ON TAME \( \mathbb{Z}/p\mathbb{Z} \)-EXTENSIONS WITH PRESCRIBED RAMIFICATION

FARSHID HAJIR, CHRISTIAN MAIRE, RAVI RAMAKRISHNA

Abstract. The tame Gras-Munnier Theorem gives a criterion for the existence of a \( \mathbb{Z}/p\mathbb{Z} \)-extension of a number field \( K \) ramified at exactly a set \( S \) of places of \( K \) prime to \( p \) (allowing real Archimedean places when \( p = 2 \)) in terms of the existence of a dependence relation on the Frobenius elements of these places in a certain governing extension. We give a new and simpler proof of this theorem that also relates the set of such extensions of \( K \) to the set of these dependence relations. After presenting this proof, we then reprove the key Proposition \( 3 \) using the more sophisticated Wiles-Greenberg formula based on global duality.

1. Introduction:

Let \( D \in \mathbb{Z} \) be squarefree and odd. Our convention is that \( \infty | D \) if \( D < 0 \). It is a standard result that there exists a quadratic extension \( K/\mathbb{Q} \) ramified at exactly the set \( \{ v : v | D \} \) if and only if \( D \equiv 1 \pmod{4} \). The key is how the Frobenius elements of \( v | D \) lie in the Galois group of the ‘governing extension’ \( \mathbb{Q}(i)/\mathbb{Q} \). Let \( \sigma_v \) denote Frobenius at \( v \) in this extension with \( \sigma_\infty \) being the nontrivial element of \( \text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \). We frame this as the following theorem:

**Theorem** There exists a quadratic extension \( K/\mathbb{Q} \) ramified exactly at a tame (not containing 2 but allowing \( \infty \)) set \( S \) of places if and only if \( \sum_{v \in S} \sigma_v \) is the trivial element in \( \text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \).

In [GM] this result was generalized to \( \mathbb{Z}/p\mathbb{Z} \)-extensions of a general number field \( K \). For a fixed prime \( p \) and set \( S \) of tame places, set

\[
V_S = \{ x \in K^\times \mid (x) = J^p; \ x \in K^\times_p \ \forall \ v \in S \}.
\]

Note \( K^\times_p \subset V_S \) for all \( S \) and \( S \subset T \implies V_T \subseteq V_S \). Let \( \mathcal{O}_K^\times \) and \( \text{Cl}_K[p] \) be, respectively, the units of \( K \) and the \( p \)-torsion in the class group of \( K \). It is a standard result that \( V_\emptyset / K^\times_p \) lies in the exact sequence (see Proposition 10.7.2 of [NSW]):

\[
0 \to \mathcal{O}_K^\times \otimes \mathbb{F}_p \to V_\emptyset / K^\times_p \to \text{Cl}_K[p] \to 0.
\]

Set \( K' = K(\mu_p) \), \( L = K'(\sqrt[4]{\mathbb{Q}(i)}) \) and let \( r_1 \) and \( r_2 \) be the number of real and pairs of complex embeddings of \( K \). We call \( L/K' \) the governing extension for \( K \). When \( K = \mathbb{Q} \) and \( p = 2 \) we see \( L = \mathbb{Q}(i) \) and have recovered the field of the theorem above.

\[
\begin{aligned}
L &:= K'(\sqrt[4]{\mathbb{Q}(i)}) \\
K' &:= K(\mu_p) \\
K &
\end{aligned}
\]

The second author was partially supported by the ANR project FLAIR (ANR-17-CE40-0012) and by the EIPHI Graduate School (ANR-17-EURE-0002). The third author was partially supported by Simons Collaboration grant #524863. He also thanks FEMTO-ST for its hospitality and wonderful research environment during his visit there in the spring of 2022. All three authors were supported by ICERM for a Research in Pairs visit in January, 2022.
As $L$ is obtained by adjoining to $K'$ the $p$th roots of elements of $K$ (not $K'$), one easily shows that places $v'_1, v'_2$ of $K'$ above a fixed place $v$ of $K$ have Frobenius elements in $\text{Gal}(L/K')$ that differ by a nonzero scalar multiple. We abuse notation and for any $v'$ of $K'$ above $v$ in $K$ denote Frobenius at $v'$ by $\sigma_v$. The theorem of [GM] (also see Chapter V of [G]) below and Theorem 1 implicitly use this abuse of notation.

**Theorem** (Gras-Munnier) Let $p$ be a prime and $S$ a finite set of tame places (allowing Archimedean places if $p = 2$) of $K$. There exists a $\mathbb{Z}/p\mathbb{Z}$-extension of $K$ ramified at exactly the places of $S$ if and only if there exists a dependence relation $\sum_{v \in S} a_v \sigma_v = 0$ in the $\mathbb{F}_p$-vector space $\text{Gal}(L/K')$ with all $a_v \neq 0$.

The original proof uses class field theory in a fairly complicated way. Theorem 1 is a generalization of the Gras-Munnier Theorem. We first give a short proof that uses only one element of class field theory, (2.1) below, and elementary linear algebra. We easily prove Proposition 3 from the extension of the Gras-Munnier Theorem. We first give a short proof that uses only one element of class field theory, (2.1) below, and elementary linear algebra. We easily prove Proposition 3 from the Wiles-Greenberg formula whose proof requires the full strength of global duality. Denote by $G_S$ the Galois group over $K$ of its maximal extension pro-$\mathfrak{p}$ unramified outside $S$. Our main result is:

**Theorem 1.** Let $p$ be a prime and $S$ a finite set of tame places of a number field $K$ (allowing Archimedean places if $p = 2$). The sets

$$\left\{ f \in H^1(G_S, \mathbb{Z}/p\mathbb{Z}) \mid \text{the extension } K_f/K \text{ fixed by } \text{Ker}(f) \text{ is ramified exactly at the places of } S \right\}$$

and

$$\{ \text{The dependence relations } \sum_{v \in S} a_v \sigma_v = 0 \text{ in } \text{Gal}(L/K') \text{ with all } a_v \neq 0 \}$$

have the same cardinality.

It is an easy exercise to see both sets have cardinality at most one when $p = 2$, so the bijection is natural in this case.

We thank Brian Conrad for pointing out to us a proof of Lemma 4(ii) and Peter Uttenthal for helpful suggestions.

### 2. Proof of the Gras-Munnier Theorem

For any field $E$ set $\delta(E) = \left\{ \begin{array}{ll} 1 & \mu_p \subseteq E \\ 0 & \mu_p \not\subseteq E \end{array} \right.$. Observe that by Dirichlet’s unit theorem $\text{Gal}(L/K')$ is an $\mathbb{F}_p$-vector space of dimension $r_1 + r_2 - 1 + \delta(K) + \dim Cl_K[p]$. The standard fact from class field theory that we need (see §11.3 of [K] or §10.7 of [NSW]) is a formula of Shafarevich and Koch for the dimension of the space of $\mathbb{Z}/p\mathbb{Z}$-extensions of $K$ unramified outside a tame set $Z$:

$$\dim H^1(G_Z, \mathbb{Z}/p\mathbb{Z}) = -r_1 - r_2 + 1 - \delta(K) + \dim(V_Z/K^{\times p}) + \left( \sum_{v \in Z} \delta(K_v) \right).$$

Fix a tame set $S$ noting that $H^1(G_S, \mathbb{Z}/p\mathbb{Z})$ may include cohomology classes that cut out $\mathbb{Z}/p\mathbb{Z}$-extensions of $K$ that could be ramified at proper subsets of $S$. If $\delta(K_v) = 0$ for $v \in S$, there are no ramified $\mathbb{Z}/p\mathbb{Z}$-extensions of $K_v$ and thus no $\mathbb{Z}/p\mathbb{Z}$-extensions of $K$ ramified at $v$, so we always assume $\delta(K_v) = 1$. Then, as we vary $Z$ from $\emptyset$ to $S$ one place at a time, $\dim(V_Z/K^{\times p})$ may remain the same or decrease by 1. In these cases $\dim H^1(G_Z, \mathbb{Z}/p\mathbb{Z})$ increases by 1 or remains the same respectively.
Let \( W \subset Gal(L/K') \) be the \( \mathbb{F}_p \)-subspace spanned by \( \langle \sigma_v \rangle_{v \in S} \), the Frobenius elements of the places in \( S \). We will show the set of dependence relations on these Frobenius elements all of whose coefficients are nonzero has the same cardinality as the set of \( \mathbb{Z}/p\mathbb{Z} \)-extensions of \( K \) ramified exactly at the places of \( S \). Let \( I := \{ u_1, u_2, \ldots, u_r \} \subset S \) be such that \( \{ \sigma_{u_1}, \sigma_{u_2}, \ldots, \sigma_{u_r} \} \) form a basis of \( W \) and let \( D := \{ w_1, w_2, \ldots, w_s \} \subset S \) be the remaining elements of \( S \). We think of the \( \sigma_{u_i} \) as independent elements and the \( \sigma_{w_j} \) as the dependent elements. As we vary \( X \) in \( \{ \} \) from \( \emptyset \) to \( I \) by adding in one \( u_i \) at a time, we are adding 1 through the \( \delta(K_{u_i}) \) term to the right side of \( (2.1) \), but \( \dim V_X/K^{\times p} \) becomes one dimension smaller, so both sides remain unchanged. Then, as we add in the places \( w_j \) of \( D \) to get to \( S = I \cup D \) we have \( V_I/K^{\times p} = V_S/K^{\times p} \). Thus

\[
(2.2) \quad H^1(G_{\emptyset}, \mathbb{Z}/p\mathbb{Z}) = H^1(G_I, \mathbb{Z}/p\mathbb{Z}) = \dim H^1(G_S, \mathbb{Z}/p\mathbb{Z}) - s \implies \dim \frac{H^1(G_S, \mathbb{Z}/p\mathbb{Z})}{H^1(G_{\emptyset}, \mathbb{Z}/p\mathbb{Z})} = s.
\]

We can write each \( \sigma_{w_j} \) as a linear combination of the \( \sigma_{u_i} \) in a unique way:

\[
R_j : \sigma_{w_j} - \sum_{i=1}^r F_{j i} \sigma_{u_i} = 0.
\]

For \( X \subset S \) let \( R_X \) be the \( \mathbb{F}_p \)-vector space of all dependence relations on the elements \( \{ \sigma_v \}_{v \in X} \subset Gal(L/K') \). We prove a preliminary result in the spirit of Theorem \( 1 \).

**Lemma 2.** The set \( \{ R_1, R_2, \cdots, R_s \} \) forms a basis of the \( \mathbb{F}_p \)-vector space of dependence relations on the \( \sigma_{u_i} \) and \( \sigma_{w_j} \).

**Proof.** Consider any dependence relation \( R \) among the \( \sigma_{u_i} \) and \( \sigma_{w_j} \). We can eliminate each \( \sigma_{w_j} \) by adding to \( R \) a suitable multiple of \( R_j \). We are then left with a dependence relation on the \( \sigma_{u_i} \), which are independent, so it is trivial, proving the lemma. \( \square \)

**Proposition 3.** For any \( X \subset S \), \( \dim R_X = \dim \left( \frac{H^1(G_X, \mathbb{Z}/p\mathbb{Z})}{H^1(G_{\emptyset}, \mathbb{Z}/p\mathbb{Z})} \right). \)

**Proof.** Lemma \( 2 \) and \( (2.2) \) prove this for \( X = S \). Apply the same proof to \( X \subset S \). \( \square \)

**Proof of Theorem 1.** Proposition \( 3 \) does not complete the proof as \( R_S \) may contain dependence relations with support properly contained in \( S \) and \( H^1(G_S, \mathbb{Z}/p\mathbb{Z}) \) may contain elements giving rise to extensions of \( K \) ramified at proper subsets of \( S \).

**Proof Theorem 1.** The set of dependence relations with support *exactly* in \( S \) is

\[
(2.3) \quad R_S \setminus \bigcup_{v \in S} R_{S \setminus \{ v \}},
\]

those with support contained in \( S \) less the union of those with proper maximal support in \( S \). For any sets \( A_i \subset S \) it is clear that

\[
\bigcap_{i=1}^k R_{A_i} = R_{\bigcap_{i=1}^k A_i},
\]

so by inclusion-exclusion

\[
(2.4) \quad \# \bigcup_{v \in S} R_{S \setminus \{ v \}} = \sum_{v \in S} \#R_{S \setminus \{ v \}} - \sum_{v \neq w \in S} \#R_{S \setminus \{ v, w \}} + \cdots
\]
Similarly the set of cohomology classes giving rise to \( \mathbb{Z}/p\mathbb{Z} \)-extensions ramified exactly at the places of \( S \) (up to unramified extensions) is
\[
H^1(G_S, \mathbb{Z}/p\mathbb{Z}) \setminus \bigcup_{v \in S} H^1(G_{S \setminus \{v\}}, \mathbb{Z}/p\mathbb{Z})/H^1(G_{\emptyset}, \mathbb{Z}/p\mathbb{Z}).
\]

Since for any sets \( A_i \subseteq S \) we have
\[
\bigcap_{i=1}^k \frac{H^1(G_{A_i}, \mathbb{Z}/p\mathbb{Z})}{H^1(G_{\emptyset}, \mathbb{Z}/p\mathbb{Z})} = \frac{H^1(G_{\cap_{i=1}^k A_i}, \mathbb{Z}/p\mathbb{Z})}{H^1(G_{\emptyset}, \mathbb{Z}/p\mathbb{Z})},
\]

we see
\[
\# \bigcup_{v \in S} \frac{H^1(G_{S \setminus \{v\}}, \mathbb{Z}/p\mathbb{Z})}{H^1(G_{\emptyset}, \mathbb{Z}/p\mathbb{Z})} = \sum_{v \in S} \frac{H^1(G_{S \setminus \{v\}}, \mathbb{Z}/p\mathbb{Z})}{H^1(G_{\emptyset}, \mathbb{Z}/p\mathbb{Z})} - \sum_{v \notin w \in S} \frac{H^1(G_{S \setminus \{w\}}, \mathbb{Z}/p\mathbb{Z})}{H^1(G_{\emptyset}, \mathbb{Z}/p\mathbb{Z})} + \ldots
\]

Proposition 3 implies the terms on the right sides of (2.4) and (2.6) are equal so the left sides are equal as well. The result follows from (2.3), (2.5) and applying Proposition 3 with \( X = S \). \( \square \)

3. A proof via the Wiles-Greenberg formula

As the association of dependence relations and cohomology classes in Theorem 1 resembles a duality result, we now prove Proposition 3 using the Wiles-Greenberg formula, which follows from local duality. We assume familiarity with local and global Galois cohomology and their duality theories.

As we will need to apply the Wiles-Greenberg formula, we henceforth assume its hypothesis that \( Z \) is a set of places of \( K \) containing all those above infinity and \( p \). For each \( v \in Z \), let \( G_v := \text{Gal}(K_v/K_v) \) and consider a subspace \( L_v \subset H^1(G_v, \mathbb{Z}/p\mathbb{Z}) \). Under the local duality pairing (see Chapter 7, §2 of [NSW])
\[
H^1(G_v, \mathbb{Z}/p\mathbb{Z}) \times H^1(G_v, \mu_p) \to H^2(G_v, \mu_p) \cong \frac{1}{p} \mathbb{Z}/\mathbb{Z}
\]

\( L_v \) has an annihilator \( L_v^\perp \subset H^1(G_v, \mu_p) \). Set
\[
H^1_{\perp}(G_Z, \mathbb{Z}/p\mathbb{Z}) := \text{Ker} \left( H^1(G_Z, \mathbb{Z}/p\mathbb{Z}) \to \bigoplus_{v \in Z} \frac{H^1(G_v, \mathbb{Z}/p\mathbb{Z})}{L_v} \right)
\]

and
\[
H^1_{\perp \perp}(G_Z, \mu_p) := \text{Ker} \left( H^1(G_Z, \mu_p) \to \bigoplus_{v \in Z} \frac{H^1(G_v, \mu_p)}{L_v^\perp} \right).
\]

We call \( \{L_v\}_{v \in Z} \) and \( \{L_v^\perp\}_{v \in Z} \) the Selmer and dual Selmer conditions and \( H^1_{\perp}(G_Z, \mathbb{Z}/p\mathbb{Z}) \) and \( H^1_{\perp \perp}(G_Z, \mu_p) \) the Selmer and dual Selmer groups.

We state two results that we need for our second proof of Proposition 3. As Lemma 4 (ii) is perhaps not so well-known, we include a sketch of its proof.

Lemma 4. (i) Suppose \( v \nmid p \). Then \( H^1_{\perp}(G_v, \mathbb{Z}/p\mathbb{Z}) \) and \( H^1_{\perp}(G_v, \mu_p) \), the unramified cohomology annihilators, are exact annihilators of one another under the local duality pairing.
(ii) Suppose \( v|p \). Recall \( K'_v = K_v(\mu_p) \). The annihilator in \( H^1(G_v, \mu_p) \) of \( H^1_{\perp}(G_v, \mathbb{Z}/p\mathbb{Z}) \subset H^1(G_v, \mathbb{Z}/p\mathbb{Z}) \) is \( H^1_f(G_v, \mu_p) \), the peu ramifiée classes, namely those \( f \in H^1_f(G_v, \mu_p) \) whose fixed field \( L_{vf} \) of \( \text{Ker}(f|G_{K'_{K_v}}) \) arises from adjoining the \( p \)th root of a unit \( u_f \in K_v \).

Proof. (i) This is standard - see 7.2.15 of [NSW].
(ii) Cohomology taken over Spec(\( \mathcal{O}_{K_v} \)) in what follows is flat. Here
\[
H^1_f(G_v, \mu_p) = H^1(\text{Spec}(\mathcal{O}_{K_v}), \mu_p) = \mathcal{O}_{K_v}^\times / \mathcal{O}_{K_v}^{xp} \subset K_v^\times / K_v^{xp}
\]
where the containment is codimension one as $\mathbb{F}_p$-vector spaces. Recall
\[ \mathbb{Z}/p\mathbb{Z} \simeq H^1_{nr}(G_v, \mathbb{Z}/p\mathbb{Z}) = H^1(\text{Spec}(\mathcal{O}_{K_v}), \mathbb{Z}/p\mathbb{Z}) \]
and by Lemma 1.1 of Chapter III of [M] we have the injections
\[ H^1(\text{Spec}(\mathcal{O}_{K_v}), \mathbb{Z}/p\mathbb{Z}) \hookrightarrow H^1(G_v, \mathbb{Z}/p\mathbb{Z}) \text{ and } H^1(\text{Spec}(\mathcal{O}_{K_v}), \mu_p) \hookrightarrow H^1(G_v, \mu_p) \]
and the pairing
\[ H^1(\text{Spec}(\mathcal{O}_{K_v}), \mathbb{Z}/p\mathbb{Z}) \times H^1(\text{Spec}(\mathcal{O}_{K_v}), \mu_p) \to H^2(\text{Spec}(\mathcal{O}_{K_v}), \mu_p) = 0 \]
which is consistent with the local duality pairing
\[ H^1(G_v, \mathbb{Z}/p\mathbb{Z}) \times H^1(G_v, \mu_p) \to H^2(G_v, \mu_p) = \frac{1}{p} \mathbb{Z}/\mathbb{Z}. \]
As $H^1(\text{Spec}(\mathcal{O}_{K_v}), \mathbb{Z}/p\mathbb{Z}) = H^1_{nr}(G_v, \mathbb{Z}/p\mathbb{Z})$ and $H^1(\text{Spec}(\mathcal{O}_{K_v}), \mu_p) = H^1_{V}(G_v, \mu_p)$ are, respectively, dimension 1 and codimension 1 in $H^1(G_v, \mathbb{Z}/p\mathbb{Z})$ and $H^1(G_v, \mu_p)$, they are exact annihilators of one another, proving (ii).

\section*{Theorem (Wiles-Greenberg)} Assume $Z$ contains all places above $\{p, \infty\}$. Then
\[ \dim H^1_{L}(G_{Z}, \mathbb{Z}/p\mathbb{Z}) - \dim H^1_{L}(G_{Z}, \mu_{p}) = \dim H^0(\mathcal{O}_{Z}, \mathbb{Z}/p\mathbb{Z}) - \dim H^0(G_{Z}, \mu_{p}) + \sum_{v \in Z} (\dim L_{v} - \dim H^0(G_{v}, \mathbb{Z}/p\mathbb{Z})). \]

See 8.7.9 of [NSW] for details of this result.

\section*{Second proof of Proposition 3} Recall $X$ is tame and write $X := X_{<\infty} \cup X_{\infty}$. Set $Z := Z_{p} \cup X_{<\infty} \cup Z_{\infty}$ where $Z_{p} := \{v : v|p\}$ and $Z_{\infty}$ is the set of all real Archimedean places of $K$ (so $X_{\infty} \subseteq Z_{\infty}$). We assume for all $v \in X_{<\infty}$ that $N(v) \equiv 1 \mod p$.

Recall that for a complex Archimedean place $v$ of $K$ we have $G_{v} = \{e\}$ so the Selmer and dual Selmer conditions are trivial. For a real Archimedean place $v$, $\dim H^1(G_{v}, \mathbb{Z}/2\mathbb{Z}) = \dim H^1(G_{v}, \mu_{2}) = 1$ and the pairing between them is perfect - see Chapter I, Theorem 2.13 of [M]. It is easy to see in this case that the unramified cohomology groups are trivial.

In the table below we choose $\{M_{v}\}_{v \in Z}$ and $\{N_{v}\}_{v \in Z}$ so that $H^1_{L}(G_{Z}, \mathbb{Z}/p\mathbb{Z}) = H^1(\mathcal{O}_{\emptyset}, \mathbb{Z}/p\mathbb{Z})$ and $H^1_{L}(G_{Z}, \mathbb{Z}/p\mathbb{Z}) = H^1(G_{X}, \mathbb{Z}/p\mathbb{Z})$. The previous paragraph and Lemma 3 justify the stated dual Selmer conditions of the table.

| $v \in Z_{p}$ | $M_{v}^{1}$ | $M_{v}^{1}$ | $N_{v}$ | $N_{v}^{1}$ |
|---------------|-----------|-----------|--------|----------|
| $v \in X_{>\infty}$ | $H_{nr}(G_{v}, \mathbb{Z}/p\mathbb{Z})$ | $H_{nr}(G_{v}, \mu_{p})$ | $H_{nr}(G_{v}, \mathbb{Z}/p\mathbb{Z})$ | $H_{nr}(G_{v}, \mu_{p})$ |
| $v \in Z_{\infty}$ | $H_{nr}(G_{v}, \mathbb{Z}/2\mathbb{Z})$ | $H_{nr}(G_{v}, \mathbb{Z}/2\mathbb{Z})$ | $H_{nr}(G_{v}, \mathbb{Z}/p\mathbb{Z})$ | $H_{nr}(G_{v}, \mu_{p})$ |
| $v \in X_{<\infty}$ | $H_{nr}(G_{v}, \mathbb{Z}/p\mathbb{Z})$ | $H_{nr}(G_{v}, \mu_{p})$ | $H_{nr}(G_{v}, \mathbb{Z}/p\mathbb{Z})$ | $H_{nr}(G_{v}, \mu_{p})$ |

Applying the Wiles-Greenberg formula for $\{M_{v}\}_{v \in Z}$ and $\{N_{v}\}_{v \in Z}$ and subtracting the first equation from the second:
\[ \dim H^1(G_{X}, \mathbb{Z}/p\mathbb{Z}) - \dim H^1(\mathcal{O}_{\emptyset}, \mathbb{Z}/p\mathbb{Z}) = \dim H^1_{L}(G_{Z}, \mathbb{Z}/p\mathbb{Z}) - \dim H^1(\mathcal{O}_{\emptyset}, \mathbb{Z}/p\mathbb{Z}) \]
\[ = \dim H^1_{L}(G_{Z}, \mathbb{Z}/p\mathbb{Z}) - \dim H^1(\mathcal{O}_{\emptyset}, \mathbb{Z}/p\mathbb{Z}) + \sum_{v \in Z} (\dim N_{v} - \dim M_{v}) \]

For $v \in X_{<\infty}$ local class field theory implies $\dim H^1_{nr}(G_{v}, \mathbb{Z}/p\mathbb{Z}) = 1$ and $\dim H^1(G_{v}, \mathbb{Z}/p\mathbb{Z}) = 2$ so
\[ \dim N_{v} - \dim M_{v} = \begin{cases} 0 & v \in Z_{p} \\ 1 & v \in X_{\infty}, \ p = 2 \\ 0 & v \in Z_{\infty} \setminus X_{\infty} \\ 1 & v \in X_{<\infty} \end{cases} \]
and we have

\[(3.1) \quad \dim \left( \frac{H^1(G_X, \mathbb{Z}/p\mathbb{Z})}{H^1(G_0, \mathbb{Z}/p\mathbb{Z})} \right) = \dim H^1_{\mathcal{X}}(G_Z, \mu_p) - \dim H^1_{\mathcal{M}}(G_Z, \mu_p) + \#X.\]

To prove Proposition 3 we need to show this last quantity is \(\dim R_X = s\), the dimension of the space of dependence relations on the set \(\{\sigma_v\}_{v \in X} \subset W = Gal(K'(\sqrt[p]{\alpha})/K').\)

An element \(f \in H^1_{\mathcal{M}}(G_Z, \mu_p)\) gives rise to the field diagram below where \(L_f/K'\) is a \(\mathbb{Z}/p\mathbb{Z}\) extension peu ramifiée at \(v \in Z_p\), with no condition on \(v \in Z_\infty\) and unramified at \(v \in X_{<\infty}\). We show the composite of all such \(L_f\) is \(K'(\sqrt[p]{\alpha})\).

\[
\begin{array}{c}
L_f := K'(\sqrt[p]{\alpha}) \\
K' := K(\mu_p) \\
\downarrow \\
K
\end{array}
\]

Kummer Theory implies \(\alpha_f \in K'/K'^{\times p}\), which decomposes into eigenspaces under the action of \(Gal(K'/K)\). If it is not in the trivial eigenspace, then \(Gal(L_f/K')\) is not acted on by \(Gal(K'/K)\) via the cyclotomic character, a contradiction, so we may assume (up to \(p\)th powers) \(\alpha_f \in K\). Since \(L_f/K'\) is unramified at \(v \in X_{<\infty}\), we see that at all such \(v\) that \(\alpha_f = u\pi_v^{p^r}\) where \(u \in K_v\) is a unit. At \(v \in Z_p\) being peu ramifiée implies that locally at \(v \in X_p\) we have \(\alpha_f = u\pi_v^{p^r}\) where \(u \in K_v\) is a unit. Together, these mean that the fractional ideal \((\alpha_f)\) of \(K\) is a \(p\)th power, which implies that \(\alpha_f \in V_0\). Conversely, if \(\alpha \in V_0\), then, recalling that \(\alpha = J^p\) for some ideal of \(K\), we have that \(K'(\sqrt[p]{\alpha})/K'\) is a \(\mathbb{Z}/p\mathbb{Z}\)-extension peu ramifiée at \(v \in Z_p\), with no condition at \(v \in Z_\infty\). Thus \(\alpha\) gives rise to an element \(f_\alpha \in H^1_{\mathcal{M}}(G_Z, \mu_p)\) so \(L := K'(\sqrt[p]{\alpha})\) is the composite of all \(L_f\) for \(f \in H^1_{\mathcal{M}}(G_Z, \mu_p)\).

An element \(f \in H^1_{\mathcal{X}}(G_Z, \mu_p)\) gives rise to a \(\mathbb{Z}/p\mathbb{Z}\)-extension of \(K'\) peu ramifiée at \(v \in Z_p\) and split completely at \(v \in X\). We denote the composite of all these fields by \(D \subset K'(\sqrt[p]{\alpha})\).

\[
\begin{array}{c}
L := K'(\sqrt[p]{\alpha}) \\
D \\
K' := K(\mu_p) \\
\downarrow \\
K
\end{array}
\]

Recall that \(r\) is the dimension of the space \(\langle \sigma_v \rangle_{v \in X} \subset Gal(L/K')\). Clearly \(D\) is the field fixed of \(\langle \sigma_v \rangle_{v \in X}\) so \(\dim_{\mathbb{Q}_p} Gal\left( K'\left( \sqrt[p]{\alpha} \right)/D \right) = r = \#I\) from the first section of this note. Thus

\[
\dim H^1_{\mathcal{X}}(G_Z, \mu_p) = \dim(V_0/K^{\times p}) - r
\]

so

\[
\dim H^1_{\mathcal{X}}(G_Z, \mu_p) - \dim H^1_{\mathcal{M}}(G_Z, \mu_p) + \#X = \\
(\dim(V_0/K^{\times p}) - r) - \dim(V_0/K^{\times p}) + (r + s) = s = \dim R_X
\]
and we have shown the the left hand side of (3.1) is $\dim R_X$ proving Proposition 3.

We have now proven Proposition 3 using the Wiles-Greenberg formula. The rest of the proof of Theorem 1 follows as in the previous section.

References

[G] G. Gras, Class Field Theory: from theory to practice, corr. 2nd ed., Springer Monographs in Mathematics, Springer (2005), xiii+507 pages.

[GM] Gras, G. and Munnier, A., Extensions cycliques $T$-totalement ramifiées, Publ. Math. Besançon, 1997/98.

[K] Koch, H. Galois Theory of $p$-extensions, Springer 2002.

[M] Arithmetic duality Theorems, Academic press, 1986 First Edition. Second edition available https://www.jmilne.org/math/Books/ADTnot.pdf

[NSW] Neukirch, J.; Schmidt, A.; Wingberg, K. Cohomology of Number Fields, Springer. Second edition, second corrected printing 2013.