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 tame set S of places of K, the finite $v \in S$ necessarily having norm 1 mod p. The criterion is the existence of a dependence relation on the Frobenius elements of these places in a certain *governing extension*. We give a short new proof which extends the theorem by showing the subset of elements of $H^1(G_S, \mathbb{Z}/p\mathbb{Z})$ giving rise to such extensions of K has the same cardinality as the set of these dependence relations. We then reprove the key Proposition 3 using the more sophisticated Greenberg-Wiles formula based on global duality.

1. INTRODUCTION:

Let $D \in \mathbb{Z}$ be squarefree and odd and write $\infty | D$ if $D < 0$. It is well-known that there exists a quadratic extension $K/\mathbb{Q}$ ramified at exactly the set of places $\{v : v|D\}$ if and only if $D \equiv 1 \bmod 4$. The key is how the Frobenius elements of the $v|D$ lie in the Galois group of the *governing extension* $\mathbb{Q}(i)/\mathbb{Q}$. Let σ_v denote Frobenius at v in this extension with σ_∞ being the nontrivial element of $Gal(\mathbb{Q}(i)/\mathbb{Q})$. We frame this result as the following Fact:

Fact. *There exists a quadratic extension $K/\mathbb{Q}$ ramified exactly at a tame (not containing 2 but allowing ∞) set S of places if and only if $\sum_{v \in S} \sigma_v = 0$ in $Gal(\mathbb{Q}(i)/\mathbb{Q})$.*

The paper [GM] extended this to $\mathbb{Z}/p\mathbb{Z}$-extensions of a general number field K and with some hypotheses to $\mathbb{Z}/p^e\mathbb{Z}$-extensions of K. To explain the result precisely we need some background. For a fixed prime p and set S of tame places (prime to p and allowing real Archimedean places), let

$$V_S := \{x \in K^\times \mid (x) = J^p;\ x \in K_v^{\times p}\ \ \forall\ \ v \in S\}$$

where J is a fractional ideal of K. Note $K^{\times p} \subset V_S$ for all S and $S \subseteq T \implies V_T \subseteq V_S$. Let $\mathcal{O}_K^\times$ and $Cl_K[p]$ be, respectively, the units of K and the p-torsion in the class group of K. That $V_\emptyset / K^{\times p}$ lies in the exact sequence

$$0 \to \mathcal{O}_K^\times \otimes \mathbb{F}_p \to V_\emptyset / K^{\times p} \to Cl_K[p] \to 0 \tag{1.1}$$

is well-known (see, e.g., Proposition 10.7.2 of [NSW], though note that the definition of $V_\emptyset$ in [NSW] is formulated slightly differently than the one used here, but they are easily shown to be equivalent. Click here for the updated online version 2.3). Set $K' := K(\mu_p)$ and $L := K'(\sqrt[p]{V_\emptyset})$. We call L/K' the *governing extension* for K. When $K = \mathbb{Q}$ and $p = 2$ one easily has $L = \mathbb{Q}(i)$ and we have recovered the field of the Fact.

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. We thank Brian Conrad for pointing out to us a proof of Lemma 4(ii) and Peter Uttenthal for helpful suggestions. We are grateful to the referee for a careful reading of the manuscript and making many helpful suggestions.

$$\begin{tikzcd}[column sep=small]
 & L := K'(\sqrt[p]{V_\emptyset}) \arrow[dl, dash] \\
K' := K(\mu_p) \arrow[d, dash] & \\
K &
\end{tikzcd}$$

As L is obtained by adjoining to K' the pth 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 $Gal(L/K')$ 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 σ_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 (prime to p and allowing real Archimedean places if $p = 2$) of K. For $v \in S$ finite we require that $N(v) \equiv 1 \bmod p$. 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 $\sum_{v \in S} a_v \sigma_v = 0$ with all $a_v \neq 0$ in the $\mathbb{F}_p$-vector space $Gal(L/K')$.*

Theorem 1 below is a generalization of the Gras-Munnier Theorem. We first give a short proof that uses only one element of Class Field Theory, the Koch-Shafarevich formula (2.1). We easily prove Proposition 3 from (2.1), after which one only needs a standard inclusion-exclusion argument to prove Theorem 1. The cardinalities of the two sets of Theorem 1 being equal suggests a duality. In the final section of this note we give an alternative proof of Proposition 3 using the Greenberg-Wiles formula whose proof requires the full strength of global duality. Denote by G_S the Galois group over K of its maximal extension pro-p unramified outside S and recall that for $0 \neq f \in H^1(G_S, \mathbb{Z}/p\mathbb{Z}) = Hom(G_S, \mathbb{Z}/p\mathbb{Z})$, Kernel$(f)$ fixes a $\mathbb{Z}/p\mathbb{Z}$-extension of K unramified outside S. Our main result is:

Theorem 1. *Let p be a prime and S a finite set of tame places (prime to p and allowing real Archimedean places if $p = 2$) of a number field K where we require $N(v) \equiv 1 \bmod p$. The sets below have the same cardinality:*

$$\left\{ f \in \frac{H^1(G_S, \mathbb{Z}/p\mathbb{Z})}{H^1(G_\emptyset, \mathbb{Z}/p\mathbb{Z})} \;\middle|\; \textit{the extension } K_f/K \textit{ fixed by } Kernel(f) \textit{ is ramified exactly at the places of } S \right\}$$

and

$$\{\textit{Dependence relations } \sum_{v \in S} a_v \sigma_v = 0 \textit{ with all } a_v \neq 0 \textit{ in } Gal(L/K')\}.$$

When $p = 2$ there is clearly at most one dependence relation. If $K(\sqrt{\alpha_1})$ and $K(\sqrt{\alpha_2})$ are both ramified at all $v \in S$, the 'diagonal' extension $K(\sqrt{\alpha_1\alpha_2})$ is unramified everywhere, so there is a unique $f \in \dfrac{H^1(G_S, \mathbb{Z}/2\mathbb{Z})}{H^1(G_\emptyset, \mathbb{Z}/2\mathbb{Z})}$ giving rise to the ramified extension and the bijection is natural in this case.

For examples and applications, we refer the reader to [HMR], especially the examples in §3. Note that $p = 2$ in those examples and the primes of S all have trivial Frobenius element in the governing extension.

2. Proof of Theorem 1

For any field E set $\delta(E) = \begin{cases} 1 & \mu_p \subset E \\ 0 & \mu_p \not\subset E \end{cases}$. Dirichlet's unit theorem and (1.1) imply $Gal(L/K')$ is an $\mathbb{F}_p$-vector space of dimension $r_1 + r_2 - 1 + \delta(K) + \dim Cl_K[p]$ where r_1 and r_2 are the number of real and pairs of complex embeddings of K. The standard fact from class field theory that we need (see §11.3 of [K] or §10.7 of [NSW]) is a formula of Koch and Shafarevich for the dimension of the space of $\mathbb{Z}/p\mathbb{Z}$-extensions of K unramified outside a tame (prime to p and allowing real Archimedean places if $p = 2$) set Z:

$$\dim H^1(G_Z, \mathbb{Z}/p\mathbb{Z}) = -r_1 - r_2 + 1 - \delta(K) + \dim(V_Z/K^{\times p}) + \left(\sum_{v\in Z} \delta(K_v)\right). \tag{2.1}$$

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. 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. Since $\delta(K_v) = 1$, we see $\dim H^1(G_Z, \mathbb{Z}/p\mathbb{Z})$ 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. Recall that each σ_v is well-defined up to a non-zero scalar multiple so W is well-defined. Let $I := \{u_1, u_2, \cdots, u_r\} \subset S$ be such that $\{\sigma_{u_1}, \sigma_{u_2}, \cdots, \sigma_{u_r}\}$ form a basis of W and let $D := \{w_1, w_2, \cdots, w_s\} \subset S$ be the remaining elements of S. We think of the σ_{u_i} as independent elements and the σ_{w_j} as the dependent elements. Recall $L := K'(\sqrt[p]{V_\emptyset})$ so $Gal(L/K')$ is dual to $V_\emptyset/K^{\times p}$, so as we vary Z in (2.1) 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, but $\dim V_Z/K^{\times p}$ becomes one dimension smaller. Thus both sides remain unchanged. Then, as we add in the dependent places w_j of D to get to $S = I \cup D$, we are not changing the span of the Frobenius elements so we have $V_I/K^{\times p} = V_S/K^{\times p}$. Thus

$$H^1(G_\emptyset, \mathbb{Z}/p\mathbb{Z}) = H^1(G_I, \mathbb{Z}/p\mathbb{Z}) \text{ and } \dim\left(\frac{H^1(G_S, \mathbb{Z}/p\mathbb{Z})}{H^1(G_\emptyset, \mathbb{Z}/p\mathbb{Z})}\right) = s. \tag{2.2}$$

We write each σ_{w_j} uniquely as a linear combination of the σ_{u_i}:

$$R_j : \ \sigma_{w_j} - \sum_{i=1}^{r} F_{ji}\sigma_{u_i} = 0.$$

For $X \subseteq S$ let R_X be the $\mathbb{F}_p$-vector space of all dependence relations on the elements $\{\sigma_v\}_{v\in X} \subset Gal(L/K')$.

Lemma 2. *The set $\{R_1, R_2, \cdots, R_s\}$ forms a basis of the $\mathbb{F}_p$-vector space of R_S.*

Proof. Clearly $\{R_j\}_{j=1,\ldots,s}$ is independent. We show they span R_S. Consider *any* dependence relation $R \in R_S$. We can eliminate any σ_{w_j} term in R by adding a suitable multiple of R_j. We are left with a dependence relation on the σ_{u_i}, which are independent, so it is trivial. □

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

Proof. Lemma 2 and (2.2) prove this for $X = S$. For $X \subset S$, let $W_X \subset Gal(L/K')$ be the span of the Frobenius elements of X. Form I_X and D_X as we formed I and D above and apply the proof above with X, I_X and D_X playing the roles of S, I and D. □

Proposition 3 does *not* complete the proof of Theorem 1 as R_S may contain dependence relations with support properly contained in S and $\frac{H^1(G_S, \mathbb{Z}/p\mathbb{Z})}{H^1(G_\emptyset, \mathbb{Z}/p\mathbb{Z})}$ 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

$$R_S \setminus \bigcup_{v\in S} R_{S\setminus\{v\}}, \tag{2.3}$$

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 $\bigcap R_{A_i} = R_{\bigcap A_i}$, so by inclusion-exclusion

$$\#\bigcup_{v\in S} R_{S\setminus\{v\}} = \sum_{v\in S} \#R_{S\setminus\{v\}} - \sum_{v\neq w\in S} \#R_{S\setminus\{v,w\}} + \cdots \tag{2.4}$$

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

$$\frac{H^1(G_S,\mathbb{Z}/p\mathbb{Z})}{H^1(G_\emptyset,\mathbb{Z}/p\mathbb{Z})} \setminus \bigcup_{v\in S} \frac{H^1(G_{S\setminus\{v\}},\mathbb{Z}/p\mathbb{Z})}{H^1(G_\emptyset,\mathbb{Z}/p\mathbb{Z})}. \tag{2.5}$$

Since for any sets $A_i \subset S$ we have

$$\bigcap \frac{H^1(G_{A_i},\mathbb{Z}/p\mathbb{Z})}{H^1(G_\emptyset,\mathbb{Z}/p\mathbb{Z})} = \frac{H^1(G_{\cap A_i},\mathbb{Z}/p\mathbb{Z})}{H^1(G_\emptyset,\mathbb{Z}/p\mathbb{Z})},$$

we see

$$\#\bigcup_{v\in S} \frac{H^1(G_{S\setminus\{v\}},\mathbb{Z}/p\mathbb{Z})}{H^1(G_\emptyset,\mathbb{Z}/p\mathbb{Z})} = \sum_{v\in S} \# \frac{H^1(G_{S\setminus\{v\}},\mathbb{Z}/p\mathbb{Z})}{H^1(G_\emptyset,\mathbb{Z}/p\mathbb{Z})} - \sum_{v\neq w\in S} \# \frac{H^1(G_{S\setminus\{v,w\}},\mathbb{Z}/p\mathbb{Z})}{H^1(G_\emptyset,\mathbb{Z}/p\mathbb{Z})} + \cdots \tag{2.6}$$

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 theorem follows from (2.3), (2.5) and applying Proposition 3 with $X = S$. $\square$

3. A proof via the Greenberg-Wiles formula

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

Henceforth we assume the hypothesis of the Greenberg-Wiles formula that Z is a set of places of K containing all those above $\{p,\infty\}$. For each $v \in Z$, let $G_v := Gal(\bar{K}_v/K_v)$ where $\bar{K}_v$ is an algebraic closure of K_v, and consider a subspace $L_v \subseteq H^1(G_v,\mathbb{Z}/p\mathbb{Z})$. Under the perfect local duality pairing (see Chapter 7, §2 of [NSW])

$$H^1(G_v,\mathbb{Z}/p\mathbb{Z}) \times H^1(G_v,\mu_p) \to H^2(G_v,\mu_p) \simeq \frac{1}{p}\mathbb{Z}/\mathbb{Z}$$

L_v has an annihilator $L_v^\perp \subseteq H^1(G_v,\mu_p)$. Set

$$H^1_{\mathcal{L}}(G_Z,\mathbb{Z}/p\mathbb{Z}) := \text{Kernel}\left(H^1(G_Z,\mathbb{Z}/p\mathbb{Z}) \to \oplus_{v\in Z} \frac{H^1(G_v,\mathbb{Z}/p\mathbb{Z})}{L_v}\right)$$

and

$$H^1_{\mathcal{L}^\perp}(G_Z,\mu_p) := \text{Kernel}\left(H^1(G_Z,\mu_p) \to \oplus_{v\in Z} \frac{H^1(G_v,\mu_p)}{L_v^\perp}\right).$$

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

We need Lemma 4 and the Greenberg-Wiles formula below 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) For $v \nmid p$ the unramified cohomology classes $H^1_{nr}(G_v,\mathbb{Z}/p\mathbb{Z})$ and $H^1_{nr}(G_v,\mu_p)$ are exact annihilators of one another under the local duality pairing.*
(ii) Suppose $v|p$ and set $K'_v = K_v(\mu_p)$. The annihilator of $H^1_{nr}(G_v,\mathbb{Z}/p\mathbb{Z}) \subset H^1(G_v,\mathbb{Z}/p\mathbb{Z})$ is $H^1_f(G_v,\mu_p) \subset H^1(G_v,\mu_p)$, the peu ramifiée classes, namely those $f \in H^1(G_v,\mu_p)$ whose fixed field $L_{v,f}$ of Kernel$(f|_{G_{K'_v}})$ arises from adjoining the pth root of a unit $u_f \in K_v$.

Proof. (i) This is standard - see Theorem 7.2.15 of [NSW].
(ii) This result is Corollary 1.4 of Chapter III of [M], but we sketch the proof. It follows once we explain the commutative diagram below.

$$\begin{array}{ccccc}
H^1(Spec(\mathcal{O}_{K_v}),\mathbb{Z}/p\mathbb{Z}) & \times & H^1(Spec(\mathcal{O}_{K_v}),\mu_p) & \longrightarrow & H^2(Spec(\mathcal{O}_{K_v}),\mu_p)=0 \\
\big\downarrow & & \big\downarrow & & \big\downarrow \\
H^1(G_v,\mathbb{Z}/p\mathbb{Z}) & \times & H^1(G_v,\mu_p) & \longrightarrow & H^2(G_v,\mu_p)=\frac{1}{p}\mathbb{Z}/\mathbb{Z}
\end{array}$$

Cohomology taken over $Spec(\mathcal{O}_{K_v})$ is flat. The rows are cup product pairings in flat and Galois cohomology. Recall $\mathbb{Z}/p\mathbb{Z} \simeq H^1_{nr}(G_v,\mathbb{Z}/p\mathbb{Z}) = H^1(Spec(\mathcal{O}_{K_v}),\mathbb{Z}/p\mathbb{Z}) \subset H^1(G_v,\mathbb{Z}/p\mathbb{Z})$ and

$$H^1_f(G_v,\mu_p) = H^1(Spec(\mathcal{O}_{K_v}),\mu_p) = \mathcal{O}^\times_{K_v}/\mathcal{O}^{\times p}_{K_v} \subset K_v^\times/K_v^{\times p} = H^1(G_v,\mu_p)$$

where the containment is codimension one as $\mathbb{F}_p$-vector spaces. Lemma 1.1 of Chapter III of [M] gives the two left vertical injections and the triviality of the top pairing. This last pairing is consistent with the local duality pairing of the bottom row of the above diagram. As $H^1_{nr}(G_v,\mathbb{Z}/p\mathbb{Z}) \subset H^1(G_v,\mathbb{Z}/p\mathbb{Z})$ and $H^1_f(G_v,\mu_p) \subset H^1(G_v,\mu_p)$ are dimension 1 and codimension 1 respectively, they are exact annihilators of one another, proving (ii). □

Theorem *(Greenberg-Wiles) Assume Z contains all places above $\{p,\infty\}$. Then*

$$\begin{aligned}&\dim H^1_{\mathcal{L}}(G_Z,\mathbb{Z}/p\mathbb{Z}) - \dim H^1_{\mathcal{L}^\perp}(G_Z,\mu_p) = \\ &\dim H^0(G_Z,\mathbb{Z}/p\mathbb{Z}) - \dim H^0(G_Z,\mu_p) + \textstyle\sum_{v\in Z}\left(\dim L_v - \dim H^0(G_v,\mathbb{Z}/p\mathbb{Z})\right).\end{aligned}$$

See Theorem 8.7.9 of [NSW] for a proof.

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_∞ is the set of all real Archimedean places of K (so $X_\infty \subseteq Z_\infty$).

For v complex Archimedean we have $G_v = \{e\}$ so the Selmer and dual Selmer conditions are trivial. For v real Archimedean, $\dim H^1(G_v,\mathbb{Z}/2\mathbb{Z}) = \dim H^1(G_v,\mu_2) = 1$ 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 $H^1_{\mathcal{M}}(G_Z,\mathbb{Z}/p\mathbb{Z}) = H^1(G_X,\mathbb{Z}/p\mathbb{Z})$ and $H^1_{\mathcal{N}}(G_Z,\mathbb{Z}/p\mathbb{Z}) = H^1(G_\emptyset,\mathbb{Z}/p\mathbb{Z})$. We now establish the validity of the entries in the table. The previous paragraph and Lemma 4 justify the stated dual Selmer conditions of the table. The first three entries of the right column are clear. As $\delta(K_v) = 1$, local class field theory implies $\dim H^1(G_v,\mathbb{Z}/p\mathbb{Z}) = 2$. That $\dim H^1_{nr}(G_v,\mathbb{Z}/p\mathbb{Z}) = 1$ follows as there is a unique unramified $\mathbb{Z}/p\mathbb{Z}$-extension of any local field. This establishes the last entry.

	M_v	$M_v^\perp$	N_v	$N_v^\perp$	$\dim M_v - \dim N_v$
$v \in Z_p$	$H^1_{nr}(G_v,\mathbb{Z}/p\mathbb{Z})$	$H^1_f(G_v,\mu_p)$	$H^1_{nr}(G_v,\mathbb{Z}/p\mathbb{Z})$	$H^1_f(G_v,\mu_p)$	0
$v \in X_\infty$	$H^1(G_v,\mathbb{Z}/2\mathbb{Z})$	0	$H^1_{nr}(G_v,\mathbb{Z}/2\mathbb{Z})=0$	$H^1(G_v,\mu_2)$	1
$v \in Z_\infty \setminus X_\infty$	$H^1_{nr}(G_v,\mathbb{Z}/2\mathbb{Z})=0$	$H^1(G_v,\mu_2)$	$H^1_{nr}(G_v,\mathbb{Z}/2\mathbb{Z})=0$	$H^1(G_v,\mu_2)$	0
$v \in X_{<\infty}$	$H^1(G_v,\mathbb{Z}/p\mathbb{Z})$	0	$H^1_{nr}(G_v,\mathbb{Z}/p\mathbb{Z})$	$H^1_{nr}(G_v,\mu_p)$	1

Applying the Greenberg-Wiles formula for $\{M_v\}_{v\in Z}$ and $\{N_v\}_{v\in Z}$ and subtracting the second equation from the first and recalling $\#X = \#I + \#D = r + s$:

$$\begin{aligned}&\dim H^1(G_X,\mathbb{Z}/p\mathbb{Z}) - \dim H^1(G_\emptyset,\mathbb{Z}/p\mathbb{Z}) = \\ &\dim H^1_{\mathcal{M}}(G_Z,\mathbb{Z}/p\mathbb{Z}) - \dim H^1_{\mathcal{N}}(G_Z,\mathbb{Z}/p\mathbb{Z}) = \\ &\dim H^1_{\mathcal{M}^\perp}(G_Z,\mu_p) - \dim H^1_{\mathcal{N}^\perp}(G_Z,\mu_p) + \textstyle\sum_{v\in Z}(\dim M_v - \dim N_v) = \\ &\dim H^1_{\mathcal{M}^\perp}(G_Z,\mu_p) - \dim H^1_{\mathcal{N}^\perp}(G_Z,\mu_p) + r + s.\end{aligned} \tag{3.1}$$

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 $\{\sigma_v\}_{v\in X} \subset W = Gal(K'(\sqrt[p]{V_\emptyset})/K')$.

An element $f \in H^1_{\mathcal{N}^\perp}(G_Z, \mu_p)$ 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 $K'\left(\sqrt[p]{V_\emptyset}\right)$.

$$\begin{tikzcd}[column sep=small]
 & L_f := K'\left(\sqrt[p]{\alpha_f}\right) \arrow[dl, dash] \\
K' := K(\mu_p) \arrow[d, dash] & \\
K &
\end{tikzcd}$$

By the nature of cohomology classes in $H^1(G_Z, \mu_p)$, the extension L_f/K is Galois. Kummer Theory implies $\alpha_f \in K'/K'^{\times p}$, which decomposes into ω^i-eigenspaces where $\omega : Gal(K'/K) \to (\mathbb{Z}/p\mathbb{Z})^\times$ is the cyclotomic character given by $\sigma(\zeta_p) = \zeta_p^{\omega(\sigma)}$ for ζ_p a primitive pth root of unity. As $\mu_p \simeq \mathbb{Z}/p\mathbb{Z}(\omega)$, Kummer Theory gives the $Gal(K'/K)$-equivariant pairing

$$\frac{\alpha_f K'^{\times p}}{K'^{\times p}} \times Gal(L_f/K') \to \mu_p \simeq \mathbb{Z}/p\mathbb{Z}(\omega).$$

That $f \in H^1(G_Z, \mathbb{Z}/p\mathbb{Z}(\omega))$ implies $Gal(L_f/K')$ is in the ω-eigenspace as is $\mathbb{Z}/p\mathbb{Z}(\omega)$. Thus α_f is in the trivial eigenspace of $K'^\times/K'^{\times p}$. We will show we may assume $\alpha_f \in K$. If $K' = K$ this is obvious so we assume $1 < d = [K' : K] \mid p-1$. Since α_f is in the trivial eigenspace, $N_K^{K'}(\alpha_f) \equiv \alpha_f^d$ mod $K'^{\times p}$. But $N_K^{K'}(\alpha_f) \in K^\times$ and $(d,p) = 1$ so a suitable power $N_K^{K'}(\alpha_f)^r$ is congruent to α_f mod $K'^{\times p}$. Just replace α_f by $N_K^{K'}(\alpha_f)^r \in K$.

Since L_f/K' is unramified at all finite tame v we have $\alpha_f = u\pi_v^{pr}$ where $u \in K_v$ is a unit and π_v is a uniformizer. At $v \in Z_p$ being peu ramifiée implies that locally at $v \in X_p$ we again have $\alpha_f = u\pi_v^{pr}$. Together, these mean that the fractional ideal (α_f) of K is a pth power, which implies that $\alpha_f \in V_\emptyset$. Conversely, if $\alpha \in V_\emptyset$, then, recalling that $(\alpha) = J^p$ for some ideal of K, we have that $K'\left(\sqrt[p]{\alpha}\right)/K'$ is a $\mathbb{Z}/p\mathbb{Z}$-extension peu ramifiée at $v \in Z_p$, with no condition at $v \in Z_\infty$. Thus α gives rise to an element $f_\alpha \in H^1_{\mathcal{N}^\perp}(G_Z, \mu_p)$ so $L := K'\left(\sqrt[p]{V_\emptyset}\right)$ is the composite of all L_f for $f \in H^1_{\mathcal{N}^\perp}(G_Z, \mu_p)$ and $\dim H^1_{\mathcal{N}^\perp}(G_Z, \mu_p) = \dim(V_\emptyset/K^{\times p})$.

An element $f \in H^1_{\mathcal{M}^\perp}(G_Z, \mu_p)$ 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 $D \subset K'\left(\sqrt[p]{V_\emptyset}\right)$.

$$\begin{tikzcd}[column sep=small]
 & & L := K'\left(\sqrt[p]{V_\emptyset}\right) \arrow[dl, dash] \\
 & D \arrow[dl, dash] & \\
K' := K(\mu_p) \arrow[d, dash] & & \\
K & &
\end{tikzcd}$$

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 $\dim_{\mathbb{F}_p} Gal\left(K'\left(\sqrt[p]{V_\emptyset}\right)/D\right) = r = \#I$ from the second section of this note. Thus

$\dim H^1_{\mathcal{M}^\perp}(G_Z, \mu_p) = \dim(V_\emptyset/K^{\times p}) - r$ so the right side of (3.1) is

$$\big(\dim(V_\emptyset/K^{\times p}) - r\big) - \dim(V_\emptyset/K^{\times p}) + (r+s) = s = \dim R_X$$

proving Proposition 3. □

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.; Munnier, A., *Extensions cycliques T-totalement ramifiées*, Publ. Math. Besançon, 1997/98.

[HMR] Hajir, F.; Maire, C.; Ramakrishna, R. *On the Shafarevich group of restricted ramification extensions of number fields in the tame case*, Indiana Univ. Math. J. 70 (2021), no. 6, 2693-2710.

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

[M] Milne, J. *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, corrected second printing. 2013.

Department of Mathematics & Statistics, University of Massachusetts, Amherst, MA 01003, USA

FEMTO-ST Institute, Université de Franche-Comté, CNRS, 15B avenue des Montboucons, 25000 Besançon, FRANCE

Department of Mathematics, Cornell University, Ithaca, NY 14853-4201USA

E-mail address: hajir@math.umass.edu, christian.maire@univ-fcomte.fr, ravi@math.cornell.edu