MURPHY'S LAW FOR GALOIS DEFORMATION RINGS

ANDREEA IORGA

Abstract. In this paper, 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 $H/K/F$ with the property that H is the maximal pro-p extension of K that is unramified everywhere, and $\mathrm{Gal}(H/K) = G$. 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.

1. Introduction

Let p be a prime. Let Φ be a finite group of order prime to p, and let G be a finite p-group with an action of Φ. Throughout this paper, Φ will be fixed, and G will represent any p-group with an action of Φ. Let $\Gamma = G \rtimes \Phi$ be the semi-direct product of G and Φ. For any number field F, let $L_p(F)$ denote the maximal unramified p-extension of F. If Φ is the trivial group, Ozaki's Theorem (Theorem 1 in [12]) states that any p-group $\Gamma = G$ can be written as the Galois group of $L_p(F)/F$, for some totally complex number field F. A recent paper by Hajir, Maire and Ramakrishna ([6]) 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 paper, we prove a different generalization in the case of regular primes:

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 L/E such that*

- *L/E is Galois with Galois group Φ,*
- *E contains μ_p, and is totally imaginary if $p = 2$,*
- *L has class number prime to p,*
- *L/E satisfies property **P** below.*

For any p-group G with an action of Φ, there exist extensions of number fields $H/K/F$ such that

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

Definition 1.1. We say that an extension of number fields L/K has property **P** if for all primes $\mathfrak{p}$ of K, and $\mathfrak{P} \mid \mathfrak{p}$, either $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is unramified or $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is tamely ramified with ramification index e and $e \mid (q-1)$, where q is the cardinality of the residue field of $K_{\mathfrak{p}}$.

When Φ is trivial, we can recover Ozaki's result 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 regular primes); a similar hypothesis is present in the first version (arXiv:0705.2293) of Ozaki's paper [12]. The proof of this theorem is presented in Section 2, and it is inspired by Ozaki's theorem

and techniques. Throughout this paper, we will present the similarities and differences between our methods and Ozaki's methods.

A motivating example and a consequence of Theorem 1 is Theorem 2 below. Consider a continuous absolutely irreducible residual Galois representation $\overline{\rho}\colon G_F \to \mathrm{GL}_2(\mathbb{F}_p)$. One can associate to $\overline{\rho}$ a number of deformation rings. These pro-represent functors of deformations from the category $\mathcal{C}$ of local Artinian rings $(A, \mathfrak{m})$ with $A/\mathfrak{m} = \mathbb{F}_p$.

Definition 1.2. Consider a deformation $\rho\colon G_F \to \mathrm{GL}_2(A)$ of $\overline{\rho}$ for a finite $(A, \mathfrak{m})$. It factors through some finite group, and the fixed field of the kernel is a finite extension; call it $F(\rho)$. We say that ρ is unramified if the extension $F(\rho)/F(\overline{\rho})$ 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. What possible rings R can occur as universal everywhere unramified deformation rings of such $\overline{\rho}$?

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 (Proposition 16 in [14]). The Unramified Fontaine-Mazur Conjecture (Conjecture 5a in [3]) 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 Proposition 10 in [1]), 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 $R \to \mathbb{Z}_p$ with finite (as a set) kernel I. In this paper, 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 R is a universal everywhere unramified deformation ring.*

This result can be seen as an example of Murphy's Law for moduli spaces, an idea introduced by Ravi Vakil in [16]: all possible singularities occur inside deformation spaces. When considering unramified deformation rings, the analogue of this is to say that all finite artinian local rings appear as unramified Galois deformation rings.

We now outline the structure of the proof, and the differences and similarities to Ozaki's methods. The proof of Theorem 1 is done by induction, as follows. Since Φ acts on the p-group G, it must preserve the centre $Z(G)$ and the p-torsion of the centre of this group. It follows that each such p-group fits into an exact sequence of p-groups

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

where V is a central subgroup of exponent p on which Φ acts by an irreducible representation. Therefore, there exists a sequence of p-groups

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

where each map is surjective and $\ker(G_i \to G_{i-1}) = V$ at each step. It follows that there exists a sequence of surjections

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

such that the kernel at each step is isomorphic to V, where $\Gamma_i = G_i \rtimes \Phi$. The base case of the inductive process is the assumption of Theorem 1. The inductive step follows from Proposition 2.2, whose proof is presented in Section 6. Just as in Ozaki's case, the extensions are constructed using Kummer Theory. The main difference between our proof and Ozaki's is

that we are not working with p-groups, but with p-groups with a Φ-action. Thus, we need to construct a big number of primes satisfying a series of congruence conditions. Constructing enough primes relies on the fact that the base field has a large enough degree over $\mathbb{Q}$. To ensure this, we perform a series of base changes using Proposition 2.1, whose proof is presented in Section 4. The proof relies on the theory of modular representations of $\mathbb{F}_p[\Gamma]$. Finally, the proof of Theorem 2 can be found in the last section. In fact, Section 7 presents a proof that works in general for any prime $p \geq 5$ with the assumption that there exists a Φ-extension of $\mathbb{Q}(\zeta_p)$ with class number prime to p that satisfies property $\mathbf{P}$.

2. Strategy for proving Theorem 1

Theorem 1 can be derived from the following two propositions, which will be proved in Sections 4 and 6.

Proposition 2.1. *With the above notation, let K/F be a Galois extension of number fields with Galois group Φ satisfying:*

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

Then there exists a cyclic extension F'/F of degree p such that if $K' = F'.K$, then: $F' \cap L_p(K) = F$, $L_p(K') = F'.L_p(K)$ and $\mathrm{Gal}(L_p(K')/F') \cong \Gamma$. Moreover, if the initial extension K/F satisfies property $\boldsymbol{P}$, then the new extension K'/F' also satisfies property $\boldsymbol{P}$.

Proposition 2.2. *Let K/F be a Galois extension of number fields satisfying the four conditions of Proposition 2.1 and property $\boldsymbol{P}$. Assume Φ acts irreducibly on a 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 K'/F' such that

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

The proof of Theorem 1 is inspired by Ozaki's results, and follows from Propositions 2.1 and 2.2 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 K_i/F_i satisfying the conditions of Proposition 2.1 for G_i and Γ_i. Using Proposition 2.1 repeatedly, we can construct

a finite extension F_i' of F_i such that if $K_i' = F_i'.K_i$, then $F_i' \cap L_p(K_i) = F_i$, $L_p(K_i') = F_i'.L_p(K_i)$, and $\mathrm{Gal}(L_p(K_i')/F_i') \cong \Gamma_i$. Moreover, repeatedly constructing extensions using Proposition 2.1, we increase the degree $[F_i' \colon \mathbb{Q}]$, while keeping $2(2d(G_{i+1}) + r(G_{i+1}) + d(\Phi))$ unchanged. Thus, we can also assume that $[F_i' \colon \mathbb{Q}] \geq 2(2d(G_{i+1}) + r(G_{i+1}) + d(\Phi))$. Since this extension K_i'/F_i' satisfies the conditions of Proposition 2.2, there exists a finite extension K_{i+1}/F_{i+1} such that $F_i' \subset F_{i+1}$, $K_i' \subset K_{i+1}$, $\mathrm{Gal}(K_{i+1}/F_{i+1}) \cong \Phi$, $\mathrm{Gal}(L_p(K_{i+1})/F_{i+1}) \cong \Gamma_{i+1}$, every prime of F_{i+1} lying over p splits completely in $L_p(K_{i+1})$ and $L_p(K_{i+1})/F_{i+1}$ satisfies property **P**. Therefore, we have obtained fields $F = F_n$, $K = K_n$ and $H = L_p(K_n)$ with the desired properties.

3. Tools for the proof

In this section, we present some facts that will be useful later in the paper. Most of these results can either be found in [12] or are generalizations of results in [12]. We will follow Ozaki's notation.

Suppose F is a number field. Let $U_{\mathfrak{p}}(F)$ be the pro-p-part of the local unit group of the complete field $F_{\mathfrak{p}}$ of F at $\mathfrak{p}$ and $U(F) = \oplus_{\mathfrak{p}|p} U_{\mathfrak{p}}(F)$. We embed the unit group of the localisation $\mathcal{O}_{F,\mathfrak{p}}$ of the maximal order $\mathcal{O}_F$ of F at p diagonally into $U(F)$ as usual, and let $U'_{\mathfrak{p}}(F)$ be the submodule of $U_{\mathfrak{p}}(F)$ consisting of all the elements u such that $F_{\mathfrak{p}}(\sqrt[p]{u})/F_{\mathfrak{p}}$ is unramified; let $U'(F) = \oplus_{\mathfrak{p}|p} U'_{\mathfrak{p}}(F)$. Since we have that $U(F)^p \subset U'(F) \subset U(F)$, we can define $R(F) = U(F)/U(F)^p$ and $R'(F) = U(F)/U'(F)$.

Lemma 3.1. *If K/F is a Galois extension with Galois group Φ as above, then*

(1) $R(K) \cong \mathbb{F}_p[\Phi]^{[F\colon \mathbb{Q}]+s}$ and $R'(K) \cong \mathbb{F}_p[\Phi]^{[F\colon \mathbb{Q}]}$,

(2) $R(L_p(K)) \cong \mathbb{F}_p[\Gamma]^{[F\colon \mathbb{Q}]+s}$ and $R'(L_p(K)) \cong \mathbb{F}_p[\Gamma]^{[F\colon \mathbb{Q}]}$,

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

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

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

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

Lemma 3.2. *Let p be any prime number, F a number field with $L_p(F) = F$ 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 $L_p(F_S) = F_S$.

Proof. See Lemma 7 in [12]. □

Corollary 3.3. *Let S and F_S be as in Lemma 3.2. If F_S/F is a cyclic extension, then $L_p(F_S) = F_S$.*

The following is a variant of Lemma 9 of [12], which only applies to $M = L_p(K)$. Our modification works for both $M = L_p(K)$ and $M = K$.

Lemma 3.4. *Let $L_p(K)/F$ be an extension as above. Let $M = K$ or $L_p(K)$, 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 L 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

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

where the map $\rho\colon R(M) \to \mathrm{Gal}(L/M)$ is the map induced by class field theory, and the third map is the natural surjection $f\colon \mathrm{Gal}(L/M) \to \mathrm{Gal}(H/M)$. Let $\sigma = \rho(u) \in \mathrm{Gal}(L/M)$. Let N be the maximal unramified abelian extension of M. Note that L and N are linearly disjoint over H, and let $\tilde{L}$ be their compositum. Observe that $\tilde{L}$ and $\tilde{M}$ are linearly disjoint over M. Let $\tilde{\sigma} \in \mathrm{Gal}(\tilde{L}/M)$ be an element with the properties that $\mathrm{res}(\tilde{\sigma}) \mid_L = \sigma^{-1}$ and $\mathrm{res}(\tilde{\sigma}) \mid_N = 1$. Such an element exists because L and N are linearly disjoint over H, and the restrictions $\sigma^{-1} \in \mathrm{Gal}(L/M)$ 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 $(\alpha, \tilde{L}/M) = \tilde{\sigma}$ and $(\alpha, \tilde{M}/M) = \tau$. The first condition implies that $(\alpha, L/M) = \sigma^{-1}$ and $(\alpha, N/M) = 1$. The second property 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 the first condition, 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. □

4. Proof of Proposition 2.1

In this section, we provide a proof for Proposition 2.1, which is our version of Proposition 1 in the first version of [12]. Our proof follows the idea of Ozaki's proof, modified to work in 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 theory of $\mathbb{F}_p$-representations of groups of the form $G \rtimes \Phi$, where G is a p-group and Φ is a group of order prime-to-p. Throughout this section, assume that the conditions of Proposition 2.1 hold.

We would like to find an element Λ of $L_p(K)$ such that

(1) The ideal $\Lambda\mathcal{O}_{L_p(K)}$ is a prime ideal of degree 1, not lying over p.
(2) If S denotes the set of primes of $L_p(K)$ dividing $\eta = N_{L_p(K)/F}(\Lambda)$, then $L_p(K)(\sqrt[p]{\eta})$ is the maximal elementary abelian p-extension of $L_p(K)$ unramified outside S.

Lemma 4.1. *Assume such an element Λ exists. Let $F' = F(\sqrt[p]{\eta})$, with η as above. Then F'/F is an extension that satisfies Proposition 2.1.*

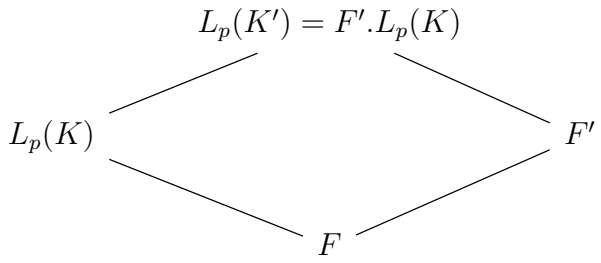
Proof. Since $\eta\mathcal{O}_F$ is a prime ideal of $\mathcal{O}_F$, it follows that $\sqrt[p]{\eta} \notin F$, so F' is a degree p extension of F. Let $K' = K.F'$. The fields K and F' are linearly disjoint over F, so K'/K is a degree

p extension. We want to prove that $F' \cap L_p(K) = F$, $L_p(K') = F'.L_p(K)$, and that the extension $L_p(K')/F'$ is Galois with Galois group isomorphic to Γ.

Consider $F' \cap L_p(K)$. This is equal to F' if $F' \subset L_p(K)$; otherwise, it is equal to F. Assume $F' \subset L_p(K)$. By construction, this implies that $K' \subset L_p(K)$. But $L_p(K)$ is the maximal unramified p-extension of K, and K' is a ramified p-extension of K, so they must be linearly disjoint over K, and $K' \not\subset L_p(K)$. It follows that our assumption was false, and so $F' \cap L_p(K) = F$, which proves the first part.

Using the previous part, we observe that $F'.L_p(K) = L_p(K)(\sqrt[p]{\eta})$ and $K'.L_p(K) = L_p(K)(\sqrt[p]{\eta})$. By construction, $L_p(K)(\sqrt[p]{\eta})$ is the maximal elementary abelian p-extension of $L_p(K)$ unramified outside S, so Corollary 3.3 tells us that $L_p(L_p(K)(\sqrt[p]{\eta})) = L_p(K)(\sqrt[p]{\eta})$. On one hand, since $K' \subset K'.L_p(K)$, we must have $L_p(K') \subset L_p(K'.L_p(K)) = K'.L_p(K)$. On the other hand, $K'.L_p(K)$ is an unramified p-extension of K', so $K'.L_p(K) \subset L_p(K')$. Combining these remarks, we obtain that $L_p(K') = K'.L_p(K) = F'.L_p(K)$, proving the second part.

Finally, consider the following diagram



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

To conclude the proof, assume that the initial extension K/F has property **P**. Let $\mathfrak{p}'$ be any prime of F' and $\mathfrak{p}$ be a prime of F below $\mathfrak{p}'$. Let e and e' be the ramification indices of $\mathfrak{p}$ in K/F and of $\mathfrak{p}'$ in K'/F', respectively. Let q and q' be the number of elements of the residue fields of $F_{\mathfrak{p}}$ and $F'_{\mathfrak{p}'}$, respectively. Since the order of Φ is prime to p, we must have that $e = e'$, and $q' = q$ or $q' = q^p$. Since K/F has property **P**, then either $e = 1$ or $K_{\mathfrak{p}}/F_{\mathfrak{p}}$ is tamely ramified with $e \mid (q-1)$. It follows that either $e' = e = 1$ or $K'_{\mathfrak{p}'}/F'_{\mathfrak{p}'}$ is tamely ramified with $e' \mid (q-1) \mid (q'-1)$, so the new extension K'/F' has property **P**. □

Now, assume that Λ has property (1). Let S be the set of primes of $L_p(K)$ dividing η. If $L_p(K)(\sqrt[p]{\alpha})/L_p(K)$ is unramified outside S, for some $\alpha \in L_p(K)$, then

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

with $a_\sigma \in \mathbb{F}_p$, $\varepsilon \in \mathcal{O}^\times_{L_p(K)}$. Since $L_p(K)(\sqrt[p]{\alpha})/L_p(K)$ is unramified at the primes above p, it must be true that

$$(\varepsilon \mod U'(L_p(K))) + \sum_{\sigma \in \Gamma} a_\sigma (\sigma\Lambda \mod U'(L_p(K))) \equiv 0.$$

If this equation only holds for $\varepsilon \in (\mathcal{O}^\times_{L_p(K)})^p$ and $a_\sigma = a$, $\forall \sigma \in \Gamma$, for some $a \in \mathbb{F}_p$, then

$$\alpha \mod U(L_p(K))^p \equiv a \sum_{\sigma \in \Gamma} \sigma(\Lambda \mod U(L_p(K))^p) = a(\eta \mod U(L_p(K))^p).$$

Thus, $\sqrt[p]{\alpha} \in L_p(K)(\sqrt[p]{\eta})$, so condition (2) also holds.

Let $E = E(L_p(K))$ be the image of the map $\mathcal{O}^\times_{L_p(K)} \otimes \mathbb{F}_p \to R'(L_p(K))$. The extension $L_p(K)(\sqrt[p]{\varepsilon})/L_p(K)$ must be ramified at some prime lying over p, for any $\varepsilon \in \mathcal{O}^\times_{L_p(K)} \setminus (\mathcal{O}^\times_{L_p(K)})^p$, so this map is injective: $E \cong \mathcal{O}^\times_{L_p(K)} \otimes \mathbb{F}_p$. It follows that the map $\mathcal{O}^\times_{L_p(K)} \otimes \mathbb{F}_p \to R(L_p(K))$ is also injective, and by abuse of notation we denote its image by E.

The following Lemma represents a key step in the proof of Proposition 2.1. It is a variation of Lemma 8 in [12] 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 $\mathbb{F}_p[G]$ 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 prime-to-p group). To deal with this, we turn to the theory of modular representations for groups of the form $G \rtimes \Phi$ ([17]) and we make use of some of the ideas that appear in Section 6 of [5].

Lemma 4.2. *Let N be the kernel of the projection $R(L_p(K)) \to R'(L_p(K))$. Then there exist free $\mathbb{F}_p[\Gamma]$-modules M, N, Q of $R(L_p(K))$ such that*

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

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 (see Section 8.5 in [17]). In particular, any free $\mathbb{F}_p[\Gamma]$-module is injective.

Since Φ has order prime to p, the projective indecomposable $\mathbb{F}_p[\Gamma]$-modules P_S are in a one-to-one correspondence with the simple $\mathbb{F}_p[\Phi]$-modules S (Proposition 8.3.2 in [17]). It follows that $\mathbb{F}_p[\Gamma]$ can be decomposed as a sum of projective indecomposable modules

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

where $n_s = \dim_D(S)$, $D = \operatorname{End}_{\mathbb{F}_p[\Phi]} S$.

From Section 8.5 in [17], we know that any $\mathbb{F}_p[\Gamma]$-module has a unique injective hull. Let $\tilde{M} = \oplus P_S^{\alpha_S}$ be the injective hull of the $\mathbb{F}_p[\Gamma]$-module E. Consider the following diagram

$$\begin{array}{ccc} E & \xrightarrow{\quad f \quad} & \tilde{M} \\ \downarrow{\scriptstyle i} & \swarrow{\scriptstyle g} & \\ R(L_p(K)) & & \end{array}$$

The $\mathbb{F}_p[\Gamma]$-module $R(L_p(K))$ is free by Lemma 3.1, so it is injective. The map i is the usual inclusion map from E to $R(L_p(K))$. The map f is the essential monomorphism $E \to \tilde{M}$. Since $R(L_p(K))$ is an injective $\mathbb{F}_p[\Gamma]$-module, there exists a map $g\colon \tilde{M} \to R(L_p(K))$ such that $g \circ f = i$. Moreover, since f is an essential monomorphism, the map g is injective. Let $M_1 = \operatorname{Im}(g) \subset R(L_p(K))$; 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

$$1 \to N \to R(L_p(K)) \to R'(L_p(K)) \to 1.$$

Since $R'(L_p(K))$ is a free module (Lemma 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 (Example 4.7(3) in [10]).

Consider the intersection $M_1 \cap N$. Let $\mathrm{Soc}(M_1 \cap N)$ be the socle of $M_1 \cap N$. For details about this notion, see Section 6.3 of [17]. 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. Moreover, $M_1 \cap N$ is a submodule of M_1. Using the facts that $\mathrm{Soc}\, E \cong \mathrm{Soc}\, M_1$, $\mathrm{Soc}\, K \subset K$ and $\mathrm{Soc}\, K = K \cap \mathrm{Soc}\, M_1$, for all submodules K of M_1, we obtain

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

It follows that $M_1 \cap N = 0$, so $M_1 + N$ is a direct sum in $R(L_p(K))$. Since $M_1 \oplus N$ is a projective $\mathbb{F}_p[\Gamma]$-module, it must also be injective, so the following exact sequence splits:

$$1 \to M_1 \oplus N \to R(L_p(K)) \to R(L_p(K))/(M_1 \oplus N) \to 1.$$

Let $Q_1 = R(L_p(K))/(M_1 \oplus N)$. 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 $\alpha_S + \beta_S = [F\colon \mathbb{Q}] \cdot n_S$.

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 [5].

On one hand, from the exact sequence

$$0 \to \mathcal{O}^\times_{L_p(K)}/\mu_p \xrightarrow{p} \mathcal{O}^\times_{L_p(K)} \to \mathcal{O}^\times_{L_p(K)}/p \to 0,$$

we derive the sequence

$$(\mathcal{O}^\times_{L_p(K)}/\mu_p)^G \to (\mathcal{O}^\times_{L_p(K)})^G \to (\mathcal{O}^\times_{L_p(K)}/p)^G \to H^1(G, \mathcal{O}^\times_{L_p(K)}/\mu_p).$$

We observe that

- $(\mathcal{O}^\times_{L_p(K)}/p)^G = E^G$,
- $(\mathcal{O}^\times_{L_p(K)})^G/(\mathcal{O}^\times_{L_p(K)}/\mu_p)^G \cong (\mathcal{O}^\times_K)/(\mathcal{O}^\times_K/\mu_p) \cong \mathcal{O}^\times_K/\mathcal{O}^{\times p}_K$,

so the sequence becomes

$$\mathcal{O}^\times_K/\mathcal{O}^{\times p}_K \to E^G \to H^1(G, \mathcal{O}^\times_{L_p(K)}/\mu_p). \tag{1}$$

On the other hand, from the exact sequence

$$0 \to \mu_p \to \mathcal{O}^\times_{L_p(K)} \to \mathcal{O}^\times_{L_p(K)}/\mu_p \to 0,$$

we get the exact sequence

$$H^1(G, \mathcal{O}^\times_{L_p(K)}) \to H^1(G, \mathcal{O}^\times_{L_p(K)}/\mu_p) \to H^2(G, \mu_p). \tag{2}$$

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.

Now, if $j\colon \mathrm{Cl}_K \to \mathrm{Cl}_{L_p(K)}$ is the map induced by the inclusion $K \hookrightarrow L_p(K)$, then $H^1(G, \mathcal{O}^\times_{L_p(K)}) \cong \ker j$ (see 2 in [8]). Moreover, $\ker j$ is equal to the p-primary part of Cl_K,

which is isomorphic to $\mathrm{Gal}(L_p(K)/K)^{\mathrm{ab}} = G^{\mathrm{ab}}$, by class field theory. From the semisimple version of Dirichlet's unit theorem (Theorem 6.1 in [5]; for a proof, see Theorem 6.1 in [4]) and the fact that F is totally imaginary, we obtain that

$$\mathrm{rank}_{\mathbb{F}_p[\Phi]}(\mathcal{O}_K^\times/\mathcal{O}_K^{\times p}) \leq \frac{1}{2}[F\colon \mathbb{Q}]. \tag{3}$$

From (1), (2) and (3) it follows that

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

where d_p is the usual p-rank, and $d(G)$ and $r(G)$ are the number of generators and relations of G. Therefore:

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

We can thus choose $t \geq (\frac{1}{2}[F\colon \mathbb{Q}] - d(G) - r(G))$ 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

$$R(L_p(K)) = M_1 \oplus N \oplus Q_1 \cong M_1 \oplus N \oplus Q \oplus P \cong M \oplus N \oplus Q,$$

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

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 a prime Λ of $L_p(K)$ with properties (1) and (2). The proof follows the steps of Proposition 1 in the first version of [12]. Let M and $Q = \bigoplus_{i=1}^t \mathbb{F}_p[\Gamma] q_i$ be the $\mathbb{F}_p[\Gamma]$-submodules of $R(L_p(K))$ given by Lemma 4.2. Then, by assumption,

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

Let $\{\sigma_1, \ldots, \sigma_d\}$ be a system of minimal generators for Γ, $d = d(\Gamma)$. Let $u = \sum_{i=1}^d (\sigma_i - 1) q_i \in Q \subset R(L_p(K))$. By Lemma 3.4 for $M = L_p(K)$, there exists $\Lambda\mathcal{O}_{L_p(K)}$ a prime of degree 1, not lying over p, such that $u = (\Lambda \mod U(L_p(K))^p)$. Assume that there exist $\varepsilon \in \mathcal{O}^\times_{L_p(K)}$ and $a_\sigma \in \mathbb{F}_p$ such that $(\varepsilon \mod U'(L_p(K))) + \sum_{\sigma\in\Gamma} a_\sigma(\sigma\Lambda \mod U'(L_p(K))) = 0$. Observe that:

- $\varepsilon \mod U(L_p(K))^p + \sum_{\sigma\in\Gamma} a_\sigma(\sigma\Lambda \mod U(L_p(K))^p) \in N$;
- $\sum_{\sigma\in\Gamma} a_\sigma(\sigma\Lambda \mod U(L_p(K))^p) = \sum_{\sigma\in\Gamma} a_\sigma(\sigma u) \in Q$;

- $\varepsilon \mod U(L_p(K))^p \in E \subset M$.

By Lemma 4.2, it follows that $\varepsilon \mod U(L_p(K))^p = \sum_{\sigma\in\Gamma} a_\sigma(\sigma\Lambda \mod U(L_p(K))^p) = 0$. On one hand, since $U(L_p(K))^p \cap \mathcal{O}^\times_{L_p(K)} = \mathcal{O}^{\times p}_{L_p(K)}$, it follows that $\varepsilon \in \mathcal{O}^{\times p}_{L_p(K)}$. On the other hand, $\sum_{\sigma\in\Gamma} a_\sigma(\sigma\Lambda \mod U(L_p(K))^p) = 0$ 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 $1 \le i \le d$, 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.

5. Embedding Problem

In this section, we introduce some results about the embedding problem, used in the proof of Proposition 2.2. A detailed exposition of this can be found in [11].

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 (Satz 2.3 in [7]). We are only interested in the case when the extension is nonsplit, so we can assume that if a solution to the embedding problem exists, then it is proper. This is the same as 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 $F_\mathfrak{p}$ (resp. $K_\mathfrak{p}$) the completion of F at $\mathfrak{p}$ (resp. 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 group 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 [11] (Satz 2.2, Satz 4.7, Satz 5.1).

Theorem 5.1. *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 5.2. *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 5.3. *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 $n' = \prod_{p|e} p^{v_p(n)}$ and q is the number of elements of the residue field of $F_{\mathfrak{p}}$.

Going back to our case, consider the following embedding problem:

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

with $\mathrm{Gal}(L_p(K)/F) = \Gamma = G \rtimes \Phi$, $\mathrm{Gal}(K/F) = \Phi$, and K/F satisfies property **P** (which implies that $L_p(K)/F$ also satisfies this property). By Theorem 5.3, all the local embedding problems have solutions, so in order to use Theorem 5.1, we need to prove that the map

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

is injective. Note that V is not a trivial $\mathbb{F}_p[\Gamma]$-module, so we can't apply Theorem 5.2 directly. Consider the following commutative diagram

$$\begin{array}{ccc} H^2(G_F, V) & \longrightarrow & \prod_{\mathfrak{p}} H^2(G_{F_{\mathfrak{p}}}, V) \\ \downarrow \mathrm{res} & & \downarrow \mathrm{res} \\ H^2(G_K, V) & \longrightarrow & \prod_{\mathfrak{p}} H^2(G_{K_{\mathfrak{p}}}, V) \end{array}$$

Using spectral sequences, we can prove that $H^2(G_K, V)^{\Phi} \cong H^2(G_F, V)$, so the map on the left is injective. Similarly, it can be proved that the map on the right is injective. Since $K = \overline{F}^{\ker \overline{\rho}}$, where $\overline{\rho}\colon G_F \to \mathrm{GL}_2(\mathbb{F}_p)$ is irreducible and has image Φ, the adjoint action coming from G_F is killed on G_K, so

$$H^2(G_K, V) \cong H^2(G_K, \mathbb{F}_p^n),$$

where $n = \dim_{\mathbb{F}_p} V$. So by Theorem 5.2, the map on the bottom is injective. It thus follows that the top map is injective, and so Theorem 5.1 applies.

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

Proposition 5.4. *Let K/F be an extension with Galois group Φ that satisfies property **P**. Consider the extension $L_p(K)/F$ with Galois group Γ. The embedding problem*

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

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

6. Proof of Proposition 2.2

In this section, we will provide a proof for Proposition 2.2. 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 K.

Let $n = \dim_{\mathbb{F}_p} V$ and let $m = |\Phi|$. Let $g_1, \dots, g_n$ 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 $[F\colon \mathbb{Q}] \geq 2d(T+2)$, where $d = d(\Phi)$ is the number of generators of Φ, by replacing F with some finite extension of F given by Proposition 2.1. Recall that Proposition 2.1 constructs a new extension that satisfies property **P** if the initial extension satisfied this property. Note that $R(L_p(K))^G \cong R(K)$ and $R'(L_p(K))^G \cong R'(K)$ as $\mathbb{F}_p[\Phi]$-modules, $N^G \cong \ker(R(K) \to R'(K))$, and $(\mathcal{O}_K^\times \otimes \mathbb{F}_p) \cap Q^G = 0$, where Q is the $\mathbb{F}_p[\Gamma]$-module obtained in Lemma 4.2. Let $\{\sigma_1, \dots, \sigma_d\}$ 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 3.4 applied to $M = K$, we obtain primes $\lambda_i \mathcal{O}_K$ that are completely split in $L_p(K)/K$, and satisfy $N(\lambda_i) \equiv 1 \pmod{p}$ and

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

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

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

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

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

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

where χ_W is the character of W. This is a modified version of Theorem 8 in [15] that works for (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 $\mathbb{F}_p$.

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 pair, 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 λ_ℓ. Lift this $\overline{r_\ell}$ to a principal ideal κ_ℓ in $\mathcal{O}_K$. 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

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

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

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

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

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

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

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

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

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

Let $R = \prod_{i,\ell} g_i^{-1}(\lambda_\ell)$. We would like to construct a prime α of $\mathcal{O}_K$ with $\alpha \equiv g_i^{-1}(A_{i,\ell}) \pmod{g_i^{-1}(\lambda_\ell)}$, for all i and ℓ. Since the ideals $g_i^{-1}(\lambda_\ell)\mathcal{O}_K$ are pairwise coprime, the Chinese remainder theorem tells us that constructing such an α is equivalent to constructing an α that satisfies a specific congruence modulo $R\mathcal{O}_K$, 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 β of $\mathcal{O}_K$ with $\beta \equiv g_i^{-1}(B_{i,\ell}) \pmod{g_i^{-1}(\lambda_\ell)}$, it is enough to construct a prime β with a specific compatible congruence modulo $R\mathcal{O}_K$, say $\beta \equiv r_2 \pmod{R}$. Use the existence theorem of class field theory to construct an abelian extension $\tilde{M}/K$ whose Galois group is in a natural correspondence with the ray classes modulo $R\mathcal{O}_K$. Use Lemma 3.4 with $M = K$ again to find two primes α and β of $\mathcal{O}_K$ that split completely in $L_p(K)/K$, prime to p, such that

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

and

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

in $R(K)$, 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 $K^\times/K^{\times p}$ is an $\mathbb{F}_p[\Phi]$-module, so we can consider the projections to the V-eigenspace of $\nu_1\alpha$ and $\nu_2\beta$. Construct K_1 to be the Galois closure of $K(\sqrt[p]{P_V(\nu_1\alpha)})$ over F, and K_2 to be the Galois closure of $K(\sqrt[p]{P_V(\nu_2\beta)})$ over F. Then $\mathrm{Gal}(K_1/F) \cong \mathrm{Gal}(K_2/F) \cong V \rtimes \Phi$. Moreover, since $P_V(\nu_1\alpha) = 0$ in $R(K)$, every prime lying over p in K splits completely in K_1/K. The same holds true for K_2/K. Consider their compositum $\tilde{K} = K_1.K_2$ and let $\tilde{L} = \tilde{K}.L_p(K)$. We claim that:

- The extension $\tilde{L}/L_p(K)$ is unramified at p.
- Recall that $g(\alpha)$, $g(\beta)$, $g(\lambda_i)$ split completely in $L_p(K)/K$ by construction, for all $g \in \Phi$ and $1 \leq i \leq T$. Let $\tilde{S}$ be the set of primes of $L_p(K)$ lying above these primes. Then $\tilde{L}/L_p(K)$ is the maximal elementary abelian p-extension of $L_p(K)$ which is unramified outside $\tilde{S}$.
- All the $(\mathbb{Z}/p\mathbb{Z})^2$-subgroups of $\mathrm{Gal}(\tilde{L}/L_p(K))$ appear as decomposition groups of some prime in $L_p(K)$ lying over $g(\lambda_i)$, for $g \in \Phi$ and $1 \leq i \leq T$.

Consider $P_V(\nu_1\alpha)$ in $R(K)$. By construction, $P_V(\nu_1\alpha) = 0$ in $R(K)$, so it must remain trivial in $R'(K)$. Similarly, $P_V(\nu_2\beta) = 0$ in $R'(K)$. It implies that K_1/K and K_2/K are unramified at p, and thus $\tilde{K}/K$ is unramified at p. Combine this with the fact that $L_p(K)/K$ is unramified everywhere to conclude that $\tilde{L} = \tilde{K}.L_p(K)/L_p(K)$ is unramified at p.

To show that $\tilde{L}$ is the maximal elementary abelian p-extension of $L_p(K)$ unramified outside $\tilde{S}$, it is enough to show that $\tilde{K}$ is the maximal elementary abelian p-extension of K unramified outside $S = \{g(\alpha), g(\beta), g(\lambda_i) \mid g \in \Phi, 1 \leq i \leq T\}$. This is true because $\tilde{S}$ represents the set of primes of $L_p(K)$ lying over the primes in S, and all the primes in S split completely in $L_p(K)/K$.

To this end, consider an elementary abelian p-extension of K unramified outside S, call it $K(\sqrt[p]{\gamma})/K$. Then

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

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

On one hand, consider $P_W(\gamma)$, for $W \neq V$:

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

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:

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

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 $R(K)$. Consider $P_V(\gamma)$:

$$0 = P_V(\gamma) = \sum_{i=1}^{T} \sum_{g\in\Phi} \left(\sum_{h\in\Phi} n_{h,V} \left(c_{gh^{-1},i} - \sum_{\tau\in\Phi} (b_{g\tau^{-1}} y_{\tau h^{-1},i} + a_{g\tau^{-1}} x_{\tau h^{-1},i}) \right) \right) g(\lambda_i).$$

Using the same argument as above, we observe that

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

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

Finally, putting these things together, we obtain that

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

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

Just as above, we observe that it is enough to prove the third claim for $\tilde{K}/K$, the statement for $\tilde{L}/L_p(K)$ following from it, since $g(\lambda_i)$ splits completely in $L_p(K)/K$, for all $g \in \Phi$ and $1 \leq i \leq T$, and $\mathrm{Gal}(\tilde{L}/L_p(K)) \cong \mathrm{Gal}(\tilde{K}/K)$. The following short lemma proves this statement for $\tilde{K}/K$.

Lemma 6.1. *All the $(\mathbb{Z}/p\mathbb{Z})^2$-subgroups of $\mathrm{Gal}(\tilde{K}/K)$ appear as decomposition groups 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 N of $\mathrm{Gal}(\tilde{K}/K)$; note that there are $T = \frac{(p^{2n}-1)(p^{2n}-p)}{(p^2-1)(p^2-p)}$ of them. Assume that N is generated by $(a_1, \ldots, a_n, b_1, \ldots, b_n)$ and $(x_1, \ldots, x_n, y_1, \ldots, y_n)$

with $(a_1,\dots,a_n,b_1,\dots,b_n)\neq 0$, $(x_1,\dots,x_n,y_1,\dots,y_n)\neq 0$, and $(a_1,\dots,a_n,b_1,\dots,b_n)$ and $(x_1,\dots,x_n,y_1,\dots,y_n)$ are not multiples of each other. From the above discussion, we know that there is a prime $\lambda = g_i(\lambda_\ell)$ such that the exponents of $g_1^{-1}(\lambda), g_2^{-1}(\lambda),\dots,g_n^{-1}(\lambda)$ are $a_1,\dots,a_n$ in ν_1, and $b_1,\dots,b_n$ in ν_2, respectively. This implies that the inertia subgroup corresponding to λ in $\mathrm{Gal}(\tilde{K}/K)$ is generated by $(a_1,\dots,a_n,b_1,\dots,b_n)$. Moreover, the prime λ satisfies

$$\begin{aligned}\alpha &\equiv g_j^{-1}(A_{j,\ell}) \pmod{g_j^{-1}(\lambda)},\\ \beta &\equiv g_j^{-1}(B_{j,\ell}) \pmod{g_j^{-1}(\lambda)},\end{aligned}$$

for all $1\leq j\leq n$, which implies that the fixed field of inertia is nontrivial, but the fixed field of N is trivial. Thus, the decomposition group of λ is isomorphic to N. This concludes the proof, since N was chosen arbitrary. □

We claim that the extension $\tilde{L}/L_p(K)$ satisfies the conditions of Lemma 3.2, with $\tilde{S}$ instead of S. We know that $L_p(L_p(K)) = L_p(K)$ and we have just proved that $\tilde{L}$ is the maximal elementary abelian p-extension of $L_p(K)$ unramified outside $\tilde{S}$, so the only thing left to prove is that the following map is surjective

$$\bigoplus_v H_2(D_v,\mathbb{Z}) \to H_2(\mathrm{Gal}(\tilde{L}/L_p(K)),\mathbb{Z}),$$

where the sum is over all the primes of $L_p(K)$. The key fact is that for a finite abelian group G, the homology group $H_2(G,\mathbb{Z})$ is isomorphic to the second exterior power of G, $\bigwedge^2(G)$ (Lemma 5 in [13]). Recall that $\mathrm{Gal}(\tilde{L}/L_p(K)) \cong \mathrm{Gal}(\tilde{K}/K) \cong (\mathbb{Z}/p\mathbb{Z})^{2n}$; assume that $\mathrm{Gal}(\tilde{L}/L_p(K))$ is generated by $\{\tau_1,\tau_2,\dots,\tau_{2n}\}$. Consider the $(\mathbb{Z}/p\mathbb{Z})^2$-subgroups of $\mathrm{Gal}(\tilde{L}/L_p(K))$ generated by pairs of two elements in $\{\tau_1,\dots,\tau_{2n}\}$. There are $n(2n-1)$ of them; call them $A_1,A_2,\dots,A_{n(2n-1)}$. In particular, $A_{k+j} = \langle\tau_i,\tau_{i+j}\rangle$, where i ranges from 1 to $2n-1$ and $k = 2n(i-1) - \frac{(i-1)i}{2}$, $1\leq j\leq 2n-i$.

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 $\mathrm{Gal}(\tilde{L}/L_p(K))$, 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 $g(\lambda_j), g(\alpha), g(\beta)$. 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 $\mathrm{Gal}(\tilde{L}/L_p(K))$, so there exists a basis $\{x_1, \dots x_{2n}\}$ of $\mathrm{Gal}(\tilde{L}/L_p(K))$ 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 $\bigwedge^2 \mathrm{Gal}(\tilde{L}/L_p(K))$, which implies that $\bigwedge^2 \mathrm{Gal}(\tilde{L}/L_p(K)) \subset \bigoplus \bigwedge^2 D_{v_i} \subset \bigoplus \bigwedge^2 D_v$, so we must have equality. Thus, the map in Lemma 3.2 is surjective, proving that $L_p(\tilde{L}) = \tilde{L}$.

Let $L_1 = K_1.L_p(K)$ and $L_2 = K_2.L_p(K)$. Then $\tilde{L} = L_1.L_2$. Note that $\mathrm{Gal}(L_1/F) \cong \mathrm{Gal}(L_2/F) \cong V \rtimes \Gamma \cong \Gamma'$, by the discussion preceding Proposition 5.4. Let K' be the Galois closure of $K(\sqrt[p]{P_V(\nu_1\alpha)P_V(\nu_2\beta)^{-1}})$ over F. We would like to show that there exists F'/F that satisfies the conditions of Proposition 2.2. Since $\mathrm{Gal}(K'/K) \cong V$ and $\mathrm{Gal}(K'/F) \cong V \rtimes \Phi$ by construction, we have the following exact sequence

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

Recall that V is a p-group and Φ is a group of order prime to p, so this sequence splits, and we can view $\mathrm{Gal}(K/F) = \Phi$ as a subgroup of $\mathrm{Gal}(K'/F)$. Let $F' = K'^{\Phi}$. The extension K'/F' is Galois and has Galois group Φ. Moreover, $K \subset K'$ and $F \subset F'$. By construction, F'/F and L_1/F are linearly disjoint, and $L_1.F' = L_1.K' = \tilde{L}$, so $\mathrm{Gal}(\tilde{L}/F') \cong \mathrm{Gal}(L_1/F) \cong \Gamma'$. We claim that $L_p(K') = \tilde{L}$. Since $\tilde{L}$ is an unramified p-extension of $L_p(K).K'$ and $L_p(K).K'$ is an unramified p-extension of K', it follows that $\tilde{L} \subset L_p(K')$. Combining this with the fact that $L_p(\tilde{L}) = \tilde{L}$, we conclude that $\tilde{L} = L_p(K')$. Moreover, every prime of F' lying over p splits completely in $\tilde{L}$. To finish the proof in the case of a split extension, we have to prove that $L_p(K')/F'$ satisfies property **P**. Since $L_p(K')/K'$ is everywhere unramified, we only have to prove that the extension K'/F' satisfies property **P**. Since $\mathrm{Gal}(K'/F') \cong \mathrm{Gal}(K/F) \cong \Phi$ has order prime to p, and F'/F is a p-extension, this argument is similar to the one at the end of the proof of Lemma 4.1, and will be omitted.

If the extension

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

is not split, we cannot work over K anymore. However, the proof is similar. We begin by proving the following lemma, which is a variation of Lemma 6 in [12]. In fact, we can recover Ozaki's lemma from the following result in the case of $\Phi = 1$, $V = \mathbb{Z}/p\mathbb{Z}$ and $\mu_p \subset K$. The proof is similar to the proof of Lemma 4 in the first version of Ozaki's paper, the main differences coming from the $\mathbb{F}_p$-dimension of V and the action of Φ on V.

Lemma 6.2. *For any group extension*

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

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

(1) $L_p(K') = L_p(K).K'$ and $L_p(K') = L_p(K).F'$; hence $\mathrm{Gal}(L_p(K')/F') \cong \mathrm{Gal}(L_p(K)/F)$ and every prime of F' lying over p splits completely in $L_p(K')$.

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

Proof. By Proposition 5.4, there exists a Galois extension L/F containing $L_p(K)$ such that $\mathrm{Gal}(L/F) \cong \Gamma'$. Let $\alpha_1, \ldots, \alpha_n$ be the Kummer generators of $L/L_p(K)$, so $L = L_p(K)(\sqrt[p]{\alpha_1}, \ldots, \sqrt[p]{\alpha_n})$. Since $K \subset L_p(K) \subset L$ and K/F is Galois, the extension L/K must be Galois, so $(\alpha_i \mod L_p(K)^{\times p}) \in (L_p(K)^\times/L_p(K)^{\times p})^G$, where $G = \mathrm{Gal}(L_p(K)/K)$. Thus, $\alpha_i \mathcal{O}_{L_p(K)} = \mathfrak{A}_i^p \mathfrak{a}_i$, for $\mathfrak{A}_i$ an ideal of $\mathcal{O}_{L_p(K)}$ and $\mathfrak{a}_i$ an ideal of $\mathcal{O}_K$. Let h be the class number of $L_p(K)$; so $(h,p) = 1$. Then, $\mathfrak{A}_i^h = A_i \mathcal{O}_{L_p(K)}$, for some $A_i \in L_p(K)$, which implies that $\alpha_i^h \mathcal{O}_{L_p(K)} = A_i^p \mathfrak{a}_i^h$. Let $\mathfrak{a}_i' = \mathfrak{a}_i^h$ and $\alpha_i' = \alpha_i^h A_i^{-p}$. Then $\mathfrak{a}_i' = \alpha_i' \mathcal{O}_{L_p(K)}$ is an ideal of $\mathcal{O}_K$, and $L = L_p(K)(\sqrt[p]{\alpha_1}, \ldots, \sqrt[p]{\alpha_n}) = L_p(K)(\sqrt[p]{\alpha_1'}, \ldots, \sqrt[p]{\alpha_n'})$.

Let p^{e_i} be the exact power of p dividing the order of the ideal class $[\alpha_i']_K$. Then $[\alpha_i']_K^{p^{e_i}}$ has order prime to p. Let $e = \max e_i$, and note that $[\alpha_i']_K^{p^e}$ has order prime to p. By using Proposition 2.1 repeatedly we obtain an extension F'/F of degree p^e such that if $K' = K.F'$, then

- $K' \cap L_p(K) = K$ and $F' \cap L_p(K) = F$,
- $L_p(K') = L_p(K).K'$ and $L_p(K') = L_p(K).F'$,
- $\mathrm{Gal}(L_p(K')/F') \cong \Gamma$.

Denote by $j\colon Cl_K \to Cl_{K'}$ the map induced by the inclusion $K \subset K'$, and by $N\colon Cl_{K'} \to Cl_K$ the norm map. The natural restriction $\mathrm{Gal}(L_p(K')/K') \to \mathrm{Gal}(L_p(K)/K)$, which is an isomorphism, induces an isomorphism $\mathrm{Gal}(L_p(K')/K')^{\mathrm{ab}} \cong G^{\mathrm{ab}}$. Then the order of $\ker N$ is prime to p by class field theory. Thus, since $N \circ j([\mathfrak{a}_i']_K) = [\mathfrak{a}_i']_K^{p^e}$, the order of $j([\mathfrak{a}_i']_K) \in Cl_{K'}$, say m_i, is prime to p. Let $m = \mathrm{lcm}(m_i)$, so m is prime to p. Let $\mathfrak{a}_i'^m = a_i' \mathcal{O}_{K'}$, for some $a_i' \in K'^\times$. Then $a_i' \mathcal{O}_{K'} = \alpha_i'^m \mathcal{O}_{L_p(K')}$. Thus, there exists $\varepsilon_i \in \mathcal{O}^\times_{L_p(K')}$ such that $\alpha_i'^m = a_i' \varepsilon_i$. Note that $L_p(\sqrt[p]{\alpha_1'}, \ldots, \sqrt[p]{\alpha_n'}) = L_p(\sqrt[p]{\alpha_1'^m}, \ldots, \sqrt[p]{\alpha_n'^m})$, so we can replace α_i' by $\alpha_i'^m$.

Recall that $\langle \alpha_i' \mod L_p(K')^{\times p} \rangle \subset (L_p(K')^\times/L_p(K')^{\times p})^G$, as a subgroup. Since the extension $L_p(K')(\sqrt[p]{\alpha_1'}, \ldots, \sqrt[p]{\alpha_n'})/F'$ has Galois group Γ', it follows that $\langle \alpha_i' \mod L_p(K')^{\times p} \rangle$ has an action of $\Gamma = G \rtimes \Phi$ and, as an $\mathbb{F}_p[\Gamma]$-representation, it is isomorphic to a copy of the projective cover of V; call it $\tilde{V}$. Hence, $\mathrm{Gal}(L_p(K')(\sqrt[p]{\alpha_1'}, \ldots, \sqrt[p]{\alpha_n'})/F')$ is isomorphic to $\mathrm{Gal}(L_p(K')(\sqrt[p]{P_{\tilde{V}}(\alpha_1')}, \ldots, \sqrt[p]{P_{\tilde{V}}(\alpha_n')})/F')$, 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 $a_i' \in K'^\times$. Since $\langle P_V(a_i') \rangle$ is isomorphic to a subrepresentation of V in $K'^\times/K'^{\times p}$, 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: $L_p(K')(\sqrt[p]{P_V(\alpha_1')}, \ldots, \sqrt[p]{P_V(\alpha_n')})/F'$ is the desired extension. On the other hand, the former implies that $\langle P_V(a_i') \rangle \cong V$, so $\mathrm{Gal}(K'(\sqrt[p]{P_V(a_1')}, \ldots \sqrt[p]{P_V(a_n')})/F') \cong V \rtimes \Phi$. Then, by Proposition 5.4, the Galois group of $L_p(K')(\sqrt[p]{P_V(a_1')}, \ldots \sqrt[p]{P_V(a_n')})/F'$ is isomorphic to $V \rtimes \Gamma$. Putting all this together, we can conclude that $\mathrm{Gal}(L_p(K')(\sqrt[p]{P_V(\varepsilon_1)}, \ldots \sqrt[p]{P_V(\varepsilon_n)})/F') \cong \Gamma'$. □

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 $L_p(K')(\sqrt[p]{\varepsilon_1}, \ldots, \sqrt[p]{\varepsilon_n})/F'$ satisfies property **P** except possibly at the primes above p.

Just as before, construct primes λ_i, in K', for $1 \leq i \leq T$, and α, β in K' with the same properties. The primes α, β, λ_i are in K', so just as in the previous case, the Galois closure of $K_1 = K'(\sqrt[p]{P_V(\nu_1\alpha)})$ over F has Galois group $V \rtimes \Phi$. Define the field $L_1 = L_p(K')(\sqrt[p]{\varepsilon_1 P_V(\nu_1\alpha)}, \ldots, \sqrt[p]{\varepsilon_n g_n(P_V(\nu_1\alpha))})$, and use Proposition 5.4 and Lemma 6.2 to observe that the Galois group of L_1/F' is Γ'. Construct K_2 and L_2 in a similar manner. Let $\tilde{K}$ be the Galois closure of $K'(\sqrt[p]{P_V(\nu_1\alpha)P_V(\nu_2\beta)^{-1}})$ over F' and let $\tilde{L} = L_1.L_2$. Construct a field $\tilde{F}$ just as in the previous case. Then the new extension $\tilde{L}/\tilde{F}$ satisfies the conditions of Proposition 2.2. Note that property **P** is now satisfied, since there is no ramification at the prime p.

7. Proof of Theorem 2

Let R be any local ring admitting a surjection to $\mathbb{Z}_p$ with finite (as a set) kernel I_R. Assume we have an absolutely irreducible residual representation

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

whose image is $\tilde{\Phi}$, a group of order prime to p. Note that the projective image Φ of this representation is A_4, S_4, S_5 or a dihedral group. Since $\tilde{\Phi}$ has order prime to p, it lifts to a representation $\tilde{\Phi} \subset \mathrm{GL}_2(\mathbb{Z}_p)$. Let $\tilde{\Gamma}$ denote the inverse image of this group inside $\mathrm{GL}_2(R)$; it lives inside a split exact sequence

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

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

Firstly, note that $\tilde{\Gamma}$ admits a deformation to $\mathrm{GL}_2(R)$ by construction, so $R_{\overline{\rho}} \twoheadrightarrow R$, so there exists an ideal $J \subset R_{\overline{\rho}}$ such that $R_{\overline{\rho}}/J \cong R$. The general case can be reduced to the case when J is finite, so from now on, we will assume that J is finite. To prove that R is universal, it is enough to prove that for every local ring S with the following properties

- There exists a finite ideal I_S such that $S/I_S \cong \mathbb{Z}_p$;
- $S \twoheadrightarrow R$;
- There is a lift $\tilde{\Gamma} \to \mathrm{GL}_2(S)$,

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

$$\begin{array}{ccc} \tilde{\Gamma} & \longrightarrow & \mathrm{GL}_2(S) \\ & \searrow & \uparrow\downarrow \\ & & \mathrm{GL}_2(R) \end{array}$$

Before proving our main result, we need to introduce several lemmas. From now on, assume that R and S are local rings with the following properties:

(1) There exist finite ideals $I_S \subset S$ and $I_R \subset R$ such that $R/I_R \cong S/I_S \cong \mathbb{Z}_p$.
(2) $S \twoheadrightarrow R$.

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 $S/J \cong R$.

We will use the following notation:

- If A is a local ring, let $\mathfrak{m}_A$ denote the maximal ideal of A.
- Let $\Gamma_S = 1 + \mathrm{M}_2(I_S)$.
- For an ideal $I \subset S$, let $\Gamma_I = 1 + \mathrm{M}_2(I)$.

Lemma 7.1. *Let S and R be 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 $\mathfrak{m}_S/(\mathfrak{m}_S^2, p) \to \mathfrak{m}_R/(\mathfrak{m}_R^2, p)$. 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.

Firstly, we claim that $x \notin S'$. Suppose otherwise, so $x = a_0 + a_1x_1 + \ldots a_dx_d + \alpha$, 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

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

$x = a_0 + \sum a_ix_i + \alpha = \sum a_ix_i$ (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 $S' \hookrightarrow R$.

On the other hand, there is an isomorphism on cotangent spaces induced by this inclusion $S' \hookrightarrow R$. In particular, the map on cotangent spaces is surjective, which implies that the original map must be surjective. Thus, the map from S' to R must be an isomorphism. □

Lemma 7.2. *Let S and R be as above and suppose that $\dim_{\mathbb{F}_p} J = 1$. Then exactly one of the following holds:*

- *$[\Gamma_S, \Gamma_S]\Gamma_S^p$ contains Γ_J.*
- *$S \cong R[x]/(x^2, px)$, for some $x \in S$.*

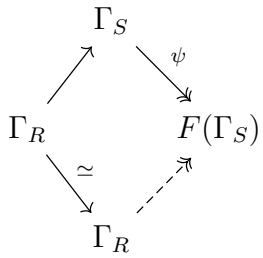
Proof. Note that $[\Gamma_S, \Gamma_S]\Gamma_S^p = \Gamma_{(I_S^2, pI_S)}$, so if $J \subset (I_S^2, pI_S)$, then the first statement holds. Assume now that J is not a subset of (I_S^2, pI_S). So, there exists $x \in J$ such that $x \notin (I_S^2, pI_S)$. Moreover, $x \notin (\mathfrak{m}_S^2, p)$. Thus, 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 7.1, 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 $S \cong S'[x]/(x^2, px) \cong R[x]/(x^2, px)$. □

Lemma 7.3. *Let S and R be as above. If $\Gamma_J \subset [\Gamma_S, \Gamma_S]\Gamma_S^p$, then there is no lift $\tilde{\Gamma} \to \mathrm{GL}_2(S)$.*

Proof. Suppose that $\Gamma_J \subset [\Gamma_S, \Gamma_S]\Gamma_S^p$ and suppose that there is a lift $\tilde{\Gamma} \to \mathrm{GL}_2(S)$. Then, we have the following commutative diagram:



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

Since $\Gamma_J \subset [\Gamma_S, \Gamma_S]\Gamma_S^p = \ker \psi$, it follows that ψ 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 quotiont 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. Therefore, there is no lift to $\mathrm{GL}_2(S)$ in this case. □

Lemma 7.4. *Let R and S be as above. Assume, moreover, that J is an $\mathbb{F}_p$-vector space of dimension n. Then exactly one of the following is true:*

(1) There is no lift $\tilde{\Gamma} \to \mathrm{GL}_2(S)$;
(2) $S \cong R[x_1, \ldots, x_n]/(x_i x_j, px_i)$, for some $x_i \in S$.

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

Base case: $n = 1$. By Lemma 7.2, we know that exactly one of the following holds:

(1) $\Gamma_J \subset [\Gamma_S, \Gamma_S]\Gamma_S^p$.
(2) $S \cong R[x]/(x^2, px)$, for some $x \in S$.

If (1) is true, then by Lemma 7.3, there is no lift $\tilde{\Gamma} \to \mathrm{GL}_2(S)$. If (2) is true, there is nothing to prove. This concludes the base case.

Inductive step: suppose 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 either there is no lift $\tilde{\Gamma} \to \mathrm{GL}_2(S)$ or $S \cong S_1[x_1]/(x_1^2, px_1)$. If the former is true, then the proof is complete. Assume 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 $S_1 \cong R[x_2, \ldots x_n]/(x_i x_j, px_i)$. Putting these two things together, we obtain that $S \cong R[x_1, \ldots x_n]/(x_i x_j, px_i)$. □

Proposition 7.5. *Let R and S be two local rings as above. Then there exists a splitting $R \to S$.*

Proof. Let I_R be the kernel of $R \twoheadrightarrow \mathbb{Z}_p$, I_S be the kernel of $S \twoheadrightarrow \mathbb{Z}_p$, and J be the kernel of $S \twoheadrightarrow R$. We will prove this result by induction on $\ell(S)$, where we define $\ell(S) = \ell(I_S)$, 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 7.4.

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

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

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 7.4, it follows that exactly one of the following is true

(1) There is no lift $\tilde{\Gamma} \to \mathrm{GL}_2(S')$;
(2) $S' \cong R[x_1, \ldots, x_n]/(x_i x_j, p x_i)$, for some $x_i \in S'$.

If there is no lift to $\mathrm{GL}_2(S')$, then there's no lift to $\mathrm{GL}_2(S)$, so there's nothing to be proved. The second case gives us a splitting $R \hookrightarrow S'$. We are in the following situation:

$$\begin{array}{ccccc} S & \xrightarrow{\pi} & S' & \longrightarrow & R \\ & & \uparrow & & \\ & & R & & \end{array}$$

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 induction step and the second map comes from the definition of S''. □

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

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

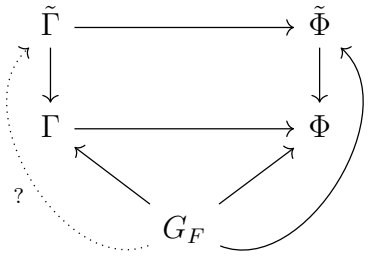
and a residual representation $\overline{\rho}\colon \tilde{\Gamma} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$. We have already proved that R is the universal deformation ring of $\overline{\rho}$. To prove that R is a universal everywhere unramified deformation ring of some residual representation, we need to find extensions $H/K/F$ with $\mathrm{Gal}(H/F) = \tilde{\Gamma}$ and H/K the maximal everywhere unramified pro-p extension of K. 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 we can reduce the problem to Φ, the projective image of $\tilde{\Phi}$: consider the following exact sequence

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

and its projective image

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

We are in the following case



To prove that there exists a lift $G_F \to \tilde{\Gamma}$, take two compatible set theoretic lifts. The centres $Z(\tilde{\Gamma}) = Z(\tilde{\Phi})$ are equal, so the 2-cocyles 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.

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 ([2]) and the Database of Number Fields `https://hobbes.la.asu.edu/NFDB/` ([9]). Note that this proof works for any regular prime $p \geq 5$ under the extra assumption that there exists a Φ-extension of $\mathbb{Q}(\zeta_p)$ with class number prime to p that satisfies property **P**.

Example. Let $p = 5$ and $\tilde{\Phi} = \tilde{A_4} = \mathrm{SL}_2(\mathbb{F}_3)$ (so $\Phi = A_4$). Let $E = \mathbb{Q}(\zeta_5)$ and let $\tilde{L_1}$ be the Galois closure of the field defined by the following polynomial over $\mathbb{Q}$:

$$x^8 - 5x^6 - 3x^5 + 28x^4 - 12x^3 - 80x^2 + 256.$$

This field has an intermediate field L_1, which is the Galois closure of the field defined by

$$x^4 - 21x^2 - 3x + 100.$$

Let $\tilde{L} = E.\tilde{L_1}$ and $L = E.L_1$. Then L is a subfield of $\tilde{L}$ and $\mathrm{Gal}(\tilde{L}/E) = \mathrm{SL}_2(\mathbb{F}_3) \twoheadrightarrow A_4 = \mathrm{Gal}(L/E)$. We used GP/Pari [2] to show that the class numbers of both L and $\tilde{L}$ are prime to 5 and that both L/E and $\tilde{L}/E$ satisfy property **P**. This concludes the proof for $p = 5$.

Example. Let $p = 7$ and $\tilde{\Phi} = \tilde{A_4} = \mathrm{SL}_2(\mathbb{F}_3)$ (so $\Phi = A_4$). Let $E = \mathbb{Q}(\zeta_7)$ and let $\tilde{L_1}$ be the Galois closure of the field defined by the following polynomial over $\mathbb{Q}$:

$$x^8 - x^7 - 11x^6 + 13x^5 + 32x^4 - 41x^3 - 23x^2 + 32x - 1.$$

This field has an intermediate field L_1, which is the Galois closure of the field defined by

$$x^4 - x^3 - 11x^2 + 4x + 12.$$

Let $\tilde{L} = E.\tilde{L_1}$ and $L = E.L_1$. Then L is a subfield of $\tilde{L}$ and $\mathrm{Gal}(\tilde{L}/E) = \mathrm{SL}_2(\mathbb{F}_3) \twoheadrightarrow A_4 = \mathrm{Gal}(L/E)$. We used GP/Pari [2] to show that the class numbers of both L and $\tilde{L}$ are prime to 7 and that both L/E and $\tilde{L}/E$ satisfy property **P**. This concludes the proof for $p = 7$.

Acknowledgements

I would like to thank my PhD advisor Frank Calegari for suggesting this problem, and for the constant support and helpful discussions on this topic. I also want to thank Professor Ravi Ramakrishna for taking the time to read the first draft of this paper and for all his valuable suggestions. I would also like to thank Sam Quinn for the useful comments and discussions throughout the project. Finally, I would like to thank Gal Porat for the help provided when I first started working on the proof of Proposition 2.2.

References

[1] P. B. Allen and F. Calegari, *Finiteness of unramified deformation rings*, Algebra & Number Theory, 8 (2014), pp. 2263–2272.

[2] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier, *User's Guide to PARI-GP*, Laboratoire A2X, Université Bordeaux I, France, 1998.

[3] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, in Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), vol. I of Ser. Number Theory, Int. Press, Cambridge, MA, 1995, pp. 41–78.

[4] G. Gras, *Théorèmes de réflexion*, J. Théor. Nombres Bordeaux, 10 (1998), pp. 399–499.

[5] F. Hajir and C. Maire, *Analytic lie extensions of number fields with cyclic fixed points and tame ramification*, arXiv:1710.09214, (2017).

[6] F. Hajir, C. Maire, and R. Ramakrishna, *On Ozaki's theorem realizing prescribed p-groups as p-class tower groups*, arXiv:2204.08408, (2022).

[7] K. Hoechsmann, *Zum Einbettungsproblem*, J. Reine Angew. Math., 229 (1968), pp. 81–106.

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

[9] J. W. Jones and D. P. Roberts, *A database of number fields*, LMS J. Comput. Math., 17 (2014), pp. 595–618.

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

[11] J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math., 21 (1973), pp. 59–116.

[12] M. Ozaki, *Construction of maximal unramified p-extensions with prescribed Galois groups*, Invent. Math., 183 (2011), pp. 649–680.

[13] M. J. Razar, *Central and genus class fields and the Hasse norm theorem*, Compositio Math., 35 (1977), pp. 281–298.

[14] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., 15 (1972), pp. 259–331.

[15] ——, *Linear representations of finite groups*, vol. Vol. 42 of Graduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, french ed., 1977.

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

[17] P. Webb, *A course in finite group representation theory*, vol. 161 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 2016.

The University of Chicago, 5734 S University Ave, Chicago, IL 60637, USA
Email address: aiorga@uchicago.edu