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 in terms of 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 a standard result that there exists a quadratic extension $K/\mathbb{Q}$ ramified at exactly the set of places $\{v : v|D\}$ if and only if $D \equiv 1 \mod 4$. 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 $\sum_{v \in S} \sigma_v$ is the trivial element in $Gal(\mathbb{Q}(i)/\mathbb{Q})$.*

[GM] generalized this result to $\mathbb{Z}/p\mathbb{Z}$-extensions of a general number field K. To explain the result precisely we need some notation and terminology. For a fixed prime p and set S of tame places, let

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

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 Proposition 10.7.2 of [NSW]. Set $K' = K(\mu_p)$, $L = K'(\sqrt[p]{V_\emptyset})$ 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 Fact.

$$\begin{tikzcd} & L := K'(\sqrt[p]{V_\emptyset}) \\ K' := K(\mu_p) \arrow[ur, dash] & \\ K \arrow[u, dash] & \end{tikzcd}$$

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 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 (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 $Gal(L/K')$ with all $a_v \neq 0$.*

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, (2.1) below, and elementary linear algebra in characteristic p. 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 of a number field K (allowing Archimedean places if $p = 2$). The sets*

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

and

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

have the same cardinality.

When $p = 2$ both sets have cardinality at most one 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 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 $r_1 + r_2 - 1 + \delta(K) + \dim Cl_K[p]$. 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:

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

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. If $\delta(K_v) = 0$ 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 $\delta(K_v) = 1$. 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. Recall that each σ_v is only well-defined up to the line that it spans 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. 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, 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

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

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

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

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 σ_{u_i} and σ_{w_j}.*

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

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

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 $X = S$. Apply the same proof to $X \subseteq S$. □

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 result 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.

As we will need to apply the Greenberg-Wiles 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 $G_v := Gal(\bar{K}_v/K_v)$ 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 $f \in H^1_f(G_v, \mu_p)$ 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 7.2.15 of [NSW].
(ii) Cohomology taken over $Spec(\mathcal{O}_{K_v})$ in what follows is flat. Here

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

where the containment is codimension one as $\mathbb{F}_p$-vector spaces. Recall

$$\mathbb{Z}/p\mathbb{Z} \simeq H^1_{nr}(G_v, \mathbb{Z}/p\mathbb{Z}) = H^1(Spec(\mathcal{O}_{K_v}), \mathbb{Z}/p\mathbb{Z})$$

and by Lemma 1.1 of Chapter III of [M] we have the injections

$$H^1(Spec(\mathcal{O}_{K_v}), \mathbb{Z}/p\mathbb{Z}) \hookrightarrow H^1(G_v, \mathbb{Z}/p\mathbb{Z}) \text{ and } H^1(Spec(\mathcal{O}_{K_v}), \mu_p) \hookrightarrow H^1(G_v, \mu_p)$$

and the pairing

$$H^1(Spec(\mathcal{O}_{K_v}), \mathbb{Z}/p\mathbb{Z}) \times H^1(Spec(\mathcal{O}_{K_v}), \mu_p) \to H^2(Spec(\mathcal{O}_{K_v}), \mu_p) = 0.$$

This last pairing is consistent with the local duality pairing

$$H^1(G_v,\mathbb{Z}/p\mathbb{Z})\times H^1(G_v,\mu_p)\to H^2(G_v,\mu_p)=\frac{1}{p}\mathbb{Z}/\mathbb{Z}. \tag{3.1}$$

As $H^1(Spec(\mathcal{O}_{K_v}),\mathbb{Z}/p\mathbb{Z})=H^1_{nr}(G_v,\mathbb{Z}/p\mathbb{Z})$ and $H^1(Spec(\mathcal{O}_{K_v}),\mu_p)=H^1_f(G_v,\mu_p)$ 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 in (3.1), 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 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 $H^1_{\mathcal{N}}(G_Z,\mathbb{Z}/p\mathbb{Z})=H^1(G_\emptyset,\mathbb{Z}/p\mathbb{Z})$. The previous paragraph and Lemma 4 justify the stated dual Selmer conditions of the table.

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

Applying the Greenberg-Wiles formula for $\{M_v\}_{v\in Z}$ and $\{N_v\}_{v\in Z}$ and subtracting the first equation from the second:

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

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

$$\dim M_v-\dim N_v=\begin{cases}0 & v\in Z_p\\ 1 & v\in X_\infty,\ p=2\\ 0 & v\in Z_\infty\setminus X_\infty\\ 1 & v\in X_{<\infty}\end{cases},$$

and then

$$\dim\left(\frac{H^1(G_X,\mathbb{Z}/p\mathbb{Z})}{H^1(G_\emptyset,\mathbb{Z}/p\mathbb{Z})}\right)=\dim H^1_{\mathcal{M}^\perp}(G_Z,\mu_p)-\dim H^1_{\mathcal{N}^\perp}(G_Z,\mu_p)+\#X. \tag{3.2}$$

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 $K'\left(\sqrt[p]{V_\emptyset}\right)$.

$$
\begin{tikzcd}[arrows=dash]
 & L_f := K'\left(\sqrt[p]{\alpha_f}\right) \\
K' := K(\mu_p) \arrow[ur] & \\
K \arrow[u] &
\end{tikzcd}
$$

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 pth powers) $\alpha_f \in K$. Since L_f/K' is unramified at $v \in X_{<\infty}$, we see that at all such v that $\alpha_f = u\pi_v^{pr}$ 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 $\alpha_f = u\pi_v^{pr}$ where $u \in K_v$ is a unit. 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 $D \subset K'\left(\sqrt[p]{V_\emptyset}\right)$.

$$
\begin{tikzcd}[arrows=dash]
 & & L := K'\left(\sqrt[p]{V_\emptyset}\right) \\
 & D \arrow[ur] & \\
K' := K(\mu_p) \arrow[ur] & & \\
K \arrow[u] & &
\end{tikzcd}
$$

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 first section of this note. Thus $\dim H^1_{\mathcal{M}^\perp}(G_Z, \mu_p) = \dim(V_\emptyset/K^{\times p}) - r$ so

$$
\begin{gathered}
\dim H^1_{\mathcal{M}^\perp}(G_Z, \mu_p) - \dim H^1_{\mathcal{N}^\perp}(G_Z, \mu_p) + \#X = \\
\left(\dim(V_\emptyset/K^{\times p}) - r\right) - \dim(V_\emptyset/K^{\times p}) + (r + s) = s = \dim R_X
\end{gathered}
$$

and we have shown the the left hand side of (3.2) is $\dim R_X$ 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. 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.; Wingeberg, K. *Cohomology of Number Fields*, Springer. Second edition, second corrected 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