has Galois group Γ', $\tilde{M} = (\tilde{L})^{\mathrm{ur},p}$, $\mathrm{Gal}(\tilde{M}/\tilde{L}) = G'$. Moreover, property **P** is also satisfied, since there is no ramification at the prime p. This concludes the proof of Theorem 3.0.2.

CHAPTER 4

UNIVERSAL UNRAMIFIED DEFORMATION RINGS

In this chapter, we present an application of Theorem 1 in the field of deformation theory. This application provides a partial answer to Question 2.

Throughout this chapter, let p be a prime, E a number field and $\overline{\rho}\colon G_E \to \mathrm{GL}_2(\mathbb{F}_p)$ a continuous absolutely irreducible Galois representation. Moreover, assume that the image of this representation has order prime to p. If we consider the unramified lifts of such a representation, it is natural to ask:

Question 4. What possible rings R can occur as universal unramified deformation rings of an absolutely irreducible representation with image of order prime to p?

Using Boston's Strengthening [Bos99] of the Unramified Fontaine-Mazur Conjecture [FM95], together with the proof of [AC14, Proposition 10], we observe that the expectation is that the universal unramified deformation ring is a ring R admitting a map $R \twoheadrightarrow \mathbb{Z}_p$ with finite kernel I. We expect that there are no other restrictions on R and therefore have the following conjecture:

Conjecture 1. *Let R be any local ring admitting a surjection to $\mathbb{Z}_p$ with finite kernel, for $p \geq 5$. Then there exist a number field E and an absolutely irreducible residual representation $\overline{\rho}\colon G_E \to \mathrm{GL}_2(\mathbb{F}_p)$ such that R is isomorphic to the universal unramified deformation ring of $\overline{\rho}$.*

In what follows, we will prove that a ring R admitting a surjection to $\mathbb{Z}_p$ with finite kernel is isomorphic to the universal unramified deformation ring of a certain absolutely irreducible representation (if such a representation exists). Then, we will construct absolutely irreducible representations of this specific form for $p = 5$ and $p = 7$.

4.1 Finding the Universal Unramified Deformation Ring

Let R be a local ring admitting a surjection to $\mathbb{Z}_p$ with finite kernel I_R. Assume that there exist a number field E and an absolutely irreducible residual representation

$$\overline{\psi}\colon G_E \to \mathrm{GL}_2(\mathbb{F}_p),$$

whose image is $\tilde{\Phi}$, a group of order prime to p. Note that the projective image Φ of $\overline{\psi}$ can be A_4, S_4, S_5 or a dihedral group [Ser72, Proposition 16]. Since $\tilde{\Phi}$ has order prime to p, we can view it as a subgroup of $\mathbb{Z}_p$, so $\overline{\psi}$ lifts to $\mathrm{GL}_2(\mathbb{Z}_p)$. Let $\tilde{\Gamma}$ denote the inverse image of $\tilde{\Phi}$ inside $\mathrm{GL}_2(R)$; it lives inside a split exact sequence:

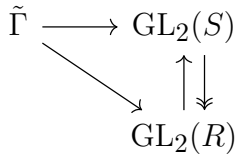
$$1 \to 1 + M_2(I_R) \to \tilde{\Gamma} \to \tilde{\Phi} \to 1.$$

Now, the group $\tilde{\Gamma}$ admits a natural residual representation via $\overline{\psi}$, call it $\overline{\rho}\colon G_E \to \tilde{\Gamma} \to \mathrm{GL}_2(\mathbb{F}_p)$. This representation is absolutely irreducible, so a universal deformation ring $R_{\overline{\rho}}$ exists (for more details, see Section 2.4). The aim of this section is to show that $R_{\overline{\rho}} \cong R$.

Note that $\tilde{\Gamma}$ admits a deformation to $\mathrm{GL}_2(R)$ by construction, so $R_{\overline{\rho}} \twoheadrightarrow R$. It follows that there exists an ideal $J \subset R_{\overline{\rho}}$ such that $R_{\overline{\rho}}/J \cong R$. Note that, by replacing $R_{\overline{\rho}}$ by $R_{\overline{\rho}}/J\mathfrak{m}_{R_{\overline{\rho}}}$, we can assume that J is finite. Here $\mathfrak{m}_{R_{\overline{\rho}}}$ is the maximal ideal of $R_{\overline{\rho}}$. It follows that the ring $R_{\overline{\rho}}$ admits a surjection onto $\mathbb{Z}_p$ with finite kernel. Therefore, to prove that R is universal, it is enough to prove that for every local ring S with the following properties:

- The ring S surjects onto $\mathbb{Z}_p$ with finite kernel I_S,
- $S \twoheadrightarrow R$,
- There is a lift $\tilde{\Gamma} \to \mathrm{GL}_2(S)$,

there exists a map $R \to S$ that makes the following diagram commute:



Throughout this section, let S be a local ring satisfying the three properties above. Since $S \twoheadrightarrow R$ and the ideals I_S and I_R are finite, it follows that there exists a finite ideal $J \subset S$ such that $S/J \cong R$.

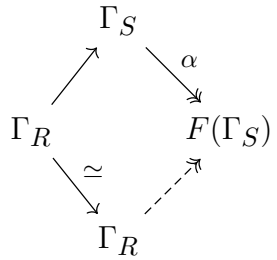
Before proving the existence of a section $R \to S$, let us introduce some notation. If A is a local ring and $I \subset A$ is an ideal, then:

- Let $\mathfrak{m}_A$ denote the maximal ideal of A.
- Let $\Gamma_I = 1 + \mathrm{M}_2(I)$.
- If the ideal $I = I_A$ is the kernel of a surjective homomorphism $A \twoheadrightarrow \mathbb{Z}_p$, then let $\Gamma_A = \Gamma_{I_A} = 1 + M_2(I_A)$.

We observe that Γ_J is not contained in the Frattini subgroup $[\Gamma_S, \Gamma_S]\Gamma_S^p$ of Γ_S:

Lemma 4.1.1. *Let S and R be two rings as above. The group Γ_J is not a subgroup of $[\Gamma_S, \Gamma_S]\Gamma_S^p$.*

Proof. Assume that $\Gamma_J \subset [\Gamma_S, \Gamma_S]\Gamma_S^p$. Recall that there exists a lift $\tilde{\Gamma} \to GL_2(S)$, and note that Γ_R is a normal, pro-p subgroup of $\tilde{\Gamma}$, by construction. It follows that, under the map $\tilde{\Gamma} \to \mathrm{GL}_2(S)$, the group Γ_R maps to Γ_S. Thus, we have the following diagram:



where $F(\Gamma_S) = \Gamma_S/[\Gamma_S, \Gamma_S]\Gamma_S^p$ is the Frattini quotient of Γ_S.

Since $\Gamma_J \subset [\Gamma_S, \Gamma_S]\Gamma_S^p = \ker \alpha$, it follows that α has to factor through Γ_R, which implies that $\Gamma_R \cong \Gamma_R \to F(\Gamma_S)$ must be surjective, so $\Gamma_R \to \Gamma_S \to F(\Gamma_S)$ must be surjective. Since $F(\Gamma_S)$ is the Frattini quotient of Γ_S, we obtain that $\Gamma_R \to \Gamma_S$ must be surjective, but this is impossible, since Γ_R has fewer elements than Γ_S. Thus, Γ_J is not contained in the Frattini subgroup $[\Gamma_S, \Gamma_S]\Gamma_S^p$ of Γ_S. □

The existence of a section $R \to S$ will be proved by induction on the length of the ideal I_S. Note that the kernel J is not necessarily an $\mathbb{F}_p$-vector space of dimension n. However, when it is an $\mathbb{F}_p$-vector space, we claim that $S \cong R[x_1, \ldots, x_n]/(x_i x_j, p x_i)$, for some $x_i \in S$. Before proving this claim, let us introduce a technical lemma: when the $\mathbb{F}_p$-dimension of the kernel J is 1, then if the kernel on the level of cotangent spaces is nontrivial, there exists a section $R \to S$.

Lemma 4.1.2. *Let S and R be two local rings as above. Suppose that $\dim_{\mathbb{F}_p} J = 1$ and suppose that there exists some $0 \neq x \in J$ such that x is sent to 0 under the map of cotangent spaces $\mathfrak{m}_S/(\mathfrak{m}_S^2, p) \to \mathfrak{m}_R/(\mathfrak{m}_R^2, p)$. Then there exists a subring $S' \subset S$ such that $S' \cong R$.*

Proof. Take generators $\overline{x_1}, \ldots, \overline{x_d}$ of $\mathfrak{m}_R/(\mathfrak{m}_R^2, p)$ and lift these generators to $\mathfrak{m}_S/(\mathfrak{m}_S^2, p)$ and then to S. Denote the lifts to S by $x_1, \ldots, x_d$. Consider the subring S' of S generated by these lifts.

Let $x \in J$ be a nonzero element that is sent to 0 under the map on cotangent spaces. We claim that $x \notin S'$. Suppose otherwise, so $x = a_0 + a_1 x_1 + \ldots a_d x_d + \alpha$, where $\alpha \in \mathfrak{m}_S^2$, $a_i \in \mathbb{Z}_p$. Since $x, x_i, \alpha \in \mathfrak{m}_S$, it follows that $a_0 \in \mathfrak{m}_S \cap \mathbb{Z}_p = (p)$. Recall that under the map

$$\mathfrak{m}_S/(\mathfrak{m}_S^2, p) \to \mathfrak{m}_R/(\mathfrak{m}_R^2, p),$$

$x = a_0 + \sum a_i x_i + \alpha = \sum a_i x_i$ (in $\mathfrak{m}_S/(\mathfrak{m}_S^2, p)$) is sent to 0. Since $\overline{x_i}$ generate $\mathfrak{m}_R/(\mathfrak{m}_R^2, p)$, this is true if and only if $a_i = 0 \in \mathfrak{m}_R/(\mathfrak{m}_R^2, p)$, for all i, which is true if and only if $a_i \in \mathbb{Z}_p \cap (\mathfrak{m}_R^2, p) = (p)$. Thus, $x \in (\mathfrak{m}_S^2, p)$, which is a contradiction. So $x \notin S'$, which

implies that $S' \hookrightarrow R$.

The inclusion $S' \hookrightarrow R$ induces an isomorphism on cotangent spaces. In particular, the map on cotangent spaces is surjective, which implies that the original map must be surjective [Sch68, Lemma 1.1]. Thus, the map from S' to R must be an isomorphism. □

We can now prove the statement in the case when the kernel J is an $\mathbb{F}_p$-vector space.

Lemma 4.1.3. *Let R and S be two local rings as above. Assume, moreover, that J is an $\mathbb{F}_p$-vector space of dimension n. Then there exist $x_i \in S$ such that $S \cong R[x_1, \ldots, x_n]/(x_i x_j, px_i)$.*

Proof. This will be proved by induction on $n = \dim_{\mathbb{F}_p} J$.

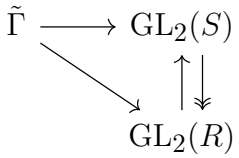
Base case: $n = 1$. By Lemma 4.1.1, the group Γ_J is not a subgroup of $[\Gamma_S, \Gamma_S]\Gamma_S^p$. Combining this with the fact that $[\Gamma_S, \Gamma_S]\Gamma_S^p = \Gamma_{(I_S^2, pI_S)}$, we observe that J is not a subset of (I_S^2, pI_S). So, there exists $x \in J$ such that $x \notin (I_S^2, pI_S)$. Moreover, $x \notin (\mathfrak{m}_S^2, p)$. Thus, under the map

$$\mathfrak{m}_S/(\mathfrak{m}_S^2, p) \to \mathfrak{m}_R/(\mathfrak{m}_R^2, p),$$

the nonzero element x is sent to 0. From Lemma 4.1.2, we know that there exists a subring $S' \subset S$ such that $S' \cong R$ and $x \notin S'$. Consider the map $S'[x] \to S$: it is a surjection and px, x^2 are elements of the kernel. Thus $S \cong S'[x]/(x^2, px) \cong R[x]/(x^2, px)$, which concludes the base case.

Inductive step: suppose that the result is true for $m < n$ and consider the case $n = \dim_{\mathbb{F}_p} J$. Suppose $J = (x_1, \ldots, x_n)$, for some $x_i \in S$. Let $S_1 = S/(x_1)$. Apply the base case to S, S_1 and (x_1) instead of S, R and J to obtain that $S \cong S_1[x_1]/(x_1^2, px_1)$. By construction, S_1 still surjects onto R with kernel $J_1 = J/(x_1)$. Note that $\dim_{\mathbb{F}_p} J_1 < n = \dim_{\mathbb{F}_p} J$. By induction, we know that $S_1 \cong R[x_2, \ldots x_n]/(x_i x_j, px_i)$, for some $x_2, \ldots, x_n \in S$. Putting these two things together, we obtain that $S \cong R[x_1, \ldots x_n]/(x_i x_j, px_i)$. □

We can finally prove that for two rings R, S as above, there exists a map $R \to S$ that makes the following diagram commute:



Proposition 4.1.4. *Let R and S be two local rings as above. Then there exists a splitting $R \to S$ that makes the diagram above commute.*

Proof. As previously mentioned, we will prove this result by induction on $\ell(S)$, where we define $\ell(S) = \ell(I_S)$ to be the length of the ideal I_S.

Base case: $\ell(S) = \ell(R) + 1$. Replacing S by $S/\mathfrak{m}_S J$, if necessary, we can assume that J is an $\mathbb{F}_p$-vector space. We can do this, because to find a lift to S, it is enough to find a lift to $S/\mathfrak{m}_S J$. Then the condition $\ell(S) = \ell(R) + 1$ translates to $\dim_{\mathbb{F}_p} J = 1$, and this follows from the base case in Lemma 4.1.3.

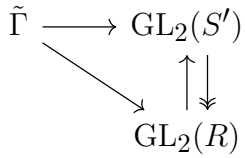
Inductive step: suppose that the statement is true for $\ell(S) < N$; we would like to prove that for $\ell(S) = N$ there exists a splitting $R \to S$ that makes the diagram commute. If $S \twoheadrightarrow R$ has kernel J, then consider

$$S \xrightarrow{\pi} S/\mathfrak{m}_S J \twoheadrightarrow S/J = R.$$

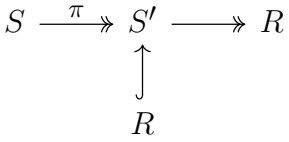
Let $S' = S/\mathfrak{m}_S J$. Then S' is a local $\mathbb{Z}_p$-algebra with maximal ideal $\mathfrak{m}_{S'} = \mathfrak{m}_S/\mathfrak{m}_S J$. Moreover, there is a surjection from S' to R with kernel $J' = J/\mathfrak{m}_S J$. This new local $\mathbb{Z}_p$-algebra has the following properties:

- $S'/J' = R$;
- $\mathfrak{m}_{S'} J = 0$;
- J' is a $S/\mathfrak{m}_S = \mathbb{F}_p$-vector space.

Thus, by Lemma 4.1.3, it follows that $S' \cong R[x_1, \ldots, x_n]/(x_i x_j, p x_i)$, for some elements $x_i \in S'$. So, there is a splitting $R \hookrightarrow S'$ that makes the following diagram commute:



We are in the following situation:



Let $S'' = \pi^{-1}(R) \subset S$. Then $\ell(S'') < \ell(S)$, so by induction there is a lift $R \to S''$. Then we can conclude that there is a lift

$$R \to S'' \to S,$$

where the first map comes from the inductive step and the second map comes from the definition of S''. Moreover, this lift makes our diagram commute, which concludes the proof. □

By taking $S = R_{\overline{\rho}}$, we conclude that there is a splitting $R \to R_{\overline{\rho}}$ corresponding to the surjection $R_{\overline{\rho}} \twoheadrightarrow R$. It follows that $R \cong R_{\overline{\rho}}$.

4.2 Existence of Residual Representations

We can now prove Theorem 2. Recall that at the beginning of the previous section, we assumed the existence of an absolutely irreducible residual representation $\overline{\psi}\colon G_E \to GL_2(\mathbb{F}_p)$, whose image is $\tilde{\Phi}$, a group of order prime to p. From this, we obtained a short exact sequence

$$1 \to G \to \tilde{\Gamma} \to \tilde{\Phi} \to 1,$$

and a residual representation $\overline{\rho}\colon \tilde{\Gamma} \to \mathrm{GL}_2(\mathbb{F}_p)$. We have already proved that R is the universal deformation ring of $\overline{\rho}$. In order to prove that R is the universal *unramified* deformation

ring of $\overline{\rho}$, we need to consider the unramified lifts of this representation. Note that the existence of an absolutely irreducible residual representation with image with order prime to p whose universal unramified deformation ring is isomorphic to R reduces to finding field extensions $M/L/K$ satisfying $\mathrm{Gal}(M/K) = \tilde{\Gamma}$ and M is the maximal unramified p-extension of L. We observe that the existence of such extensions is given by Theorem 1, under the assumption that there exists a $\tilde{\Phi}$-extension of $\mathbb{Q}(\zeta_p)$ with class number prime to p that satisfies property **P**.

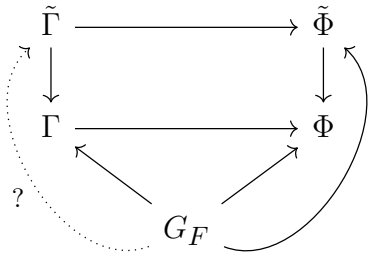
We claim that instead of working with a $\tilde{\Phi}$-extension with the desired properties, we can work with a Φ-extension, where Φ is the projective image of $\tilde{\Phi}$. To this end, consider the following exact sequence

$$1 \to G \to \tilde{\Gamma} \to \tilde{\Phi} \to 1$$

and its projective image

$$1 \to G \to \Gamma \to \Phi \to 1.$$

Note that if we have a lift $G_E \to \Gamma$, we are in the following situation:



To prove that there exists a lift $G_F \to \tilde{\Gamma}$, take two compatible set theoretic lifts. The centres $Z(\tilde{\Gamma})$ and $Z(\tilde{\Phi})$ are equal, so the 2-cocycles will be the same. Since any set theoretic lift to $\tilde{\Phi}$ is a homomorphism, it follows that the lift to $\tilde{\Gamma}$ must be a homomorphism, and we are done. Therefore, it is enough to construct Φ-extensions.

Recall that by [Ser72], we know that Φ is dihedral, A_4, S_4 or S_5. Let $\Phi = A_4$ and consider the Schur covering group $\tilde{\Phi} = \mathrm{SL}_2(\mathbb{F}_3)$ of A_4. Note that for $p \geq 5$, we have

inclusions $\Phi \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_p)$ and $\tilde{\Phi} \hookrightarrow \mathrm{GL}_2(\mathbb{F}_p)$.

To finish the proof of Theorem 2, we constructed extensions with the desired properties for $p = 5$ and $p = 7$ (see the two examples below) using GP/Pari and the Database of Number Fields `https://hobbes.la.asu.edu/NFDB/` ([JR14]).

Example. Let $p = 5$. Let $\Phi = A_4 \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_5)$ and $\tilde{\Phi} = \tilde{A_4} = \mathrm{SL}_2(\mathbb{F}_3) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_5)$. Let E be the compositum of $\mathbb{Q}(\zeta_5)$ with the field defined by

$$x^4 - x^3 + 2x^2 + 4x + 3$$

and let $\tilde{F_1}$ be the Galois closure of the field defined by the following polynomial over $\mathbb{Q}$:

$$x^8 - 2x^7 - 28x^6 + 25x^5 + 226x^4 + 70x^3 - 307x^2 - 121x + 1.$$

This field has an intermediate field F_1, which is the Galois closure of the field defined by

$$x^4 - x^3 - 22x^2 + 8x + 24.$$

Let $\tilde{F} = E.\tilde{F_1}$ and $F = E.F_1$. Then F is a subfield of $\tilde{F}$ and $\mathrm{Gal}(\tilde{F}/E) = \mathrm{SL}_2(\mathbb{F}_3) \twoheadrightarrow A_4 = \mathrm{Gal}(F/E)$. We used GP/Pari to show that both F/E and $\tilde{F}/E$ satisfy the conditions of Theorem 1. This concludes the proof for $p = 5$.

Example. Let $p = 7$. Let $\Phi = A_4 \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_7)$ and $\tilde{\Phi} = \tilde{A_4} = \mathrm{SL}_2(\mathbb{F}_3) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_7)$. Let E be the compositum of $\mathbb{Q}(\zeta_7)$ with the field defined by

$$x^3 - 3x - 1$$

and let $\tilde{F}_1$ be the Galois closure of the field defined by the following polynomial over $\mathbb{Q}$:

$$x^8 - 3x^7 - 3x^6 - x^5 - 34x^4 + 480x^3 + 451x^2 - 463x + 2686.$$

This field has an intermediate field F_1, which is the Galois closure of the field defined by

$$x^4 - x^3 - 16x^2 + 17x + 38.$$

Let $\tilde{F} = E.\tilde{F}_1$ and $F = E.F_1$. Then F is a subfield of $\tilde{F}$ and $\mathrm{Gal}(\tilde{F}/E) = \mathrm{SL}_2(\mathbb{F}_3) \twoheadrightarrow A_4 = \mathrm{Gal}(F/E)$. We used GP/Pari to show that both F/E and $\tilde{F}/E$ satisfy the conditions of Theorem 1. This concludes the proof for $p = 7$.

This concludes the proof of Theorem 2. Note that this proof does not rely on p until this last step, which is a purely computational one. For $p > 7$, the difficulty comes from the fact that computational tools like Pari and MAGMA have limitations when computing class numbers of high degree fields. As previously mentioned, we believe that Conjecture 1 holds, making this result true for all $p \geq 5$.

4.3 Murphy's Law for Galois Deformation Rings

Theorem 2 can be viewed through the lens of "Murphy's Law for moduli spaces", an idea introduced by Ravi Vakil in [Vak06]: all possible singularities occur inside deformation spaces. When considering Galois deformation rings, the analogue of this is to say that all possible local rings (that satisfy certain obvious conditions) occur as deformation rings. When considering unramified deformation rings, the expectation is that another class of rings appearing as unramified deformation rings is represented by finite artinian local rings. To prove this result for all such rings, one would have to also consider representations whose images have order divisible by p, requiring a modification of Theorems 1 and 2.

REFERENCES

[AC14] Patrick B. Allen and Frank Calegari. Finiteness of unramified deformation rings. *Algebra & Number Theory*, 8(9):2263–2272, 2014.

[Bos99] Nigel Boston. Some cases of the Fontaine-Mazur conjecture. II. *J. Number Theory*, 75(2):161–169, 1999.

[FM95] Jean-Marc Fontaine and Barry Mazur. Geometric Galois representations. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, volume I of *Ser. Number Theory*, pages 41–78. Int. Press, Cambridge, MA, 1995.

[GM99] Georges Gras and Adeline Munnier. Extensions cycliques T-totalement ramifiées. In *Théorie des nombres, Années 1996/97–1997/98*, Publ. Math. UFR Sci. Tech. Besançon, page 16. Univ. Franche-Comté, Besançon, 1999.

[Gra98] Georges Gras. Théorèmes de réflexion. *J. Théor. Nombres Bordeaux*, 10(2):399–499, 1998.

[GS64] E. S. Golod and I. R. Safarevich. On the class field tower. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28:261–272, 1964.

[HM17] Farshid Hajir and Christian Maire. Analytic lie extensions of number fields with cyclic fixed points and tame ramification. *arXiv:1710.09214*, 2017.

[HMR24a] Farshid Hajir, Christian Maire, and Ravi Ramakrishna. On Ozaki's theorem realizing prescribed p-groups as p-class tower groups. *Algebra Number Theory*, 18(4):771–786, 2024.

[HMR24b] Farshid Hajir, Christian Maire, and Ravi Ramakrishna. On tame $\mathbb{Z}/p\mathbb{Z}$-extensions with prescribed ramification. *Canad. Math. Bull.*, 67(1):40–48, 2024.

[Hoe68] Klaus Hoechsmann. Zum Einbettungsproblem. *J. Reine Angew. Math.*, 229:81–106, 1968.

[Ior23] Andreea Iorga. Murphy's law for Galois deformation rings. *arXiv:2310.07105*, 2023.

[Iwa56] Kenkichi Iwasawa. A note on the group of units of an algebraic number field. *J. Math. Pures Appl. (9)*, 35:189–192, 1956.

[JR14] John W. Jones and David P. Roberts. A database of number fields. *LMS J. Comput. Math.*, 17(1):595–618, 2014.

[Lam06] T. Y. Lam. *Serre's problem on projective modules*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006.

[Maz89] B. Mazur. Deforming Galois representations. In *Galois groups over* $\mathbf{Q}$ *(Berkeley, CA, 1987)*, volume 16 of *Math. Sci. Res. Inst. Publ.*, pages 385–437. Springer, New York, 1989.

[Neu73] Jürgen Neukirch. Über das Einbettungsproblem der algebraischen Zahlentheorie. *Invent. Math.*, 21:59–116, 1973.

[Oza11] Manabu Ozaki. Construction of maximal unramified p-extensions with prescribed Galois groups. *Invent. Math.*, 183(3):649–680, 2011.

[Raz77] Michael J. Razar. Central and genus class fields and the Hasse norm theorem. *Compositio Math.*, 35(3):281–298, 1977.

[Sch68] Michael Schlessinger. Functors of Artin rings. *Trans. Amer. Math. Soc.*, 130:208–222, 1968.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups*, volume Vol. 42 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, french edition, 1977.

[Vak06] Ravi Vakil. Murphy's law in algebraic geometry: badly-behaved deformation spaces. *Invent. Math.*, 164(3):569–590, 2006.

[Web16] Peter Webb. *A course in finite group representation theory*, volume 161 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2016.