MURPHY’S LAW FOR GALOIS DEFORMATION RINGS

ANDREEA IORGA

Abstract. In this paper, we prove, under a specific assumption, that any semi-direct product of a \( p \)-group \( G \) with a group of order prime-to-\( p \) \( \Phi \) can appear as the Galois group of a tower of extensions \( H/F/E \) with the property that \( H \) is the maximal pro-\( p \) extension of \( F \) that is unramified everywhere, and \( \text{Gal}(H/F) = G \). 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 be written as an universal everywhere unramified deformation ring.

1. Introduction

Let \( p \) be a prime. Let \( \Phi \) be a finite group of order prime to \( p \), and let \( G \) be a finite \( p \)-group with an action of \( \Phi \). Let \( \Gamma = G \rtimes \Phi \) be the semi-direct product of \( G \) and \( \Phi \) corresponding to the given action of \( \Phi \) on \( G \). For any number field \( F \), let \( L_p(F) \) denote the maximal unramified \( p \)-extension of \( F \). If \( \Phi \) 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]) gives both a simplification (the base field can have arbitrary signature, as long as its class number is prime to \( p \)) and an extension (the degree of the base field over \( \mathbb{Q} \) can be controlled) of Ozaki’s result. In this paper, we prove a different generalization:

Theorem 1.1. Assume there exists an extension \( L/K \) such that

- \( L/K \) is Galois with Galois group \( \Phi \),
- \( K \) contains \( \mu_p \),
- \( L \) has class number prime to \( p \),
- \( L/K \) satisfies property \( P \) below.

Then there exist number fields \( H/F/E \) such that

1. \( H/F \) is the maximal pro-\( p \) extension of \( F \) that is unramified everywhere,
2. \( \text{Gal}(H/F) = G \),
3. \( \text{Gal}(H/E) = \Gamma \),
4. \( H/E \) satisfies property \( P \) below.

Definition 1.1. We say that an extension \( L/K \) has property \( P \) if for all primes \( p \) of \( K \), and \( \mathfrak{p} \mid p \), 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 number of elements of the residue field of \( K_{\mathfrak{p}} \).

When \( \Phi \) is trivial, we can recover Ozaki’s result in the case when \( p \) is a regular prime, a similar hypothesis 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 1.1 is Theorem 1.2 below. Consider a continuous absolutely irreducible residual Galois representation \( \overline{\rho} : G_K \rightarrow \text{GL}_2(\mathbb{F}_p) \). One can
associate to $\mathfrak{p}$ a number of deformation rings. These pro-represent functors of deformations to the category $\mathcal{C}$ of local Artinian rings $(A, m)$ with $A/m = \mathbb{F}_p$.

**Definition 1.2.** Consider a deformation $\rho: G_F \to \text{GL}_2(A)$ of $\mathcal{C}$ for a finite $(A, m)$. It factors through some finite group, and the fixed field of the kernel is a finite extension; call it $F(\rho)$. We say that $\rho$ is unramified if the extension $F(\rho)/F(\mathcal{C})$ 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 $\rho$?

Assume that the image of $\rho$ has order prime to $p$, so its projective image is $A_4$, $S_4$ or $A_5$ (Proposition 16 in [14]). The Unramified Fontaine-Mazur Conjecture (Conjecture 5a in [3]) predicts that the only $\mathbb{Q}_p$-points will have finite image. Moreover, the tangent space to any $\mathbb{Q}_p$-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 $\mathbb{Q}_p$. 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 1.2.** 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.

The proof of this result can be found in the last section. In fact, Section 7 presents a proof that works in general for any regular prime $p \geq 5$ with the assumption that there exists an $A_4$ (or $S_4$ or $A_5$) extension of $\mathbb{Q}(\zeta_p)$ with class number prime to $p$ that satisfies property $P$.

### 2. Strategy for proving Theorem 1.1

Theorem 1.1 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 $\Phi$ 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 $\mu_p$, 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 $[F: \mathbb{Q}] \geq 2(2d(G) + r(G) + d(\Phi))$, where $d(G)$ is the minimal number of generators $G$ and $r(G)$ is the minimal number of relations of $G$.

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 $\text{Gal}(L_p(K')/F') \cong \Gamma$. Moreover, if the initial extension $K/F$ satisfies property $P$, then the new extension $K'/F'$ also satisfies property $P$.

**Proposition 2.2.** Let $K/F$ be a Galois extension of number fields satisfying the four conditions of Proposition 2.1 and property $P$. Assume $\Phi$ 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 $K'/F'$ such that

1. $F \subset F'$ and $K \subset K'$,

...
(2) The extension $K'/F'$ is Galois and has Galois group isomorphic to $\Phi$,
(3) The extension $L_p(K')/F'$ is Galois and has Galois group isomorphic to $\Gamma'$,
(4) Every prime of $F'$ lying over $p$ splits completely in $L_p(K')$,
(5) The extension $L_p(K')/F'$ satisfies property $P$.

The proof of Theorem 1.1 is inspired by Ozaki’s results, and follows from Propositions 2.1 and 2.2 by induction. Restrict to $p$-groups $G$ such that the filtered irreducible $\mathbb{F}_p[\Phi]$-representations are all isomorphic to $V$. For any $p$-group in our category, there exists a sequence of $p$-groups with surjections

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

such that $\ker(G_i \to G_{i-1}) = V$ 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 $V$. The assumption of Theorem 1.1 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 $\Gamma_i$. 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 $\text{Gal}(L_p(K'_i)/F'_i) \cong \Gamma_i$ and $[F'_i: \mathbb{Q}] \geq 2(2d(G_{i+1}) + r(G_{i+1}) + d(\Phi))$. 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 $F'_i \subset F_{i+1}$, $K'_i \subset K_{i+1}$, and $\text{Gal}(K_{i+1}/F_{i+1}) \cong \Phi$, $\text{Gal}(L_p(K_{i+1})/F_{i+1}) \cong \Gamma_{i+1}$, 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 $E = F_n$, $F = K_n$ 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 $U_p(F)$ be the pro-$p$-part of the local unit group of the complete field $F_p$ of $F$ at $p$ and $U(F) = \bigoplus_{p|\mathfrak{p}} U_p(F)$. We embed the unit group of the localisation $\mathcal{O}_{F,p}$ of the maximal order $\mathcal{O}_F$ of $F$ at $p$ diagonally into $U(F)$ as usual, and let $U_p^0(F)$ be the submodule of $U_p(F)$ consisting of all the elements $u$ such that $F_p(\sqrt[p]{u})/F_p$ is unramified; let $U'(F) = \bigoplus_{p|\mathfrak{p}} U'_p(F)$. 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 $\Phi$ as above, then

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

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

Proof. Note that $U(F) = \bigoplus_{p|\mathfrak{p}} U_p(F) = \bigoplus_{p|\mathfrak{p}} \mathcal{O}_{F_p}^\times \otimes_{\mathbb{Z}_p} \mathbb{Z}_p$. Tensoring with $\mathbb{F}_p$ and taking the quotient by $p$-powers, we obtain that $(\mathcal{O}_{F_p}^\times \otimes_{\mathbb{Z}_p} \mathbb{Z}_p)^p \cong \mathbb{F}_p^{d+1}$, where $d = [F_p: \mathbb{Q}_p] = [F: \mathbb{Q}]$. It follows that $R(F) \cong \mathbb{F}_p^{[F: \mathbb{Q}]s}$. Similarly, $R'(F) \cong \mathbb{F}_p^{[F: \mathbb{Q}]s}$.

Because every prime of $F$ lying over $p$ splits completely in $K/F$, we have a natural isomorphism of $\Phi$-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 $R(K) \cong \mathbb{F}_p[\Phi][F: \mathbb{Q}]^s$ and $R'(K) \cong \mathbb{F}_p[\Phi][F: \mathbb{Q}]^s$. 

MURPHY'S LAW FOR GALOIS DEFORMATION RINGS
Similarly, since every prime of $F$ lying over $p$ splits completely in $L_p(K)/F$, we obtain that $R(L_p(K)) \cong \mathbb{F}_p[\Gamma|F: \mathbb{Q}]^{+*}$ and $R'(L_p(K)) \cong \mathbb{F}_p[\Gamma|F: \mathbb{Q}]$.

**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 $\text{Gal}(F_S/F)$ at the prime $v$. We assume that the map $\bigoplus_v H_2(D_v, \mathbb{Z}) \to H_2(\text{Gal}(F_S/F), \mathbb{Z})$ induced by the natural inclusion $D_v \subset \text{Gal}(F_S/F)$ is surjective. Then $L_p(F_S) = F_S$.

**Corollary 3.3.** Under the assumptions of Lemma 3.2, if $F_S/F$ is a cyclic extension, then $L_p(F_S) = F_S$.

**Proof.** See Lemma 7 in [12].

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 $\tau \in \text{Gal}(\tilde{M}/M)$, there exist infinitely many prime ideals $\Lambda O_M$ of $O_M$ such that $\Lambda O_M$ is prime to $p$, $(\Lambda \mod U(M)) = u$ in $R(M)$, and $(\Lambda O_M, \tilde{M}/M) = \tau$.

**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

$$O_M^* \otimes_p \mathbb{F}_p \to R(M) \xrightarrow{\rho} \text{Gal}(L/M) \xrightarrow{f} \text{Gal}(H/M) \to 1,$$

where the map $\rho: R(M) \to \text{Gal}(L/M)$ is the map induced by class field theory, and the third map is the natural surjection $f: \text{Gal}(L/M) \to \text{Gal}(H/M)$. Let $\sigma = \rho(u) \in \text{Gal}(L/M)$. 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 $\tilde{\sigma} \in \text{Gal}(\tilde{L}/M)$ be an element with the properties that $\text{res}(\tilde{\sigma})|_{L} = \sigma^{-1}$ and $\text{res}(\tilde{\sigma})|_{N} = 1$. Such an element exists because $L$ and $N$ are linearly disjoint over $H$, and the restrictions $\sigma^{-1} \in \text{Gal}(L/M)$ and $1 \in \text{Gal}(H/M)$ agree on $H/M$, since $\text{res}(\sigma^{-1})|_H = \text{res}(1)|_H$ if and only if $\sigma^{-1} \in \ker(f) = \text{Im}(\rho)$, which is true by construction.

By Chebotarev density theorem, there are infinitely many degree one primes $\alpha$ of $O_M$ 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 $\alpha$ is a principal ideal in $O_M$, so there exists $\Lambda_0 \in M$ such that $\alpha = \Lambda_0 O_M$. Combining this with the first condition, we obtain that $\Lambda_0 = \Lambda_0 \varepsilon$, for some $\varepsilon \in O_M^*$ and some $\Lambda \in M$. The element $\Lambda$ has the properties $(\Lambda \mod U(M)) = u$ in $R(M)$ and $(\Lambda O_M, \tilde{M}/M) = \tau$, which is what we wanted.  

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 $G \times \Phi$, where $G$ is a $p$-group and $\Phi$ 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 $\Lambda$ of $L_p(K)$ such that

1. The ideal $\Delta O_{L_p(K)}$ 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 $L_p(K)(\sqrt{\eta})$ is the maximal elementary abelian $p$-extension of $L_p(K)$ unramified outside $S$.

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

**Proof.** Since $\eta O_F$ is a prime ideal of $O_F$, it follows that $\sqrt{\eta} \not\in F$, 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 $\Gamma$.

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 $F'.L_p(K) = L_p(K)(\sqrt{\eta})$ and $K'.L_p(K) = L_p(K)(\sqrt{\eta})$. By construction, $L_p(K)(\sqrt{\eta})$ is the maximal elementary abelian $p$-extension of $L_p(K)$ unramified outside $S$, so Corollary 3.3 tells us that $L_p(L_p(K)(\sqrt{\eta})) = L_p(K)(\sqrt{\eta})$. 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

$$
\begin{array}{ccc}
L_p(K) & \xrightarrow{F'} & F'\\
\downarrow & & \downarrow \\
L_p(K') & = & F'.L_p(K) \\
\downarrow & & \\
F & &
\end{array}
$$

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

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

Now, assume that \( \Lambda \) has property (1). If \( L_p(K)(\sqrt[p]{\alpha})/L_p(K) \) is unramified outside \( S \), for some \( \alpha \in L_p(K) \), then

\[
\alpha \mod L_p(K)^{xp} \equiv (\varepsilon \mod L_p(K)^{xp}) + \sum_{\sigma \in \Gamma} a_\sigma(\sigma\Lambda \mod L_p(K)^{xp}),
\]

with \( a_\sigma \in \mathbb{F}_p \), \( \varepsilon \in \mathcal{O}_{L_p(K)}^x \). 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 holds only for \( \varepsilon \in (\mathcal{O}_{L_p(K)}^x)^p \) 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 \( \mathcal{O}_{L_p(K)}^x \otimes \mathbb{F}_p \to R'(L_p(K)) \). The extension \( L_p(K)(\sqrt[p]{\varepsilon})/L_p(K) \) must be ramified at some prime lying over \( p \), for any \( \varepsilon \in \mathcal{O}_{L_p(K)}^x \setminus (\mathcal{O}_{L_p(K)}^x)^p \), so this map is injective: \( E \cong \mathcal{O}_{L_p(K)}^x \otimes \mathbb{F}_p \). It follows that the map \( \mathcal{O}_{L_p(K)}^x \otimes \mathbb{F}_p \to R(L_p(K)) \) 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 \( \Gamma = \mathbb{G} \times \Phi \) (for \( G \) a \( p \)-group and \( \Phi \) a prime-to-\( p \) group). To deal with this, we turn to the theory of modular representations for groups of the form \( \mathbb{G} \times \Phi \) ([16]) 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 \( M, Q \) of \( R(L_p(K)) \) such that

- \( R(L_p(K)) = M \oplus N \oplus Q \) and \( R'(L_p(K)) = M \oplus Q \).
- \( E \subseteq M \).
- \( \mathrm{rank}_{\mathbb{F}_p[\Gamma]} Q \geq \frac{1}{2}[F: \mathbb{Q}] - d(G) - r(G) \).

**Proof.** Since \( \Phi \) 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 [16]). 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 \( n_S = \dim_D(S), D = \mathrm{End}_{\mathbb{F}_p[\Phi]} S \).

Note that any \( \mathbb{F}_p[\Gamma] \)-module has a unique injective hull and that injective \( \mathbb{F}_p[\Gamma] \)-modules are the same as projective \( \mathbb{F}_p[\Gamma] \)-modules (see Section 8.5 in [16]). Thus, the \( \mathbb{F}_p[\Gamma] \)-module \( E \)
has an injective hull \( \tilde{M} = \oplus P_S^{\alpha_S} \). Consider the following diagram

\[
\begin{array}{ccc}
E & \xleftarrow{f} & \tilde{M} \\
\downarrow{i} & & \kappa \downarrow{g} \\
R(L_p(K)) & & \\
\end{array}
\]

The map \( i \) is the usual inclusion map from \( E \) to the injective module \( R(L_p(K)) \). 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 \( g: \tilde{M} \to R(L_p(K)) \) such that \( g \circ f = i \). Moreover, since \( f \) is an essential monomorphism, the map \( g \) is injective. Let \( M_1 = \text{Im}(g) \subset R(L_p(K)) \); the module \( E \) can be seen as a submodule of \( M_1 \).

Consider the module \( N \). By definition, we have a short exact sequence of \( \mathbb{F}_p[\Gamma] \)-modules

\[ 1 \to N \to R(L_p(K)) \to R'(L_p(K)) \to 1 \]

that 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 \( M_1 \cap N \). If this intersection is nonempty, then the socle of \( M_1 \cap N \) must be nonempty. Moreover, \( M_1 \cap N \) is a submodule of \( M_1 \). Using the facts that \( \text{Soc} E = \text{Soc} M_1 \), \( \text{Soc} K \subseteq K \) and \( \text{Soc} K = K \cap \text{Soc} M_1 \), for all submodules \( K \) of \( M_1 \), we obtain

\[
\text{Soc}(M_1 \cap N) = (M_1 \cap N) \cap \text{Soc} M_1 \\
= N \cap \text{Soc} M_1 \\
= N \cap \text{Soc} E \\
\subseteq N \cap E \\
= 0.
\]

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 \( \alpha_S + \beta_S = [F: \mathbb{Q}] \cdot n_S \).

We would like to estimate \( \beta_S \). Let \( r = \text{rank}_{\mathbb{F}_p[\Phi]} E^G = \text{rank}_{\mathbb{F}_p[\Phi]}(E^G)^* = \text{rank}_{\mathbb{F}_p[\Phi]}(E^*)_G \).

Thus, \( \mathbb{F}_p[\Phi]^r \to (E^*)_G \). By Nakayama’s Lemma, \( \mathbb{F}_p[\Gamma]^r \to E^* \). Taking duals and using the fact that \( \mathbb{F}_p[\Gamma] \) is self-dual, we obtain that \( E \cong E^{**} \to \mathbb{F}_p[\Gamma]^r \). Since \( \tilde{M} \) is the injective hull of \( E \) and \( \mathbb{F}_p[\Gamma] \) is an injective module, we obtain that \( \tilde{M} \to \mathbb{F}_p[\Gamma]^r \), 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

\[ 0 \to \mathcal{O}_{L_p(K)/\mu_p}^x \to \mathcal{O}_{L_p(K)}^x \to \mathcal{O}_{L_p(K)/\mu_p}^x \to 0, \]

we derive the sequence

\[
(\mathcal{O}_{L_p(K)/\mu_p}^x)^G \to (\mathcal{O}_{L_p(K)}^x)^G \to (\mathcal{O}_{L_p(K)/\mu_p}^x)^G \to H^1(G, \mathcal{O}_{L_p(K)/\mu_p}^x).
\]

We observe that
\[ (\mathcal{O}_{L_p(K)}/p)^G = E^G, \]
\[ (\mathcal{O}_{L_p(K)}^\times)^G / (\mathcal{O}_{L_p(K)}/\mu_p)^G \cong \mathcal{O}_K^\times / \mathcal{O}_K^{\times p}, \]
so the sequence becomes
\[ \mathcal{O}_K^\times / \mathcal{O}_K^{\times p} \rightarrow E^G \rightarrow H^1(G, \mathcal{O}_{L_p(K)}/\mu_p). \]

On the other hand, from the exact sequence
\[ 0 \rightarrow \mu_p \rightarrow \mathcal{O}_{L_p(K)}^\times \rightarrow \mathcal{O}_{L_p(K)}^\times / \mu_p \rightarrow 0, \]
we get the exact sequence
\[ H^1(G, \mathcal{O}_{L_p(K)}^\times) \rightarrow H^1(G, \mathcal{O}_{L_p(K)}^\times / \mu_p) \rightarrow H^2(G, \mu_p). \]
The \( p \)-group \( G \) acts trivially on \( \mu_p \), so for \( i = 1, 2 \), the groups \( H^i(G, \mu_p) \) describe the generators and relations of \( G \).

Now, if \( j: \text{Cl}_K \rightarrow \text{Cl}_{L_p(K)} \) is the map induced by the inclusion \( K \hookrightarrow L_p(K) \), then \( H^1(G, \mathcal{O}_{L_p(K)}^\times) \cong \text{ker } j \) (see 2 in [8]). Moreover, \( \text{ker } j \) is equal to the \( p \)-primary part of \( \text{Cl}_K \), which is isomorphic to \( \text{Gal}(L_p(K)/K)^{ab} = G^{ab} \), 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
\[ \text{rank}_{\mathbb{F}_p[\Gamma]}(\mathcal{O}_K^\times / \mathcal{O}_K^{\times p}) \leq \frac{1}{2} [F : \mathbb{Q}]. \]

From 1, 2 and 3 it follows that
\[ r = \text{rank}_{\mathbb{F}_p[\Gamma]}(E^G) \leq \text{rank}(\mathcal{O}_K^\times / \mathcal{O}_K^{\times p}) + d_p H^1(G, \mathcal{O}_{L_p(K)}^\times / \mu_p) \]
\[ \leq \text{rank}(\mathcal{O}_K^\times / \mathcal{O}_K^{\times p}) + d_p H^1(G, \mathcal{O}_{L_p(K)}^\times) + d_p H^2(G, \mu_p) \]
\[ \leq \frac{1}{2} [F : \mathbb{Q}] + d(G) + r(G), \]
where \( d_p \) is the usual \( p \)-rank, and \( d(G) \) and \( r(G) \) are the number of generators and relations of \( G \). Therefore:
\[ \beta_S = [F : \mathbb{Q}] \cdot n_S - \alpha_S \]
\[ \geq [F : \mathbb{Q}] \cdot n_S - n_S \cdot r \]
\[ \geq [F : \mathbb{Q}] \cdot n_S - n_S \cdot \left( \frac{1}{2} [F : \mathbb{Q}] + d(G) + r(G) \right) \]
\[ \geq n_S \left( \frac{1}{2} [F : \mathbb{Q}] - d(G) - r(G) \right). \]

We can thus choose \( t \geq (\frac{1}{2} [F : \mathbb{Q}] - d(G) - r(G)) \) such that \( Q := \bigoplus P_{S^{t-1}}^n \) 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 \( \text{rank}_{\mathbb{F}_p[\Gamma]} Q \geq \frac{1}{2} [F : \mathbb{Q}] - d(G) - r(G) \).
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. \( \square \)
The only thing left to show is the existence of a prime $\Lambda$ 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,

$$t \geq \frac{1}{2} |F: Q| - d(G) - r(G) \geq d(G) + d(\Phi) \geq d(\Gamma).$$

Let $\{\sigma_1, \ldots, \sigma_d\}$ be a system of minimal generators for $\Gamma$, $d = d(\Gamma)$. 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 $\Lambda O_{L_p(K)}$ a prime of degree 1, not lying over $p$, such that $u = (\Lambda \mod U(L_p(K))^p)$. Assume that there exist $\varepsilon \in \mathcal{O}_{L_p(K)}^x$ 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:

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

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 $U(L_p(K))^p \cap \mathcal{O}_{L_p(K)}^x = \mathcal{O}_{L_p(K)}^{xp}$, it follows that $\varepsilon \in \mathcal{O}_{L_p(K)}^{xp}$. On the other hand, $\sum_{\sigma \in \Gamma} a_\sigma (\sigma \Lambda \mod U(L_p(K))^p) = 0$ implies $\sum_{\sigma \in \Gamma} a_\sigma \sum_{i=1}^{d} (\sigma_i - 1)q_i = 0$. This implies $\sum_{\sigma \in \Gamma} a_\sigma (\sigma_i - 1) = 0$, for all $1 \leq i \leq d$, so $\sum_{\sigma \in \Gamma} a_\sigma (\tau - 1) = 0$, for all $\tau \in \Gamma$, meaning that $a_\sigma$ 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 $\Lambda$ 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 $(\varepsilon): 1 \to A \to E \to G \to 1$, the embedding problem $(G_F, \varepsilon)$ is defined by the diagram

$$
\begin{array}{c}
G_F \\
\downarrow \varphi \\
1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1,
\end{array}
$$

where $\varphi$ is the canonical surjection. A continuous homomorphism $\psi: G_F \to E$ is called a solution of $(G_F, \varepsilon)$ if it satisfies the condition $\pi \circ \psi = \varphi$. A solution $\psi$ is called a proper solution if it is surjective. If $(\varepsilon)$ 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 $\text{Gal}(M/F) \cong E$ compatibly with $\text{Gal}(K/F) = G$. When such a solution exists, we say that $(G_F, \varepsilon)$ is solvable.

For each prime $p$ of $F$, we denote by $F_p$ (resp. $K_p$) the completion of $F$ at $p$ (resp. of $K$ at a prime above $p$). Let $G_{F_p}$ be the absolute Galois group of $F_p$, $G_p = \varphi(G_{F_p}) \subset G$ (which is
isomorphic to the decomposition group of \( p \) in \( \text{Gal}(K/F) \) and \( E_p = \pi^{-1}(G_p) \subset E \). Then the local embedding problem \((G_{F_p}, \varepsilon_p)\) is defined by

\[
\begin{array}{c}
G_{F_p} \\
\downarrow \varepsilon_p \\
1 \rightarrow A \rightarrow E_p \rightarrow \pi_p \rightarrow G_p \rightarrow 1
\end{array}
\]

We have the following results from [11] (Satz 2.2, Satz 4.7, Satz 5.1).

**Theorem 5.1.** Let \((G_F, \varepsilon)\) be an embedding problem with abelian kernel \( A \). If the map

\[ H^2(G_F, A) \rightarrow \prod_{p \in P} H^2(G_{F_p}, A) \]

is injective, then the embedding problem \((G_F, \varepsilon)\) has a solution if and only if the local embedding problems \((G_{F_p}, \varepsilon_p)\) have solutions, for all \( p \in P \). 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

\[ H^q(F, A) \rightarrow \prod_{p \in P} H^q(F_p, A), \quad q \geq 0, \]

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

**Theorem 5.3.** If \( K_p/F_p \) is a cyclic extension of local fields, then the following conditions are equivalent.

(i) Every embedding problem corresponding to the extension \( K_p/F_p \) with an arbitrary (not necessarily abelian) kernel \( A \) of exponent \( n \) is solvable.

(ii) Every \( n \)-th root of unity in \( F_p \) is the norm of an element of \( K_p \).

This is always true if \( K_p/F_p \) is unramified.

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

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

\[
\begin{array}{c}
G_F \\
\downarrow \\
1 \rightarrow V \rightarrow \Gamma' \rightarrow \Gamma \rightarrow 1
\end{array}
\]

with \( \text{Gal}(L_p(K)/F) = \Gamma = G \rtimes \Phi, \text{Gal}(K/F) = \Phi, \) and \( K/F \) satisfies property \( \mathcal{P} \) (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

\[ H^2(G_F, V) \rightarrow \prod_{p \in P} H^2(G_{F_p}, V) \]

is injective. Note that \( V \) is not a trivial \( F_p[\Gamma] \)-module, so we can’t apply Theorem 5.2 directly. Consider the following commutative diagram

\[
\begin{array}{c}
1 \rightarrow A \rightarrow E_p \rightarrow \pi_p \rightarrow G_p \rightarrow 1
\end{array}
\]
Using spectral sequences, we can prove that $H^2(G_K, V) \cong H^2(G_F, V)$, so the map on the left is injective. Similarly, it can be proved that the map on the right is injective. Since $K = F^{\ker \overline{\rho}}$, where $\overline{\rho} : G_F \to \text{GL}_2(\mathbb{F}_p)$ is irreducible and has image $\Phi$, 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 $n = \dim \nabla V$. 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 $M = L_p(K)(\sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_n})/F$, with $\alpha_1, \ldots, \alpha_n \in K$, and $\text{Gal}(M/F) \cong \Gamma' \cong V \rtimes \Gamma$. 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 $\Phi$ that satisfies property $P$. Consider the extension $L_p(K)/F$ with Galois group $\Gamma$. The embedding problem

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

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

### 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 $n = \dim \nabla V$ and let $m = |\Phi|$. Let $1 = g_1, \ldots, g_n$ be generators of the action of $\Phi$ on $V$. Let $T = \frac{(\nu^{2n-1} - p^{2n-1})(\nu^{2n-1} - p^{2n})}{(p^{2n} - 1)(p^{2n} - p)}$. We can assume that $[F : \mathbb{Q}] \geq 2d(T + 2)$, where $d = d(\Phi)$ is the number of generators of $\Phi$, 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 $R'(L_p(K))^G \cong R'(K)$, $N^G \cong \ker(R(K) \to R'(K))$, and $(\mathcal{O}_K^K \otimes \mathbb{F}_p) \cap Q^G = 0$, where $Q$ is the $\mathbb{F}_p[\Gamma]$-module obtained in Lemma 4.2. Now, let $\{\sigma_1, \ldots, \sigma_d\}$ be a generator system of $\Phi$, and let $Q^G = \bigoplus_{i=1}^t \mathbb{F}_p[\Phi] q_i$ be a system of free basis of the free $\mathbb{F}_p[\Phi]$-module $Q^G$, with $t \geq d(T + 2)$.

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 $p$ and let
\( \tau = 1 \in \text{Gal}(\overline{M}/K) \). 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 \( \lambda_i \equiv 1 \pmod{p} \) and

\[
\lambda_i \quad \text{mod} \quad U(K)^p = \sum_{j=1}^{d} (1 + \sigma_j)q(i-1)d+j
\]

in \( R(K) \), for \( 1 \leq i \leq T \).

Since \( \Phi \) has order prime to \( p \), the group algebra \( \mathbb{F}_p[\Phi] \) is semisimple, so it can be decomposed as a direct sum of isotypic components. Recall that \( R(K) \) is a free \( \mathbb{F}_p[\Phi] \)-module, so \( R(K) \) can be decomposed as a direct sum of isotypic components:

\[
R(K) = \bigoplus_W W^{nw},
\]

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 \( a_W \in W^{nw} \). The isotypic projection \( P_W \) of \( R(K) \) onto \( W^{nw} \) is given by the formula

\[
P_W = \frac{\dim W}{|\Phi| \cdot \dim_{\mathbb{F}_p} \text{End} W} \sum_{g \in \Phi} \chi_W(g^{-1})g,
\]

where \( \chi_W \) 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 \( P_W(P_U(a)) = a \) if \( U \cong W \) and \( P_W(P_U(a)) = 0 \) if \( U \not\cong W \). To ease notation, we will write \( n_{g,W} = \dim W \chi_W(g^{-1}) \), which is well-defined in \( \mathbb{F}_p \) and nonzero for \( g = g_i, 1 \leq i \leq n \), for the specific groups \( \Phi \) we are considering. We can then write \( P_W(a) = \sum n_{g,W} g(a) \).

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 \( \mathbb{F}_p^{2n} \) that are not multiples of each other. There are \( \frac{(p^{2n} - p)(p^{2n} - 1)}{(p^2 - p)(p^2 - 1)} \) such distinct pairs; 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 \( \lambda_\ell \) (we can do this since \( T = \frac{(p^{2n} - p)(p^{2n} - 1)}{(p^2 - p)(p^2 - 1)} \)) and define \( v_1 \) and \( v_2 \) to be products of conjugates of \( \lambda_\ell \), with \( 1 \leq \ell \leq T \), with the properties that the exponents of \( \lambda_\ell, g_2^{-1}(\lambda_\ell), \ldots g_n^{-1}(\lambda_\ell) \) in \( v_1 \) are \( a_1, \ldots, a_n \), and the exponents of \( \lambda_\ell, g_2^{-1}(\lambda_\ell), \ldots g_n^{-1}(\lambda_\ell) \) in \( v_2 \) 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 \( v_1 = \prod_{i=1}^{T} g(\lambda_i)^{a_{i,\ell}} \) and \( v_2 = \prod_{i=1}^{T} g(\lambda_i)^{b_{i,\ell}} \). For each \( \ell \), let \( r_\ell \) be a non-

\( p \)-power modulo \( \lambda_\ell \). Write \( g_i(v_1) = \lambda_{\ell}^{a_{i,\ell}}u_{i,\ell} \) and \( g_i(v_2) = \lambda_{\ell}^{b_{i,\ell}}z_{i,\ell} \), for all \( 1 \leq i \leq n \), with \( u_{i,\ell} \) and \( z_{i,\ell} \) not divisible by \( \lambda_\ell \). We distinguish two cases, each containing two subcases:

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

\[
\begin{align*}
  c_{j,\ell} &= x_{j,\ell}a_{i,\ell} - x_{i,\ell}a_{j,\ell}, & \text{for } j \neq i, \\
  d_{j,\ell} &= y_{j,\ell}a_{i,\ell} - y_{i,\ell}b_{j,\ell}, & \text{for all } j.
\end{align*}
\]

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

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

\[
B_{k,\ell} = r_{\ell} \cdot d_{k,\ell} \cdot z_{k,\ell}^{-1}, \text{ for all } k.
\]

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

\[
A_{k,\ell} = \begin{cases} 
  u_{k,\ell}^{-1} & \text{if } k = i \\
  r_{\ell} \cdot d_{k,\ell}^{i,\ell} \cdot u_{k,\ell}^{-1} & \text{otherwise.}
\end{cases}
\]

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

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

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

\[
d_{j,\ell} = y_{j,\ell} b_{i,\ell} - y_{i,\ell} b_{j,\ell}, \text{ for } j \neq i.
\]

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

\[
A_{k,\ell} = r_{\ell} \cdot d_{i,\ell} \cdot z_{k,\ell}^{-1}, \text{ for all } k.
\]

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

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

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

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

Let \( R = \prod_{i,\ell} g_{i,\ell}^{-1}(\lambda_\ell). \) We would like to construct a prime \( \alpha \) of \( \mathcal{O}_K \) with \( \alpha \equiv g_i^{-1}(A_i,\ell) \mod g_i^{-1}(\lambda_\ell) \), for all \( i \) and \( \ell \). Since the ideals \( g_i^{-1}(\lambda_\ell) \mathcal{O}_K \) are pairwise coprime, the Chinese remainder theorem tells us that constructing such an \( \alpha \) is equivalent to constructing an \( \alpha \) that satisfies a specific congruence modulo \( R \mathcal{O}_K \), say \( \alpha \equiv r_1 \mod R \), compatible with \( \alpha \equiv g_i^{-1}(A_i,\ell) \mod g_i^{-1}(\lambda_\ell) \). Similarly, to construct a prime \( \beta \) of \( \mathcal{O}_K \) with \( \beta \equiv g_i^{-1}(B_i,\ell) \mod g_i^{-1}(\lambda_\ell) \), it is enough to construct a prime \( \beta \) with a specific compatible congruence modulo \( R \mathcal{O}_K \), say \( \beta \equiv r_2 \mod R \). 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 $RO_K$. Use Lemma 3.4 with $M = K$ again to find two primes $\alpha$ and $\beta$ of $O_K$ that split completely in $L_p(K)/K$, prime to $p$, such that

$$\alpha \mod U(K)^p = -P_v(v_1) + \sum_{W \neq V} P_W \left( \sum_{j=1}^{d} (1 + \sigma_j)q_{Md+j} \right)$$

and

$$\beta \mod U(K)^p = -P_v(v_2) + \sum_{W \neq V} P_W \left( \sum_{j=1}^{d} (1 + \sigma_j)q_{(M+1)d+j} \right)$$

in $R(K)$, and

$$\alpha \equiv r_1 \pmod R$$
$$\beta \equiv r_2 \pmod R.$$

Observe that while taking projections $P_V(v_1)$ and $P_V(v_2)$ modifies the exponents of the primes $\lambda_i$ in $v_1$ and $v_2$ after reordering, we still have all the exponents.

Note that $K^x/K^{xp}$ is an $F_p[\Phi]$-module, so we can consider the projections to the $V$-eigenspace of $v_1\alpha$ and $v_2\beta$. Construct $K_1$ to be the Galois closure of $K(\sqrt[\Phi]{P_v(v_1\alpha)})$ over $F$, and $K_2$ to be the Galois closure of $K(\sqrt[\Phi]{P_v(v_2\beta)})$ over $F$. Then $Gal(K_1/F) \cong Gal(K_2/F) \cong V \times \Phi$. Moreover, since $P_V(v_1\alpha) = 0$ 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 $g(\alpha_i), g(\beta), g(\lambda_i)$ 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 $Gal(\tilde{L}/L_p(K))$ 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 $P_V(v_1\alpha)$ in $R(K)$. By construction, $P_V(v_1\alpha) = 0$ in $R(K)$, so it must remain trivial in $R'(K)$. Similarly, $P_V(v_2\beta) = 0$ 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 $S, K(\sqrt[\Phi]{\gamma})/K$. Then

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

for some $\eta \in O_K^\times$ and $a_g, b_g, c_{g,i} \in \mathbb{Z}$, for $1 \leq i \leq T$ and $g \in \Phi$. Since $K(\sqrt[\Phi]{\gamma})/K$ 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 \( \eta \in \mathcal{O}_K^x \otimes \mathbb{F}_p \), and \( \mathcal{O}_K^x \otimes \mathbb{F}_p \) intersects \( Q^G \) and \( N^G \) trivially, it follows that \( \eta = 0 \) in \( R'(K) \), so \( \eta \in \mathcal{O}_K^{xp} \), since \( \eta \) 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, \( \lambda_i, \alpha, \beta \) 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 \( P_V(v_1 \alpha) = 0 \) and \( P_V(v_2 \beta) = 0 \) 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

\[
\gamma \equiv \prod_{g \in \Phi} g(P_V(v_1 \alpha))^{a_g} \prod_{g \in \Phi} g(P_V(v_2 \beta))^{b_g} \mod K^{xp},
\]

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

Just as above, we observe that it is enough to prove the third claim for \( \bar{K}/K \), the statement for \( \bar{L}/L_p(K) \) 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 \( \text{Gal}(\bar{L}/L_p(K)) \cong \text{Gal}(\bar{K}/K) \). The following short lemma proves this statement for \( \bar{K}/K \).

**Lemma 6.1.** All the \((\mathbb{Z}/p\mathbb{Z})^2\)-subgroups of \( \text{Gal}(\bar{K}/K) \) appear as decomposition groups of some \( \lambda_i \), for \( 1 \leq i \leq T \).
Thus, the decomposition group of which implies that the fixed field of inertia is nontrivial, but the fixed field of $H$ with $(a_1,\ldots,a_n,b_1,\ldots,b_n)$ and $(x_1,\ldots,x_n,y_1,\ldots,y_n)$ 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. From the above discussion, we know that there is a prime $\lambda = \lambda_t$ such that the exponents of $\lambda, g_2^{-1}(\lambda),\ldots,g_n^{-1}(\lambda)$ are $a_1,\ldots,a_n$ in $v_1$, and $b_1,\ldots,b_n$ in $v_2$, respectively. This implies that the inertia subgroup corresponding to $\lambda$ in $\text{Gal}(\bar{K}/K)$ is generated by $(a_1,\ldots,a_n,b_1,\ldots,b_n)$. Moreover, the prime $\lambda$ satisfies
\begin{align*}
\alpha & \equiv g_i^{-1}(A_{i,t}) \pmod{g_i^{-1}(\lambda)}, \\
\beta & \equiv g_i^{-1}(B_{i,t}) \pmod{g_i^{-1}(\lambda)},
\end{align*}
which implies that the fixed field of inertia is nontrivial, but the fixed field of $H$ is trivial. Thus, the decomposition group of $\lambda$ is isomorphic to $H$. This concludes the proof, since $H$ was chosen arbitrary.

Proof. Take a $(\mathbb{Z}/p\mathbb{Z})^2$-subgroup $H$ of $\text{Gal}(\bar{K}/K)$; note that there are $T = (p^{2n-1})(p^{2n-1}-p)$ of them. Assume that $H$ 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 $(a_1,\ldots,a_n,b_1,\ldots,b_n) \neq 0$, $(x_1,\ldots,x_n,y_1,\ldots,y_n) \neq 0$, 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. From the above discussion, we know that there is a prime $\lambda = \lambda_t$ such that the exponents of $\lambda, g_2^{-1}(\lambda),\ldots,g_n^{-1}(\lambda)$ are $a_1,\ldots,a_n$ in $v_1$, and $b_1,\ldots,b_n$ in $v_2$, respectively. This implies that the inertia subgroup corresponding to $\lambda$ in $\text{Gal}(\bar{K}/K)$ is generated by $(a_1,\ldots,a_n,b_1,\ldots,b_n)$. Moreover, the prime $\lambda$ satisfies
\begin{align*}
\alpha & \equiv g_i^{-1}(A_{i,t}) \pmod{g_i^{-1}(\lambda)}, \\
\beta & \equiv g_i^{-1}(B_{i,t}) \pmod{g_i^{-1}(\lambda)},
\end{align*}
which implies that the fixed field of inertia is nontrivial, but the fixed field of $H$ is trivial. Thus, the decomposition group of $\lambda$ is isomorphic to $H$. This concludes the proof, since $H$ was chosen arbitrary.

We claim that the extension $\bar{L}/L_p(K)$ satisfies the conditions of Lemma 3.2, with $\tilde{S}$ instead of $S$. We know that $L_p(L_n(K)) = L_n(K)$ and we have just proved that $\bar{L}$ 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
\[
\bigoplus_v H_2(D_v,\mathbb{Z}) \to H_2(\text{Gal}(\bar{L}/L_p(K)),\mathbb{Z}),
\]
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 $\text{Gal}(\bar{L}/L_p(K)) \cong \text{Gal}(\bar{K}/K) \cong (\mathbb{Z}/p\mathbb{Z})^{2n}$, assume that $\text{Gal}(\bar{L}/L_p(K))$ is generated by $\{\tau_1,\tau_2,\ldots,\tau_{2n}\}$. Consider the $(\mathbb{Z}/p\mathbb{Z})^2$-subgroups of $\text{Gal}(\bar{L}/L_p(K))$ generated by pairs of two elements in $\{\tau_1,\ldots,\tau_{2n}\}$. There are $n(2n-1)$ of them; call them $A_1, A_2,\ldots,A_{n(2n-1)}$. Note that $T = \frac{(p^{2n-1})(p^{2n-1}-p)}{(p^2-1)(p^2-p)} \geq n(2n-1)$, for all primes $p$. From the fact that the decomposition subgroups $D_v$ span the $(\mathbb{Z}/p\mathbb{Z})^2$-subgroups of $\text{Gal}(\bar{L}/L_p(K))$, 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 $1 \leq i \leq n(2n-1)$. Consider the following intersections:
\begin{align*}
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} \\
&\quad \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{align*}
We claim that \[ For any group extension \] and \[ proof is similar to the proof of Lemma 4 in the first version of Ozaki's paper, the main Ozaki's lemma from the following result in the case of \( \Phi = 1 \), \[ K \text{ is not split, we cannot work over } p \text{ anymore. However, the proof is similar. We begin by proving the following lemma, which is a variation of Lemma 6 in [12]. In fact, we can recover Ozaki's lemma from the following result in the case of } \Phi = 1, V = \mathbb{Z}/p\mathbb{Z} \text{ and } \mu_p \subset K. \] 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 \( \Phi \) 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 $\text{Gal}(L_p(K')/F') \cong \text{Gal}(L_p(K)/F)$ and every prime of $F'$ lying over $p$ splits completely in $L_p(K')$.

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

Proof. By Proposition 5.4, there exists a Galois extension $L/F$ containing $L_p(K)$ such that $\text{Gal}(L/F) \cong \Gamma$. Let $\alpha_1, \ldots, \alpha_n$ be the Kummer generators of $L/L_p(K)$, so $L = L_p(K)(\sqrt[\alpha_1]{}, \ldots, \sqrt[\alpha_n]{})$. 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 $G = \text{Gal}(L_p(K)/K)$. 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 $\alpha_i^h \mathcal{O}_{L_p(K)} = A_i^h \mathfrak{a}_i$. Let $\alpha_i' = \alpha_i^h$ and $\alpha_i'' = \alpha_i^h A_i^{-p}$. Then $\alpha_i' \mathcal{O}_{L_p(K)}$ is an ideal of $\mathcal{O}_K$, and $L = L_p(K)(\sqrt[\alpha_1']{}, \ldots, \sqrt[\alpha_n']{}) = L_p(K)(\sqrt[\alpha_1'']{}, \ldots, \sqrt[\alpha_n'']{})$.

Let $p^e$ be the exact power of $p$ dividing the order of the ideal class $[\alpha_i']_K$. Then $[\alpha_i']^p_\mathfrak{a}_i$ has order prime to $p$. Let $e = \max e_i$, and note that $[\alpha_i']^p_\mathfrak{a}_i$ 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 $L_p(K') = L_p(K).F'$,
- $\text{Gal}(L_p(K')/F') \cong \Gamma$.

Denote by $j: C_{l KlK} \to C_{l KlK'}$ the map induced by the inclusion $K \subset K'$, and by $N: C_{l KlK'} \to C_{l KlK}$ the norm map. The natural restriction $\text{Gal}(L_p(K')/K') \to \text{Gal}(L_p(K)/K)$, which is an isomorphism, induces an isomorphism $\text{Gal}(L_p(K')/K')^{ab} \cong G^{ab}$. Then the order of $\ker N$ is prime to $p$ by class field theory. Thus, since $N \circ j([\alpha_i']_K) = [\alpha_i']_K$, the order of $j([\alpha_i']_K) \in C_{l KlK'}$, say $m_i$, is prime to $p$. Let $m = \text{lcm}(m_i)$, so $m$ is prime to $p$. Let $\alpha_i^{m_i} = \alpha_i' \mathcal{O}_{L_p(K)}$, for some $\alpha_i' \in K^{\times}$. Then $A_i \mathcal{O}_{L_p(K)} = \alpha_i^{m_i} \mathcal{O}_{L_p(K)}$. Thus, there exists $\varepsilon_i \in \mathcal{O}_{L_p(K)}^\times$ such that $\alpha_i^{m_i} = A_i^{e_i} \varepsilon_i$.

Note that $L_p(K)(\sqrt[\alpha_1'']{}, \ldots, \sqrt[\alpha_n'']{}) = L_p(K)(\sqrt[\alpha_1']{}^{m_1}, \ldots, \sqrt[\alpha_n']{}^{m_n})$, so we can replace $\alpha_i'$ by $\alpha_i^{m_i}$.

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 $L_p(K')(\sqrt[\alpha_1']{}, \ldots, \sqrt[\alpha_n'']{})/F'$ has Galois group $\Gamma'$, it follows that $\langle \alpha_i' \mod L_p(K')^{\times p} \rangle$ has an action of $\Gamma = G \times \Phi$ and, as an $\mathbb{F}_p[\Gamma]$-representation, it is isomorphic to a copy of $V$, the projective cover of $V$. Hence, $\text{Gal}(L_p(K')(\sqrt[\alpha_1'']{}, \ldots, \sqrt[\alpha_n'']{}))/F'$ is isomorphic to $\text{Gal}(L_p(K')(\sqrt[\alpha_1']{V(\alpha_1'}), \ldots, \sqrt[\alpha_n']{V(\alpha_n')}])/F'$, so we can replace $\alpha_i'$ by $P_V(\alpha_i') = P_V(a_i \varepsilon_i) = P_V(a_i) \cdot P_V(\varepsilon_i)$. Note that $P_V(a_i') = P_V(a_i')^{[G]}$, since $a_i' \in K^{\times}$. Since $P_V(\alpha_i')$ is isomorphic to a subrepresentation of $V$ in $K^{\times}/K^{\times p}$, and $V$ is an irreducible $\mathbb{F}_p[\Phi]$-representation, either $P_V(a_i') \cong V$ or $P_V(a_i') = 1$. The latter implies that $P_V(a_i') = 1$, for all $i$, which in turn implies that $P_V(\alpha_i') = P_V(\varepsilon_i)$, which finishes the proof: $L_p(K')(\sqrt[\alpha_1']{V(\alpha_1')}, \ldots, \sqrt[\alpha_n']{V(\alpha_n')})/F'$ is the desired extension. On the other hand, the former implies that $P_V(\alpha_i') \cong V$, so $\text{Gal}(K'(\sqrt[\alpha_1']{V(\alpha_1')}, \ldots, \sqrt[\alpha_n']{V(\alpha_n')})/F') \cong V \times \Phi$. Then, by Proposition 5.4, the Galois group of $L_p(K')(\sqrt[\alpha_1']{V(\alpha_1')}, \ldots, \sqrt[\alpha_n']{V(\alpha_n')})/F'$ is isomorphic to $V \times \Gamma$, which means that $\text{Gal}(L_p(K')(\sqrt[\alpha_1']{V(\alpha_1')}, \ldots, \sqrt[\alpha_n']{V(\alpha_n')})/F') \cong \Gamma'$, which is what we wanted. \qed

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 $L_p(K')(\sqrt[\alpha_1']{\varepsilon_1}, \ldots, \sqrt[\alpha_n']{\varepsilon_n})/F'$ satisfies property $P$ except possibly at the primes above $p$. 


Just as before, construct primes $\lambda_i$ in $K'$, for $1 \leq i \leq T$, and $\alpha, \beta$ in $K'$ with the same properties. The primes $\alpha, \beta, \lambda_i$ are in $K'$, so just as in the previous case, the Galois closure of $K'_1 = K'(\sqrt[p]{P_V(v_1 \alpha)})$ over $F$ has Galois group $V \times \Phi$. Define the field $L_1 = L_0(K')(\sqrt[p]{\epsilon_1 P_V(v_1 \alpha)}, \ldots, \sqrt[p]{\epsilon_n g_\alpha(P_V(v_1 \alpha))})$, and use Proposition 5.4 and Lemma 6.2 to observe that the Galois group of $L_1/F'$ is $\Gamma'$. Construct $K_2$ and $L_2$ in a similar manner. Let $\bar{K}$ be the Galois closure of $K'(\sqrt[p]{P_V(v_1 \alpha)P_V(v_2 \beta)})$ over $F'$ and let $\bar{L} = L_1, L_2$. Construct a field $\bar{F}$ just as in the previous case. Then the new extension $\bar{L}/\bar{F}$ 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 1.2

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

$$\overline{\psi}: G_K \to \text{GL}_2(\mathbb{F}_p),$$

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

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

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

Firstly, note that $\bar{\Gamma}$ admits a deformation to $\text{GL}_2(R)$ by construction, so $R_{\overline{\rho}} \to R$, 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 $\bar{\Gamma} \to \text{GL}_2(S)$,

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

$$\begin{array}{c}
\bar{\Gamma} \\
\downarrow \\
\text{GL}_2(S) \\
\downarrow \\
\text{GL}_2(R)
\end{array}$$

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 $m_A$ denote the maximal ideal of $A$.
- Let $\Gamma_S = 1 + M_2(I_S)$. 

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 $m_S/(m_S^2, p) \to m_R/(m_R^2, p)$. Then there exists a subring $S' \subset S$ such that $S' \cong R$.

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

Firstly, we claim that $x \not\in S'$. Suppose otherwise, so $x = a_0 + a_1 x_1 + \ldots + a_d x_d + \alpha$, where $\alpha \in m_S^2$, $a_i \in \mathbb{Z}_p$. Since $x, x_i, \alpha \in m_S$, it follows that $a_0 \in m_S \cap \mathbb{Z}_p = (p)$. Recall that under the map 

$$ m_S/(m_S^2, p) \to m_R/(m_R^2, p), $$

$x = a_0 + \sum a_i x_i + \alpha = \sum a_i x_i$ (in $m_S/(m_S^2, p)$) is sent to 0. Since $\overline{x_i}$ generate $m_R/(m_R^2, p)$, this is true if and only if $a_i = 0 \in m_R/(m_R^2, p)$, for all $i$, which is true if and only if $a_i \in \mathbb{Z}_p \cap (m_R^2, p) = (p)$. Thus, $x \in (m_S^2, p)$, which is a contradiction. So $x \not\in S'$, 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. \hfill \Box

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 $\Gamma_J$.
- $S \cong R[x]/(x^2, px)$, 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 $x \not\in (I_S^2, pI_S)$. Moreover, $x \not\in (m_S^2, p)$. Thus, under the map 

$$ m_S/(m_S^2, p) \to m_R/(m_R^2, p), $$

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 $x \not\in S'$.

Consider the map $S'[x] \to S$: it is a surjection and $px, x^2$ are elements of the kernel. Thus $S \cong S'[x]/(x^2, px) \cong R[x]/(x^2, px)$. \hfill \Box

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 $\tilde{\Gamma} \to \text{GL}_2(S)$.

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

$$
\begin{array}{ccc}
\Gamma_S & \xrightarrow{\psi} & F(\Gamma_S) \\
\downarrow & & \downarrow \\
\Gamma_R & \leftarrow & F(\Gamma_R)
\end{array}
$$

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 $\psi$ has to factor through $\Gamma_R$, 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 $\Gamma_S$, we obtain that $\Gamma_R \to \Gamma_S$ must be surjective, but this is impossible, since $\Gamma_R$ has fewer elements than $\Gamma_S$. Therefore, there is no lift to $GL_2(S)$ in this case. \hfill \Box

**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 $\tilde{\Gamma} \to GL_2(S)$;
2. $S \cong R[x_1, \ldots, x_n]/(x_ix_j, px_i)$, 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. $\Gamma_J \subset [\Gamma_S, \Gamma_S]_{\Gamma_S}$;
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 $\tilde{\Gamma} \to GL_2(S)$. 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 $\tilde{\Gamma} \to GL_2(S)$ 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 that surject onto $\mathbb{Z}_p$ with finite kernels $I_R$ and $I_S$, respectively. Assume moreover that $S$ surjects onto $R$ with finite kernel $J$. Then there exists a splitting $R \to S$.

**Proof.** 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 $S/mSJ$, 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 $S/mSJ$. 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 $S \to R$ has kernel $J$, then

$$S \xrightarrow{\pi} S/mSJ \to S/J = R.$$  

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

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

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

1. There is no lift $\tilde{\Gamma} \to GL_2(S')$;
2. $S' \cong R[x_1, \ldots, x_n]/(x_i x_j, px_i)$, for some $x_i \in S'$.

If there is no lift to $GL_2(S')$, then there’s no lift to $GL_2(S)$, so there’s nothing to be proved. The second case gives us a splitting $R \to S'$. 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 induction step and the second map comes from the definition of $S''$. \qed

We can now prove Theorem 1.2. Recall that at the beginning of this section we assumed the existence of an absolutely irreducible residual representation $\psi: G_K \to GL_2(\overline{\mathbb{F}}_p)$, whose image is $\overline{\Phi}$. From this, we obtained a short exact sequence

$$1 \to G \to \Gamma \xrightarrow{f} \overline{\Phi} \to 1,$$

and a residual representation $\overline{\rho}: \overline{\Gamma} \to GL_2(\overline{\mathbb{F}}_p)$. 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 $\text{Gal}(H/F) = \overline{\Gamma}$ and $H/K$ the maximal everywhere unramified pro-$p$ extension of $K$. The existence of such extensions is given by Theorem 1.1, under the assumption that there exists a $\overline{\Phi}$-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 $\Phi$ instead of $\overline{\Phi}$: consider the following exact sequence

$$1 \to G \to \Gamma \xrightarrow{f} \Phi \to 1$$

and its projective image

$$1 \to G \to \Gamma \xrightarrow{f} \Phi \to 1.$$

We are in the following case

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

To finish the proof of Theorem 1.2, 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 $\Phi$-extension of $\mathbb{Q}(\zeta_p)$ with class number prime to $p$ that satisfies property $P$. 
Example. Let $p = 5$ and $\tilde{\Phi} = \tilde{A}_4 = \text{SL}_2(\mathbb{F}_3)$ (so $\Phi = A_4$). Let $F = \mathbb{Q}(\zeta_5)$ and let $\tilde{K}_1$ 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 $K_1$, which is the Galois closure of the field defined by $x^4 - 21x^2 - 3x + 100$.

Let $\tilde{K} = F.\tilde{K}_1$ and $K = F.K_1$. Then $K$ is a subfield of $\tilde{K}$ and $\text{Gal}(\tilde{K}/F) = \text{SL}_2(\mathbb{F}_3) \rightarrow A_4 = \text{Gal}(K/F)$. We used GP/Pari [2] to show that the class numbers of both $K$ and $\tilde{K}$ are prime to 5 and that both $K/F$ and $\tilde{K}/F$ satisfy property $P$. This concludes the proof for $p = 5$.

Example. Let $p = 7$ and $\tilde{\Phi} = \tilde{A}_4 = \text{SL}_2(\mathbb{F}_3)$ (so $\Phi = A_4$). Let $F = \mathbb{Q}(\zeta_7)$ and let $\tilde{K}_1$ 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 $K_1$, which is the Galois closure of the field defined by $x^4 - x^3 - 11x^2 + 4x + 12$.

Let $\tilde{K} = F.\tilde{K}_1$ and $K = F.K_1$. Then $K$ is a subfield of $\tilde{K}$ and $\text{Gal}(\tilde{K}/F) = \text{SL}_2(\mathbb{F}_3) \rightarrow A_4 = \text{Gal}(K/F)$. We used GP/Pari [2] to show that the class numbers of both $K$ and $\tilde{K}$ are prime to 7 and that both $K/F$ and $\tilde{K}/F$ 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 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


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