INCREASING THE SIZE OF TAME SHAFAREVICH GROUPS

ANDREEA IORGA, RAVI RAMAKRISHNA

Abstract. Let K be a number field with a finite set S of primes. We study the cohomology of $\mathbb{F}_p[G_{K,S}]$-modules A, in particular the Shafarevich groups $Ш^i_S(K,A)$ for $i=1,2$ for tame sets S, i.e., for sets S that contain no primes above p. When S contains all primes above p (the "wild" setting), it is a consequence of global Poitou-Tate duality that $Ш^1_S(K,A')^\vee \simeq Ш^2_S(K,A) \overset{\simeq}{\hookrightarrow} Б_S(K,A)$ is non-increasing as S increases. The same applies when $G_{K,S}$ is replaced by its maximal pro-p quotient $G_{K,S}(p)$. In [4] it was shown that for S tame and $A=\mathbb{F}_p$ with trivial action, the group $Ш^2_S(K,A)$ can *increase* as S increases to $S\cup X$, and even attain its maximal dimension, $\dim_{\mathbb{F}_p} Б_S(K,\mathbb{F}_p)$, for carefully chosen X. We strengthen this to general $\mathbb{F}_p[G_{K,S}]$-modules A where S is tame. We use Liu's definition [7] of $Б_S(K,A)$ to show that $Ш^2_S(K,A)\hookrightarrow Б_S(K,A)$ and that there exist infinitely many tame sets of primes X of K such that $Ш^2_{S\cup X}(K,A) \overset{\simeq}{\hookrightarrow} Б_{S\cup X}(K,A) \overset{\simeq}{\twoheadleftarrow} Б_S(K,A) \hookleftarrow Ш^2_S(K,A)$.

1. Introduction

Let K be a number field with an algebraic closure $\overline{K}$ and set $G_K=\mathrm{Gal}(\overline{K}/K)$. Let S a finite set of primes of K, and p a fixed rational prime. Denote by $K_S\subset\overline{K}$ the maximal extension of K unramified outside S and by $K_S(p)\subset K_S$ the maximal pro-p extension of K unramified outside S, with $G_{K,S}$ and $G_{K,S}(p)$ the corresponding Galois groups over K. Let $K_\mathfrak{q}$ be the completion of K at the prime ideal $\mathfrak{q}$ and let $G_{K_\mathfrak{q}}$ be an absolute Galois group of $K_\mathfrak{q}$ with $G_{K_\mathfrak{q}}(p)$ its maximal pro-p quotient. For a finite cardinality $G_{K,S}$-module A, let

$$Ш^i_S(K,A)=\ker\left(H^i(G_{K,S},A)\to\prod_{\mathfrak{q}\in S}H^i(G_{K_\mathfrak{q}},A)\right),$$

as usual. As A decomposes as a direct sum of p-primary modules and cohomology commutes with direct sums, it suffices to assume A is a finite cardinality $\mathbb{Z}_p[G_{K,S}]$-module.

When S contains all primes dividing p (the "wild" setting), Poitou-Tate duality gives that $Ш^2_S(K,A)\simeq Ш^1_S(K,A')^\vee$ where $A':=\mathrm{Hom}(A,\mu_{p^\infty})$ and μ_{p^∞} is the group of all p-power roots of unity. There is also a global Euler-Poincaré characteristic formula:

$$\frac{\#H^0(G_{K,S},A)\cdot\#H^2(G_{K,S},A)}{\#H^1(G_{K,S},A)}=\prod_{\mathfrak{q}\mid\infty}\frac{\#H^0(G_{K_\mathfrak{q}},A)}{|\#A|_\mathfrak{q}}.$$

As H^0s are "easy" to calculate, this can be thought of as an H^1-H^2 duality: knowledge of one of these cohomology groups gives the other. A key ingredient in the proof of the wild Poitou-Tate duality is the exact Kummer sequence below, where $\mathcal{O}^\times_{K_S,S}$ is the group of S-units of K_S:

$$1\to\mu_p\to\mathcal{O}^\times_{K_S,S}\xrightarrow{x\mapsto x^p}\mathcal{O}^\times_{K_S,S}\to 1.$$

The authors thank Farshid Hajir and Christian Maire for helpful conversations, and Ariane Mézard for detailed comments and corrections on an early draft of the paper. The second author was supported by a Simons Travel support grant.

If S is tame, that is, if S contains no primes above p, the pth power map need not be surjective, as extracting a pth root usually introduces ramification at p.

Our goal is to obtain a partial duality result in the tame case. Recall the following definitions:

$$V_S(K,\mathbb{F}_p) := \{x \in K^\times \mid v_\mathfrak{q}(x) \equiv 0 \bmod p,\ \forall \mathfrak{q};\ x \in K_\mathfrak{q}^{\times p},\ \forall \mathfrak{q} \in S\}$$

and the dual of $V_S(K,\mathbb{F}_p)/K^{\times p}$:

$$\text{Б}_S(K,\mathbb{F}_p) := (V_S(K,\mathbb{F}_p)/K^{\times p})^\vee.$$

It is a well-known fact that for arbitrary S we have the injection $\text{Ш}^2_S(K,\mathbb{F}_p) \hookrightarrow \text{Б}_S(K,\mathbb{F}_p)$, and that this injection is an isomorphism if S contains all primes above p. Furthermore, $\dim_{\mathbb{F}_p} \text{Б}_S(K,\mathbb{F}_p) < \infty$ for all sets S. Let $\mathrm{Cl}_K[p]$ denote the p-torsion subgroup of the class group of K. When $S = \emptyset$, we have the exact sequence:

$$0 \to \frac{U_K}{U_K^p} \to \frac{V_\emptyset(K,\mathbb{F}_p)}{K^{\times p}} \to \mathrm{Cl}_K[p] \to 0. \tag{1}$$

Thus understanding $\text{Ш}^2_\emptyset(K,\mathbb{F}_p) \hookrightarrow \text{Б}_\emptyset(K,\mathbb{F}_p)$ involves, at a minimum, disentangling the units and class group of K. For references, see §11.2 and §11.3 of [5] and Theorem 8.6.7 and Proposition 10.7.2 of [8].

Building on the work of Labute [6], Schmidt [9] has proved that for an arbitrary number field K and an odd prime p, there exists a finite set Y of tame primes such that $G_{K,Y}(p)$ has p-cohomological dimension 2, and its Galois cohomology agrees with the étale cohomology of $\mathrm{Spec}(\mathcal{O}_K \setminus Y)$. Schmidt's proof relies on, among other things, choosing Y so that $\text{Б}_Y(K,\mathbb{F}_p)$ and $\text{Ш}^2_Y(K,\mathbb{F}_p)$ are trivial.

On the one hand, for a general tame set S, it is very difficult to have any control over the group $\text{Ш}^2_S(K,\mathbb{F}_p)$, and therefore to decide if $\text{Ш}^2_S(K,\mathbb{F}_p) \hookrightarrow \text{Б}_S(K,\mathbb{F}_p)$ is a proper inclusion or an isomorphism. On the other hand, setting

$$\text{Ш}^2_{S,p}(K,\mathbb{F}_p) := \ker\left(H^2(G_{K,S}(p),\mathbb{F}_p) \to \prod_{\mathfrak{q}\in S} H^2(G_{K_\mathfrak{q}}(p),\mathbb{F}_p)\right)$$

and using Proposition 20 in [10, II.§5.6], we have

$$\text{Ш}^2_{S,p}(K,\mathbb{F}_p) = \ker\left(H^2(G_{K,S}(p),\mathbb{F}_p) \to \prod_{\mathfrak{q}\in S} H^2(G_{K_\mathfrak{q}},\mathbb{F}_p)\right).$$

It is easy to show $\text{Ш}^2_{S,p}(K,\mathbb{F}_p) \hookrightarrow \text{Ш}^2_S(K,\mathbb{F}_p)$ (see Lemma 7) and then one can construct examples in which the cokernel of $\text{Ш}^2_{S,p}(K,\mathbb{F}_p) \hookrightarrow \text{Б}_S(K,\mathbb{F}_p)$ is large. In [4], it is shown that if S is a (possibly empty) tame set of primes of K and p is odd, then there exist infinitely many finite tame sets X such that

$$\text{Ш}^2_{S\cup X,p}(K,\mathbb{F}_p) \overset{\simeq}{\hookrightarrow} \text{Ш}^2_{S\cup X}(K,\mathbb{F}_p) \overset{\simeq}{\hookrightarrow} \text{Б}_{S\cup X}(K,\mathbb{F}_p) \overset{\simeq}{\twoheadleftarrow} \text{Б}_S(K,\mathbb{F}_p). \tag{2}$$

A slightly weaker result is obtained for $p = 2$. In contrast to Schmidt's result, X is chosen so $\text{Ш}^2_{S\cup X}(K,\mathbb{F}_p)$ is *maximized* as opposed to trivialized. As in Schmidt's work, the primes of X must be chosen to split appropriately in a certain governing field. For a definition of governing fields and a more detailed discussion, see [3, Chapter V]. Recall that for a prime

p and field F we define $\delta_p(F) = \begin{cases} 1 & \mu_p \subset F \\ 0 & \mu_p \not\subset F \end{cases}$ and for a prime $\mathfrak{q}$ of a number field F, we set $\chi(\mathfrak{q})$ to be the residue characteristic of $\mathfrak{q}$. From Theorem 11.8 of [5] we have

$$\dim H^1(G_{K,Z}, \mathbb{F}_p) = \sum_{\substack{\mathfrak{q}\in Z \\ \chi(\mathfrak{q})=p}} [K_\mathfrak{q} : \mathbb{Q}_p] - \delta(K) - r + 1 + \sum_{\mathfrak{q}\in Z} \delta_p(K_\mathfrak{q}) + \dim Б_Z(K, \mathbb{F}_p), \tag{3}$$

so when (2) holds, we have a partial tame H^1-H^2 duality.

In [7], Liu generalizes the definition $Б_S(K, \mathbb{F}_p)$ to finite cardinality $\mathbb{Z}_p[G_{K,S}]$-modules A. The dual of the map on the right below is, using local duality, just the restriction map.

$$Б_S(K, A) := \operatorname{coker}\left(\prod_{\mathfrak{q}\in S} H^1(G_{K_\mathfrak{q}}, A) \times \prod_{\mathfrak{q}\notin S} H^1_{nr}(G_{K_\mathfrak{q}}, A) \to H^1(G_K, A')^\vee\right).$$

When S is wild, it is an exercise in local duality ([7, Lemma 8.7]) to see that $Б_S(K, A)$ is dual to $Ш^1_S(K, A')$. We use the subscript "all" to indicate S is all places of K.

Our first result generalizes the classical injection $Ш^2_S(K, \mathbb{F}_p) \hookrightarrow Б_S(K, \mathbb{F}_p)$. We use the notation of [7] to state Theorem 1 as that paper was the inspiration for *(i)* below.

Theorem 1. *Let A be any finite cardinality $G_{K,S}$-module.*

(i) There is a natural injection $Ш^2_S(K, A) \hookrightarrow Б_S(K, A)$. We have $Б_{all}(K, A) = 0$ and $Ш^2_{all}(K, A) = 0$.

(ii) If K/Q is a finite Galois extension of number fields, S is a set of primes of K that is stable under the action of $\mathrm{Gal}(K/Q)$ and A is a finite cardinality $\mathrm{Gal}(K_S/Q)$-module, then the injection $Ш^2_S(K, A) \hookrightarrow Б_S(K, A)$ is $\mathrm{Gal}(K/Q)$-equivariant.

In [7], a version of *(i)* is established K-theoretically, that is both sides are acted on by $\mathrm{Gal}(K/Q)$ with $(\#\,\mathrm{Gal}(K/Q), p) = 1$. Liu shows the multiplicity of any irreducible constituent on the left side is less than on the right side. When $K = Q$, the result becomes $\dim Ш^2_S(K, A) \le \dim Б_S(K, A)$. We establish an actual injection. Note that Q here is any number field, and need not be $\mathbb{Q}$.

Before introducing the main results of this paper, we need some definitions.

Definition 1. *For a finite cardinality $\mathbb{Z}_p[G_K]$-module A, let $L := K(A)$ be the splitting field of A. Set $\Gamma = \mathrm{Gal}(L/K)$. If T is a set of primes of K, let $\tilde{T}$ be the set of primes of L above those in T.*

Note that if S is a set of primes of K and A is a finite $\mathbb{Z}_p[G_{L,\tilde{S}}(p) \rtimes \Gamma]$-module with the property that $\Gamma = \mathrm{Gal}(L/K) = \mathrm{Gal}(K(A)/K)$ has order prime to p, the fields L and $K_S(p)$ are linearly disjoint over K. It follows that there is no action of $G_{K,S}(p)$ on A, so the object $Ш^2_{S,p}(K, \mathbb{F}_p)$ (or $Ш^2_{S,p}(K, A)$) does not exist. In this situation, we make the following:

Definition 2. *Consider the semidirect product $G_{L,\tilde{S}}(p) \rtimes \Gamma$, given by the conjugation action of the prime-to-p group Γ on the pro-p group $G_{L,\tilde{S}}(p)$. For a finite cardinality $\mathbb{Z}_p[G_{L,\tilde{S}}(p) \rtimes \Gamma]$-module A, define the following group:*

$$Ш^2(L_{\tilde{S}}(p)/K, A) := \ker\left(H^2(G_{L,\tilde{S}}(p) \rtimes \Gamma, A) \to \prod_{\mathfrak{p}\in S} H^2(G_{K_\mathfrak{p}}, A)\right).$$

Note that the map above is obtained by restricting $H^2(G_{L,\tilde{S}}(p) \rtimes \Gamma, A)$ to the decomposition subgroups at $\mathfrak{p}$ and then inflating to $H^2(G_{K_\mathfrak{p}}, A)$.

When $\tilde{S}$ is wild, the cohomology theory of such groups was developed in [2] as part of the proof of the Sato-Tate conjecture, and later in [7] to obtain results about the number of generators of profinite Galois groups.

The main results of this paper are the following generalizations of [4, Theorem A]:

Proposition 2. *Let p be an odd prime and let A be a finite cardinality $\mathbb{F}_p[G_K]$-module. Let S be a finite set of tame primes of K. Then there exist infinitely many finite tame sets X of places of K such that*

$$(\text{Ш}^2_{\tilde{S}\cup\tilde{X},p}(L,A))^\Gamma \overset{\simeq}{\hookrightarrow} (\text{Ш}^2_{\tilde{S}\cup\tilde{X}}(L,A))^\Gamma \overset{\simeq}{\hookrightarrow} \text{Б}_{\tilde{S}\cup\tilde{X}}(L,A)^\Gamma \overset{\simeq}{\twoheadleftarrow} \text{Б}_{\tilde{S}}(L,A)^\Gamma.$$

Theorem 3. *With the notations as above, suppose S contains all ramified primes of L/K and $(\#\Gamma, p) = 1$. Then there exist infinitely many finite tame sets X of places of K such that*

$$\text{Ш}^2(L_{\tilde{S}\cup\tilde{X}}(p)/K,A) \overset{\simeq}{\hookrightarrow} \text{Ш}^2_{S\cup X}(K,A) \overset{\simeq}{\hookrightarrow} \text{Б}_{S\cup X}(K,A) \overset{\simeq}{\twoheadleftarrow} \text{Б}_S(K,A) \hookleftarrow \text{Ш}^2(L_{\tilde{S}}(p)/K,A).$$

While Schmidt's work [9] gives a very strong tame duality theorem by choosing S such that $\text{Б}_S(K,\mathbb{F}_p) = 0$, our results represent progress towards establishing a tame duality when $\text{Б}_S(K,A) \neq 0$. The obstruction to formulating an actual H^1-H^2 duality in this case lies in the significant difficulty of determining the image of the localization map. Theorem 3 most naturally generalizes the main result of [4], but if the set of ramified primes of L/K contains primes that are *not* in $\tilde{S}$, Proposition 2 is the natural result. In Section 4, we also prove that any isomorphism $\text{Ш}^2(L_{\tilde{T}}(p)/K,A) \overset{\simeq}{\hookrightarrow} \text{Ш}^2_T(K,A) \overset{\simeq}{\hookrightarrow} \text{Б}_T(K,A)$ is preserved if we increase the set T (see Corollary 11).

The method of proof of Proposition 2 is to pass to the field L where A is a trivial Galois module. Using the main result of [4] we obtain

$$\begin{tikzcd}
\text{Ш}^2_{\tilde{S},p}(L,\mathbb{F}_p^{\dim A}) \arrow[r, hook] & \text{Ш}^2_{\tilde{S}}(L,\mathbb{F}_p^{\dim A}) \arrow[r, hook] & \text{Б}_{\tilde{S}}(L,\mathbb{F}_p^{\dim A}) \arrow[d, two heads, "\simeq"] \\
\text{Ш}^2_{\tilde{S}\cup X',p}(L,\mathbb{F}_p^{\dim A}) \arrow[r, hook, "\simeq"] & \text{Ш}^2_{\tilde{S}\cup X'}(L,\mathbb{F}_p^{\dim A}) \arrow[r, hook, "\simeq"] & \text{Б}_{\tilde{S}\cup X'}(L,\mathbb{F}_p^{\dim A})
\end{tikzcd}$$

for infinitely many finite sets X' of primes of L. The key ingredient of this proof is Lemma 10, which proves that the above isomorphisms persist when we replace X' by its $\mathrm{Gal}(L/K)$-orbit $\tilde{X}$. We then take Γ-invariants to obtain Proposition 2. The descent to K in Theorem 3 uses that $(\#\Gamma, p) = 1$. The reason for working only with Galois modules that are vector spaces over $\mathbb{F}_p$ is because the results of [4] only hold for $A = \mathbb{F}_p$. To obtain our result for finite cardinality $\mathbb{Z}_p[G_K]$-modules would require extending those results to the trivial Galois modules $\mathbb{Z}/p^k\mathbb{Z}$.

In §2 we prove Theorem 1. In §3 we prove some lemmas needed in §4. In §4 we prove Proposition 2 and Theorem 3. In §5 we address the case $p = 2$. The results of [4] are slightly weaker in this case, leading to our slightly weaker results. In §6 we give explicit examples.

Definitions and Notations

- p: A prime number.
- K: A number field.
- G_K: The absolute Galois group of K.
- $\mathcal{O}_K$: The ring of integers of K.
- A prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is called tame if $\#\mathcal{O}_K/\mathfrak{p} \equiv 1 \pmod{p}$.
- K_S, $K_S(p)$: If S is a set of primes, K_S (resp. $K_S(p)$) is the maximal extension of K unramified outside S (resp. the maximal pro-p extension of K unramified outside S).
- $G_{K,S} := \mathrm{Gal}(K_S/K)$, $G_{K,S}(p) := \mathrm{Gal}(K_S(p)/K)$.
- A: A finite cardinality $\mathbb{Z}_p[G_{K,S}]$-module with dual $A' := \mathrm{Hom}(A, \mu_{p^\infty})$.
- $L := K(A)$: The splitting field of A, i.e., the subextension of K_S/K such that $\mathrm{Gal}(K_S/L)$ is the maximal subgroup of $G_{K,S}$ which acts trivially on A.
- $\Gamma := \mathrm{Gal}(L/K)$.
- $\tilde{T}$: For T a set of primes of K, this is the set of primes of L above T.
- $K_{\mathfrak{p}}$: For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, this is the completion of K at $\mathfrak{p}$.
- $G_{K_{\mathfrak{p}}}$, $G_{K_{\mathfrak{p}}}(p)$: The absolute Galois group of $K_{\mathfrak{p}}$ and its maximal pro-p quotient.
- $\mathcal{T}_{\mathfrak{p}}(K)$: The inertia subgroup of $G_{K_{\mathfrak{p}}}$.
- $H^1_{nr}(G_{K_{\mathfrak{p}}}, A) := \ker(H^1(G_{K_{\mathfrak{p}}}, A) \to H^1(\mathcal{T}_{\mathfrak{p}}(K), A))$. This is the unramified cohomology.
- $Ш^i_S(K, A) := \ker\left(H^i(G_{K,S}, A) \to \prod_{\mathfrak{p}\in S} H^i(G_{K_{\mathfrak{p}}}, A)\right)$.
- $$Ш^2_{\tilde{S},p}(L, A) := \ker\left(H^2(G_{L,\tilde{S}}(p), A) \to \prod_{\mathfrak{p}\in\tilde{S}} H^2(G_{L_{\mathfrak{p}}}(p), A)\right) \simeq \ker\left(H^2(G_{L,\tilde{S}}(p), A) \to \prod_{\mathfrak{p}\in\tilde{S}} H^2(G_{L_{\mathfrak{p}}}, A)\right).$$
  The isomorphism follows from Proposition 20 in [10, II.§5.6].
- $Ш^2(L_{\tilde{S}}(p)/K, A) := \ker\left(H^2(G_{L,\tilde{S}}(p) \rtimes \Gamma, A) \to \prod_{\mathfrak{p}\in S}(H^2(G_{K_{\mathfrak{p}}}, A)\right)$, for a finite cardinality $\mathbb{Z}_p[G_{K,S}]$-module A for which $(\#\Gamma, p) = 1$.
- $Ш^i_{all}(K, A) := \ker\left(H^i(G_K, A) \to \prod_{\text{all places}} H^i(G_{K_{\mathfrak{q}}}, A)\right)$.
- $Б_S(K, A) := \mathrm{coker}\left(\prod_{\mathfrak{q}\in S} H^1(G_{K_{\mathfrak{q}}}, A) \times \prod_{\mathfrak{q}\notin S} H^1_{nr}(G_{K_{\mathfrak{q}}}, A) \to H^1(G_K, A')^\vee\right)$, where the map is the dual of the restriction map, using local duality.
- $Б_{all}(K, A) := \mathrm{coker}\left(\prod_{\mathfrak{q}} H^1(G_{K_{\mathfrak{q}}}, A) \to H^1(G_K, A')^\vee\right)$. This group is dual to $Ш^1_{all}(K, A')$ [7, Lemma 8.7].
- $V_S(K, \mathbb{F}_p) := \{x \in K^\times \mid v_{\mathfrak{q}}(x) \equiv 0 \bmod p,\ \forall \mathfrak{q};\ x \in K_{\mathfrak{q}}^{\times p},\ \forall \mathfrak{q} \in S\}$. By [7, Proposition 8.3], $(V_S(K, \mathbb{F}_p)/K^{\times p})^\vee \simeq Б_S(K, \mathbb{F}_p)$.

2. Proof of Theorem 1

The running hypotheses and notes for this section are:

- p is any prime including 2.
- A is any finite cardinality $\mathbb{Z}_p[G_K]$-module with splitting field $L := K(A)$.
- We use Chebotarev's theorem repeatedly to choose our primes from a set of positive density. Of course this only allows us to choose Frobenius *conjugacy classes*, but as we are restricting to decomposition groups (which are defined only up to conjugacy) and taking

cohomology, we abuse notation and use the terminology of Frobenius elements. All primes chosen are degree 1 over K and unramified in L/K.

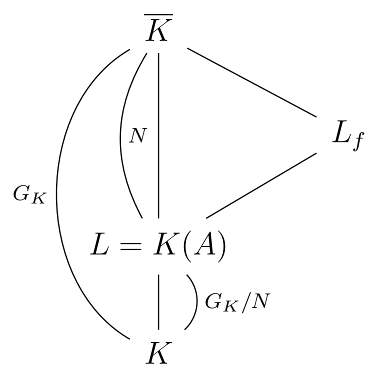
Before proving Theorem 1, we need some preliminary results.

Lemma 4. *Let $N \subset G_K$ be the maximal subgroup which acts trivially on A, so N fixes L and $A^N = A$. If $f \in H^1(G_K, A)$ does not inflate from $H^1(G_K/N, A)$, then $f \notin Ш^1_{all}(K, A)$.*

Proof. The assumption on and definition of N imply that in the inflation-restriction sequence

$$0 \to H^1(G_K/N, A) \to H^1(G_K, A) \to H^1(N, A)^{G_K/N},$$

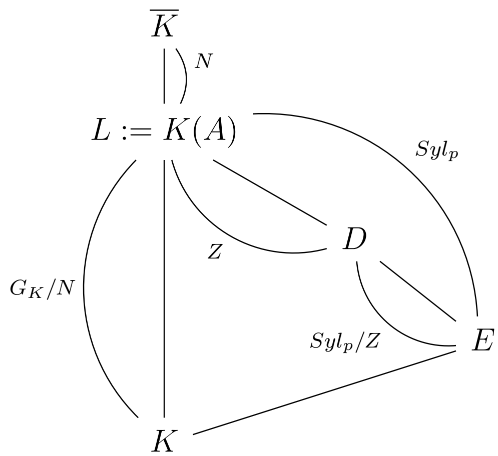
f restricts to a nonzero element of $H^1(N, A)^{G_K/N} = \mathrm{Hom}_{G_K/N}(N, A)$ and thus cuts out the nontrivial field extension L_f/L in the diagram below. Note L_f/K is a finite Galois extension. Let $\mathfrak{q}$ be any prime of K whose Frobenius in $\mathrm{Gal}(L_f/K)$ is a nontrivial element of $\mathrm{Gal}(L_f/L)$. Then $f|_{G_{K_\mathfrak{q}}} \neq 0$ so $f \notin Ш^1_{all}(K, A)$.



$\square$

Henceforth, we need only consider $f \in H^1(G_K, A)$ whose restriction to N is trivial, that is $0 \neq f \in H^1(G_K/N, A)$.

Recall we are assuming A is a finite cardinality $\mathbb{Z}_p[G_K]$-module and let Syl_p be a Sylow-p subgroup of G_K/N with fixed field E. As $\#A = p^m$ for some $m > 0$, the restriction map $H^1(G_K/N, A) \to H^1(Syl_p, A)$ is injective, so for $0 \neq f \in H^1(G_K/N, A) \subset H^1(G_K, A)$, our task is to find a $\mathfrak{q}_0$ of E such that the restriction of $f|_{Syl_p}$ to the decomposition group at $\mathfrak{q}_0$ in Syl_p is nontrivial. It then inflates nontrivially to $G_{E_{\mathfrak{q}_0}}$. For $\mathfrak{q}$ the prime of K below $\mathfrak{q}_0$ we would then have $f|_{G_{K_\mathfrak{q}}} \neq 0$, so, together with Lemma 4, we obtain $Ш^1_{all}(K, A) = 0$. As we will later choose a subgroup Z of order p in the center of Syl_p, we include it and its fixed field D in the diagram below.



The proof of Proposition 5 generalizes that of Lemma 1.2 of [11] in the $l = 5$ case.

Proposition 5. *For any number field K and any finite cardinality $\mathbb{Z}_p[G_K]$-module A with*

- *G_K/N having Sylow-p subgroup of order p^s,*
- *and $0 \neq f \in H^1(G_K/N, A)$,*

there are a positive density of degree one primes $\mathfrak{q}$ of K such that the inflation of f to G_K when restricted to $G_{K_\mathfrak{q}}$ is nonzero.

Proof. The proof is by induction on s.

Base case, $s = 1$, $\#Syl_p = p$: As $Syl_p = \langle \sigma \rangle$, we choose a prime $\mathfrak{q}_0$ of E whose Frobenius is σ. Then Syl_p is a quotient of the local Galois group $G_{E_{\mathfrak{q}_0}}$, so $f|_{G_{E_{\mathfrak{q}_0}}}$ inflates from the nonzero element $f|_{Syl_p}$ and is thus nonzero itself. Choosing $\mathfrak{q}$ of K beneath $\mathfrak{q}_0$, we have $f|_{G_{K_\mathfrak{q}}} \neq 0$. The base case holds.

Inductive step, $\#Syl_p = p^{s+1}$, $s > 0$: We assume the result has been established for all number fields and Galois modules where the Sylow-p subgroup of the Galois action has cardinality at most p^s. Since Syl_p is a nontrivial p-group, it has a nontrivial center. Let $Z \subset Syl_p$ be a subgroup of order p in the center of Syl_p. Recall $0 \neq f \in H^1(G_K/N, A)$ and denote its restriction to $H^1(Syl_p, A)$ by $\tilde{f}$. Then

$$0 \to H^1(Syl_p/Z, A^Z) \overset{Inf_Z}{\to} H^1(Syl_p, A) \overset{Res_Z}{\to} H^1(Z, A)^{Syl_p/Z}.$$

- Case I, $Res_Z(\tilde{f}) \neq 0$: Apply the base case to the $\mathbb{Z}/p\mathbb{Z}$-extension L/D corresponding to Z to find a degree one prime $\mathfrak{q}_0$ of D such that $Res_Z(\tilde{f})|_{G_{D_{\mathfrak{q}_0}}} \neq 0$. Let $\mathfrak{q}$ be the prime of K beneath $\mathfrak{q}_0$. As $Res_Z(\tilde{f}) = \tilde{f}|_{G_{D_{\mathfrak{q}_0}}}$ pulls back from $H^1(G_K/N, A)$ and $H^1(Syl_p, A)$, and then inflates to $f \in H^1(G_K, A)$, we see that $f|_{G_{K_\mathfrak{q}}} \neq 0$, so

$f \notin Ш^1_{all}(K, A)$.

$$\begin{tikzcd} G_{K_\mathfrak{q}} \arrow[r, hook] \arrow[ddrr] & G_K \arrow[r, two heads] & G_K/N \\ & & Syl_p \arrow[u, hook] \\ & & Z \arrow[u, hook] \end{tikzcd}$$

- Case II, $Res_Z(\tilde{f}) = 0$: Then $\tilde{f} = Inf_Z(f_0)$ for some nonzero $f_0 \in H^1(Syl_p/Z, A^Z)$. By the inductive hypothesis applied to Syl_p/Z, A^Z and D/E, there is a positive density of degree one primes $\mathfrak{q}_0$ of E such that $f_0|_{G_{\mathfrak{q}_0}} \neq 0$. The prime $\mathfrak{q}$ of K below $\mathfrak{q}_0$ is degree one and the set of such primes has positive density. We are assuming $\mathfrak{q}$ is unramified in L/K so σ is the Frobenius at $\mathfrak{q}_0$ in $\mathrm{Gal}(D/E)$ is also the Frobenius at $\mathfrak{q}$ in $\mathrm{Gal}(D/K)$. Again, $f|_{G_{K_\mathfrak{q}}}$ arises from inflating f to G_K and then restricting to $G_{K_\mathfrak{q}}$. In this case it is the same as going down the diagram: restricting, using that $Res_Z(\tilde{f}) = 0$ to pull back to Syl_p/Z along Inf_Z, and restricting down to $\langle\sigma\rangle$, and then inflating up and to the left to $G_{K_\mathfrak{q}}$.

$$\begin{tikzcd} G_{K_\mathfrak{q}} \arrow[r, hook] \arrow[ddddrr] & G_K \arrow[r, two heads] & G_K/N \\ & & Syl_p \arrow[u, hook] \arrow[d, two heads] & Z \arrow[l, hook'] \\ & & Syl_p/Z \\ & & \langle\sigma\rangle \arrow[u, hook] \end{tikzcd}$$

We have chosen $\mathfrak{q}_0$, $\mathfrak{q}$ and σ via the inductive hypothesis and our assumption that $Res_Z(\tilde{f}) = 0$ so that the image of $0 \neq f \in H^1(G_K/N, A)$ is nonzero at the penultimate step of the downward process. It is thus nonzero after the final diagonal inflation on a positive density of degree one primes $\mathfrak{q}$ of K.

This completes the induction. □

Corollary 6. *Both* $Ш^1_{all}(K, A)$ *and its dual* $Б_{all}(K, A')$ *are trivial.*

Proof. Let $0 \neq f \in H^1(G_K, A)$. If f does not inflate from $H^1(G_K/N, A)$, then Lemma 4 gives $f \notin Ш^1_{all}(K, A)$. On the other hand, if f inflates from $H^1(G_K/N, A)$, then by Proposition 5, $f \notin Ш^1_{all}(K, A)$. It follows that $Ш^1_{all}(K, A) = 0$, so its dual $Б_{all}(K, A') = 0$. □

We can now prove Theorem 1:

Proof. Below are some remarks to help translate between our notation and Liu's from [7].

- Our K plays the role of k in [7].
- The field Q at the end of this proof is Liu's field Q - it is *not* $\mathbb{Q}$.
- We have previously used N for the kernel of the Galois action on A, but here we follow Liu and take $N := \ker(Б_S(K, A) \twoheadrightarrow Б_{all}(K, A))$.

- $\beta : H^2(G_{K,S}, A) \to H^2(G_K, A)$ is the inflation map.

Towards the end of the proof of Proposition 8.5 of [7], there are two exact sequences

$$0 \longrightarrow \ker(\beta) \longrightarrow Ш^2_S(K,A) \xrightarrow{\beta} \beta(Ш^2_S(K,A)) \longrightarrow 0$$

$$0 \longrightarrow N \longrightarrow Б_S(K,A) \longrightarrow Б_{all}(K,A) \longrightarrow 0$$

An easy diagram chase in the proof of [7, Proposition 8.5] shows that $\ker(\beta) \hookrightarrow N$ and $\beta(Ш^2_S(K,A)) \hookrightarrow Б_{all}(K,A)$. By Corollary 6 (replacing A' by A) we know that $Б_{all}(K,A) = 0$, so $\beta(Ш^2_S(K,A)) = 0$, and the diagram above becomes

$$\begin{tikzcd} 0 \arrow[r] & \ker(\beta) \arrow[r] \arrow[d, hook] & Ш^2_S(K,A) \arrow[r] & 0 \arrow[r] & 0 \\ 0 \arrow[r] & N \arrow[r] & Б_S(K,A) \arrow[r] & 0 \arrow[r] & 0 \end{tikzcd}$$

which gives $Ш^2_S(K,A) \hookrightarrow Б_S(K,A)$, proving the first part of *(i)*. We have already proved $Б_{all}(K,A) = 0$, so $Ш^2_{all}(K,A) = 0$, completing *(i)*.

For *(ii)*, if K/Q is Galois, S is $\mathrm{Gal}(K/Q)$-stable and A is a $\mathrm{Gal}(K_S/Q)$-module, then Liu proves the injection $\ker(\beta) \hookrightarrow N$ is $\mathrm{Gal}(K/Q)$- equivariant. □

3. Some Lemmas

The running hypotheses and notes for this section are:

- p is a prime.
- A is a finite cardinality $\mathbb{Z}_p[G_K]$-module.
- T is a finite set (possibly empty) of tame primes of K.

Lemma 7 is used throughout the paper and in the examples in §6. Lemma 8 and Lemma 9 are crucial in the proofs of Proposition 2 and Theorem 3.

Lemma 7. *With the above notation,* $Ш^2_{\tilde{T},p}(L,\mathbb{F}_p) \hookrightarrow Ш^2_{\tilde{T}}(L,\mathbb{F}_p)$.

Proof. Let J be the kernel of $G_{L,\tilde{T}} \twoheadrightarrow G_{L,\tilde{T}}(p)$. Any $0 \neq \alpha \in H^1(J,\mathbb{F}_p)^{G_{L,\tilde{T}}(p)}$ gives rise to a $\mathbb{Z}/p\mathbb{Z}$-extension of $L_{\tilde{T}}(p)$ lying within $L_{\tilde{T}}$ and Galois over L. This contradicts the maximality of $L_{\tilde{T}}(p)$, so $H^1(J,\mathbb{F}_p)^{G_{L,\tilde{T}}(p)} = 0$. From the inflation-restriction sequence we have $H^2(G_{L,\tilde{T}}(p),\mathbb{F}_p) \hookrightarrow H^2(G_{L,\tilde{T}},\mathbb{F}_p)$. It is easy to see elements of $Ш^2_{\tilde{T},p}(L,\mathbb{F}_p)$ inflate to elements of $Ш^2_{\tilde{T}}(L,\mathbb{F}_p)$. □

Lemma 8. *Assume that T contains all the primes that ramify in L/K, so A is a $\mathbb{Z}_p[G_{K,T}]$-module. Assume, moreover, that $(\#\Gamma, p) = 1$. Then:*

(i) $H^i(G_{K,T}, A) \simeq H^i(G_{L,\tilde{T}}, A)^\Gamma$, *for all* $i \geq 1$.

(ii) Let $\mathfrak{p} \in T$. *Then* $H^i(G_{K_\mathfrak{p}}, A) \simeq \left(\prod_{\mathfrak{q}|\mathfrak{p}} H^i(G_{L_\mathfrak{q}}, A)\right)^\Gamma$, *for all* $i \geq 1$.

(iii) Let $\mathfrak{p} \in T$. *Then* $H^1_{nr}(G_{K_\mathfrak{p}}, A) \simeq \left(\prod_{\mathfrak{q}|\mathfrak{p}} H^1_{nr}(G_{L_\mathfrak{q}}, A)\right)^\Gamma$.

Proof. (i): As $(\#\Gamma, \#A) = 1$, we have for $m > 0$ and $n \geq 0$ that $H^m(\Gamma, H^n(G_{L,\tilde{T}}, A)) = 0$. Combining this with [8, Lemma 2.1.2], we can conclude that $H^i(G_{K,T}, A) \simeq H^i(G_{L,\tilde{T}}, A)^\Gamma$, for all $i \geq 1$.

(ii): Since L/K is Galois, the groups $\mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ are isomorphic for all $\mathfrak{q}|\mathfrak{p}$. Let $\Gamma_{\mathfrak{p}} = \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) \subset \Gamma$. By [8, Lemma 2.1.2] again, $H^i(G_{K_{\mathfrak{p}}}, A) \simeq (H^i(G_{L_{\mathfrak{q}}}, A))^{\Gamma_{\mathfrak{p}}}$ for $i \geq 1$. As Γ acts transitively on the $\#\Gamma/\Gamma_{\mathfrak{p}}$ primes $\mathfrak{q}$ above $\mathfrak{p}$ in $\tilde{T}$, the result follows.

(iii): Let $\tilde{\Gamma}_{\mathfrak{p}} \subset \Gamma_{\mathfrak{p}} = \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) \subset \Gamma$ be the inertia subgroup of $\Gamma = \mathrm{Gal}(L/K)$ at $\mathfrak{p}$ (note that this notation makes sense since L/K is Galois, so all the inertia subgroups are isomorphic). By part *(ii)* and [8, Lemma 2.1.2], we see that $H^1(G_{K_{\mathfrak{p}}}, A) \simeq H^1(G_{L_{\mathfrak{q}}}, A)^{\Gamma_{\mathfrak{p}}}$ and $H^1(\mathcal{T}_{\mathfrak{p}}(K), A) \simeq H^1(\mathcal{T}_{\mathfrak{q}}(L), A)^{\tilde{\Gamma}_{\mathfrak{p}}}$. Note that $H^1(\mathcal{T}_{\mathfrak{q}}(L), A)^{\Gamma_{\mathfrak{p}}} \subset H^1(\mathcal{T}_{\mathfrak{q}}(L), A)^{\tilde{\Gamma}_{\mathfrak{p}}}$, since $\tilde{\Gamma}_{\mathfrak{p}} \subset \Gamma_{\mathfrak{p}}$, so using the fact that there are $\#\Gamma/\Gamma_{\mathfrak{p}}$ primes $\mathfrak{q}$ above $\mathfrak{p}$ in $\tilde{T}$, we observe that

$$\left(\prod_{\mathfrak{q}|\mathfrak{p}} H^1(\mathcal{T}_{\mathfrak{q}}(L), A)\right)^{\Gamma} \simeq H^1(\mathcal{T}_{\mathfrak{q}}(L), A)^{\Gamma_{\mathfrak{p}}} \hookrightarrow H^1(\mathcal{T}_{\mathfrak{q}}(L), A)^{\tilde{\Gamma}_{\mathfrak{p}}} \simeq H^1(\mathcal{T}_{\mathfrak{p}}(K), A).$$

Combining this with the fact that $H^1(G_{K_{\mathfrak{p}}}, A) \simeq (\prod_{\mathfrak{q}|\mathfrak{p}} H^1(G_{L_{\mathfrak{q}}}, A))^{\Gamma}$, we obtain the following commutative diagram:

$$\begin{tikzcd}
H^1_{nr}(G_{K_{\mathfrak{p}}}, A) \arrow[d, hook] & \left(\prod_{\mathfrak{q}|\mathfrak{p}} H^1_{nr}(G_{L_{\mathfrak{q}}}, A)\right)^{\Gamma} \arrow[d, hook] \\
H^1(G_{K_{\mathfrak{p}}}, A) \arrow[r, "\simeq"] \arrow[d] & \left(\prod_{\mathfrak{q}|\mathfrak{p}} H^1(G_{L_{\mathfrak{q}}}, A)\right)^{\Gamma} \arrow[d] \\
H^1(\mathcal{T}_{\mathfrak{p}}(K), A) & \left(\prod_{\mathfrak{q}|\mathfrak{p}} H^1(\mathcal{T}_{\mathfrak{q}}(L), A)\right)^{\Gamma} \arrow[l, hook']
\end{tikzcd}$$

Note that the exactness of the right column follows from the left exactness of taking Γ-invariants. A routine diagram chase shows that $H^1_{nr}(G_{K_{\mathfrak{p}}}, A) \simeq (\prod_{\mathfrak{q}|\mathfrak{p}} H^1_{nr}(G_{L_{\mathfrak{q}}}, A))^{\Gamma}$. ☐

Lemma 9. *Let T be a finite set of tame primes of K, and let A be a finite cardinality $\mathbb{Z}_p[G_K]$-module.*

(i) The inclusions $Ш^2_{\tilde{T},p}(L, A) \hookrightarrow Ш^2_{\tilde{T}}(L, A) \hookrightarrow Б_{\tilde{T}}(L, A)$ are Γ-equivariant.

If, in addition, T contains all ramified primes of L/K (so A is a $\mathbb{Z}_p[G_{K,T}]$-module), and $(\#\Gamma, p) = 1$, then:

(ii) $Ш^2_{\tilde{T},p}(L, A)^{\Gamma} \simeq Ш^2(L_{\tilde{T}}(p)/K, A)$.
(iii) $Ш^2_{\tilde{T}}(L, A)^{\Gamma} \simeq Ш^2_{T}(K, A)$.
(iv) $Б_{\tilde{T}}(L, A)^{\Gamma} \simeq Б_T(K, A)$.

Proof. (i): By Lemma 7, we have an injection $Ш^2_{\tilde{T},p}(L, A) \hookrightarrow Ш^2_{\tilde{T}}(L, A)$ induced by the inclusion $H^2(G_{L,\tilde{T}}(p), A) \hookrightarrow H^2(G_{L,\tilde{T}}, A)$. As cohomology respects the conjugation by $\Gamma = \mathrm{Gal}(L/K)$, this inclusion is Γ-equivariant. The second map is Γ-equivariant by Theorem 1*(ii)*.

(ii): We use [8, Lemma 2.1.2] to observe that $H^2(G_{L,\tilde{T}}(p) \rtimes \Gamma, A) \simeq H^2(G_{L,\tilde{T}}(p), A)^\Gamma$. Now use Lemma 8*(ii)* to obtain:

$$\begin{aligned}
Ш^2(L_{\tilde{T}}(p)/K, A) &= \ker\left(H^2(G_{L,\tilde{T}}(p) \rtimes \Gamma, A) \to \prod_{\mathfrak{p}\in T} H^2(G_{K_\mathfrak{p}}, A)\right) \\
&\simeq \ker\left(H^2(G_{L,\tilde{T}}(p), A)^\Gamma \to \prod_{\mathfrak{p}\in T}\left(\prod_{\mathfrak{q}|\mathfrak{p}} H^2(G_{L_\mathfrak{q}}, A)\right)^\Gamma\right) \\
&\simeq \ker\left(H^2(G_{L,\tilde{T}}(p), A) \to \prod_{\mathfrak{q}\in\tilde{T}} H^2(G_{L_\mathfrak{q}}, A)\right)^\Gamma \\
&= Ш^2_{\tilde{T},p}(L, A)^\Gamma,
\end{aligned}$$

where the second isomorphism follows from left exactness of taking Γ-invariants.

(iii): We use Lemma 8 parts *(i)* and *(ii)*:

$$\begin{aligned}
Ш^2_T(K, A) &= \ker\left(H^2(G_{K,T}, A) \to \prod_{\mathfrak{p}\in T} H^2(G_{K_\mathfrak{p}}, A)\right) \\
&\simeq \ker\left(H^2(G_{L,\tilde{T}}, A)^\Gamma \to \prod_{\mathfrak{p}\in T}\left(\prod_{\mathfrak{q}|\mathfrak{p}} H^2(G_{L_\mathfrak{q}}, A)\right)^\Gamma\right) \\
&\simeq \ker\left(H^2(G_{L,\tilde{T}}, A) \to \prod_{\mathfrak{q}\in\tilde{T}} H^2(G_{L_\mathfrak{q}}, A)\right)^\Gamma \\
&= Ш^2_{\tilde{T}}(L, A)^\Gamma,
\end{aligned}$$

where the second isomorphism follows from left exactness of taking Γ-invariants.

(iv): We use Lemma 8, parts *(i)*, *(ii)*, and *(iii)*:

$$\begin{aligned}
Б_T(K, A) &= \operatorname{coker}\left(\prod_{\mathfrak{p}\in T} H^1(G_{K_\mathfrak{p}}, A) \times \prod_{\mathfrak{p}\notin T} H^1_{nr}(G_{K_\mathfrak{p}}, A) \to H^1(G_K, A')^\vee\right) \\
&\simeq \operatorname{coker}\left(\prod_{\mathfrak{p}\in T}\left(\prod_{\mathfrak{q}|\mathfrak{p}} H^1(G_{L_\mathfrak{q}}, A)\right)^\Gamma \times \prod_{\mathfrak{p}\notin T}\left(\prod_{\mathfrak{q}|\mathfrak{p}} H^1_{nr}(G_{L_\mathfrak{q}}, A)\right)^\Gamma \to (H^1(G_L, A')^\vee)^\Gamma\right) \\
&\simeq \operatorname{coker}\left(\prod_{\mathfrak{q}\in\tilde{T}} H^1(G_{L_\mathfrak{q}}, A) \times \prod_{\mathfrak{q}\notin\tilde{T}} H^1_{nr}(G_{L_\mathfrak{q}}, A) \to H^1(G_L, A')^\vee\right)^\Gamma \\
&= Б_{\tilde{T}}(L, A)^\Gamma.
\end{aligned}$$

The second isomorphism uses the fact that since $(\#\Gamma, p) = 1$, then taking Γ-invariants on finite cardinality $\mathbb{Z}_p[\Gamma]$-modules is exact. ∎

4. Proof of Main Results

The running hypotheses and notes for this section are:

- p is an odd prime. This is required to invoke the main result of [4]. See §5 for $p = 2$.
- A is a finite cardinality $\mathbb{F}_p[G_K]$-module. We need to restrict ourselves to this case because the main result of [4] is currently only known for $\mathbb{F}_p$.
- S is a finite set (possibly empty) of tame primes of K; $\tilde{S}$ is the set of places of L above S.

Since G_L acts trivially on the $\mathbb{F}_p[G_K]$-module A, we can now consider the groups $Ш^2_{\tilde{S},p}(L,\mathbb{F}_p)$, $Ш^2_{\tilde{S}}(L,\mathbb{F}_p)$ and $Б_{\tilde{S}}(L,\mathbb{F}_p)$ with the usual inclusion $Ш^2_{\tilde{S},p}(L,\mathbb{F}_p) \hookrightarrow Ш^2_{\tilde{S}}(L,\mathbb{F}_p) \hookrightarrow Б_{\tilde{S}}(L,\mathbb{F}_p)$. Use [4, Theorem A] to construct a tame set X' of primes of L such that:

$$\begin{tikzcd}
Ш^2_{\tilde{S},p}(L,\mathbb{F}_p) \arrow[r, hook] & Ш^2_{\tilde{S}}(L,\mathbb{F}_p) \arrow[r, hook] & Б_{\tilde{S}}(L,\mathbb{F}_p) \arrow[d, two heads, "\simeq"] \\
Ш^2_{\tilde{S}\cup X',p}(L,\mathbb{F}_p) \arrow[r, hook, "\simeq"] & Ш^2_{\tilde{S}\cup X'}(L,\mathbb{F}_p) \arrow[r, hook, "\simeq"] & Б_{\tilde{S}\cup X'}(L,\mathbb{F}_p).
\end{tikzcd}$$

Note that X' is a set of primes of L that is not necessarily Γ-stable. Let $\tilde{X}$ be the Γ-orbit of X'. By [4, Corollary 1.17], $Ш^2_{\tilde{S}\cup\tilde{X},p}(L,\mathbb{F}_p) \overset{\simeq}{\hookrightarrow} Ш^2_{\tilde{S}\cup\tilde{X}}(L,\mathbb{F}_p) \overset{\simeq}{\hookrightarrow} Б_{\tilde{S}\cup\tilde{X}}(L,\mathbb{F}_p)$. We claim that increasing the set X' to make it Γ-stable does not affect the group $Б_{\tilde{S}\cup X'}(L,\mathbb{F}_p)$:

Lemma 10. *With the above notation,* $Б_{\tilde{S}\cup X'}(L,\mathbb{F}_p) \simeq Б_{\tilde{S}\cup\tilde{X}}(L,\mathbb{F}_p)$.

Proof. We will prove that the duals are isomorphic: $V_{\tilde{S}\cup X'}(L,\mathbb{F}_p)/L^{\times p} \simeq V_{\tilde{S}\cup\tilde{X}}(L,\mathbb{F}_p)/L^{\times p}$. Firstly, since $\tilde{S}\cup X' \subset \tilde{S}\cup\tilde{X}$, we have $V_{\tilde{S}\cup\tilde{X}}(L,\mathbb{F}_p) \subset V_{\tilde{S}\cup X'}(L,\mathbb{F}_p)$, so we only need to show the other inclusion. To this end, let $x \in V_{\tilde{S}\cup X'}(L,\mathbb{F}_p)$, and let $\mathfrak{q}$ be a prime in X'. By the definition of $V_{\tilde{S}\cup X'}(L,\mathbb{F}_p)$, the primes above $\mathfrak{q}$ in $L(\zeta_p)$ split completely in $L(\zeta_p, \sqrt[p]{x})/L(\zeta_p)$. Take the Galois closure M of $L(\zeta_p, \sqrt[p]{x})$ over K. It follows that those primes also split completely in $M/L(\zeta_p)$, which implies that all their $\mathrm{Gal}(L/K)$-conjugates also split completely in $M/L(\zeta_p)$. Note that the set $\tilde{X}$ was formed by taking the $\mathrm{Gal}(L/K)$-conjugates of the elements of X', so we can conclude that $x \in V_{\tilde{S}\cup\tilde{X}}(L,\mathbb{F}_p)$, finishing the proof. $\square$

We have:

$$\begin{tikzcd}
Ш^2_{\tilde{S},p}(L,\mathbb{F}_p) \arrow[r, hook] & Ш^2_{\tilde{S}}(L,\mathbb{F}_p) \arrow[r, hook] & Б_{\tilde{S}}(L,\mathbb{F}_p) \arrow[d, two heads, "\simeq"] \\
Ш^2_{\tilde{S}\cup X',p}(L,\mathbb{F}_p) \arrow[r, hook, "\simeq"] & Ш^2_{\tilde{S}\cup X'}(L,\mathbb{F}_p) \arrow[r, hook, "\simeq"] & Б_{\tilde{S}\cup X'}(L,\mathbb{F}_p) \arrow[d, two heads, "\simeq"] \\
Ш^2_{\tilde{S}\cup\tilde{X},p}(L,\mathbb{F}_p) \arrow[r, hook, "\simeq"] & Ш^2_{\tilde{S}\cup\tilde{X}}(L,\mathbb{F}_p) \arrow[r, hook, "\simeq"] & Б_{\tilde{S}\cup\tilde{X}}(L,\mathbb{F}_p)
\end{tikzcd}$$

Proof of Proposition 2. Let X be the set of primes of K lying below $\tilde{X}$. Recall that G_L acts trivially on A and by Lemma 9*(i)* the following diagram is Γ-equivariant:

(4)
$$Ш^2_{\tilde{S},p}(L,A) \hookrightarrow Ш^2_{\tilde{S}}(L,A) \hookrightarrow Б_{\tilde{S}}(L,A) \overset{\simeq}{\twoheadrightarrow} Б_{\tilde{S}\cup\tilde{X}}(L,A) \overset{\simeq}{\hookleftarrow} Ш^2_{\tilde{S}\cup\tilde{X}}(L,A) \overset{\simeq}{\hookleftarrow} Ш^2_{\tilde{S}\cup\tilde{X},p}(L,A).$$

We can take Γ-invariants of (4) to obtain

$$\begin{tikzcd}
Ш^2_{\tilde{S},p}(L,A)^\Gamma \arrow[r, hook] & Ш^2_{\tilde{S}}(L,A)^\Gamma \arrow[r, hook] & Б_{\tilde{S}}(L,A)^\Gamma \arrow[d, two heads, "\simeq"] \\
Ш^2_{\tilde{S}\cup\tilde{X},p}(L,A)^\Gamma \arrow[r, hook, "\simeq"] & Ш^2_{\tilde{S}\cup\tilde{X}}(L,A)^\Gamma \arrow[r, hook, "\simeq"] & Б_{\tilde{S}\cup\tilde{X}}(L,A)^\Gamma
\end{tikzcd}$$

proving Proposition 2.

□

Proof of Theorem 3. To prove Theorem 3, recall that $(\#\Gamma, p) = 1$. Now, take Γ-invariants of (4) and use Lemma 9 to see

$$\begin{tikzcd}
Ш^2(L_{\tilde{S}}(p)/K,A) \arrow[r, hook] & Ш^2_{\tilde{S}}(K,A) \arrow[r, hook] & Б_S(K,A) \arrow[d, two heads, "\simeq"] \\
Ш^2(L_{\tilde{S}\cup\tilde{X}}(p)/K,A) \arrow[r, hook, "\simeq"] & Ш^2_{S\cup X}(K,A) \arrow[r, hook, "\simeq"] & Б_{S\cup X}(K,A)
\end{tikzcd}$$

□

The following result shows that once an isomorphism $Ш^2(L_{\tilde{S}}(p)/K,A) \overset{\simeq}{\hookrightarrow} Б_S(K,A)$ is established, increasing the set S by *any* set Y (tame or wild) preserves the isomorphism $Ш^2(L_{\tilde{S}\cup\tilde{Y}}(p)/K,A) \overset{\simeq}{\hookrightarrow} Б_{S\cup Y}(K,A)$.

Corollary 11. *If the injection* $Ш^2(L_{\tilde{S}}(p)/K,A) \hookrightarrow Ш^2_{\tilde{S}}(K,A) \hookrightarrow Б_S(K,A)$ *is an isomorphism, then for any set* Y *of primes of* K *we have*

$$Ш^2(L_{\tilde{S}\cup\tilde{Y}}(p)/K,A) \overset{\simeq}{\hookrightarrow} Ш^2_{S\cup Y}(K,A) \overset{\simeq}{\hookrightarrow} Б_{S\cup Y}(K,A).$$

Proof. This proof is inspired by the proofs of [4, Lemma 1.16] and [7, Lemma 8.4]. By the inflation-restriction exact sequence, one has:

$$H^1(\mathrm{Gal}(L_{\tilde{S}\cup\tilde{Y}}(p)/L_{\tilde{S}}(p)),A)^{G_{L,\tilde{S}}(p)\rtimes\Gamma} \to H^2(G_{L,\tilde{S}}(p)\rtimes\Gamma,A) \to H^2(G_{L,\tilde{S}\cup\tilde{Y}}(p)\rtimes\Gamma,A).$$

Note that the image of $H^1(\mathrm{Gal}(L_{\tilde{S}\cup\tilde{Y}}(p)/L_{\tilde{S}}(p)),A)^{G_{L,\tilde{S}}(p)\rtimes\Gamma}$ in $H^2(G_{L,\tilde{S}}(p)\rtimes\Gamma,A)$ lies in $Ш^2(L_{\tilde{S}}(p)/K,A)$, whose image lies in $Ш^2(L_{\tilde{S}\cup\tilde{Y}}(p)/K,A)$, so we have the following commutative diagram:

$$\begin{tikzcd}
H^1(\mathrm{Gal}(L_{\tilde{S}\cup\tilde{Y}}(p)/L_{\tilde{S}}(p)),A)^{G_{L,\tilde{S}}(p)\rtimes\Gamma} \arrow[r] & Ш^2(L_{\tilde{S}}(p)/K,A) \arrow[r] \arrow[d, hook] & Ш^2(L_{\tilde{S}\cup\tilde{Y}}(p)/K,A) \arrow[d, hook] \\
& Б_S(K,A) \arrow[r, two heads] & Б_{S\cup Y}(K,A)
\end{tikzcd}$$

We immediately obtain that if $Ш^2(L_{\tilde{S}}(p)/K,A) \hookrightarrow Б_S(K,A)$ is an isomorphism, then so is $Ш^2(L_{\tilde{S}\cup\tilde{Y}}(p)/K,A) \hookrightarrow Б_{S\cup Y}(K,A)$.

□

5. The case $p = 2$

As is usual, the case $p = 2$ presents extra technical difficulties. Because of this we relax slightly the running hypotheses and notes for this section:

- $p = 2$.
- A is a finite cardinality $\mathbb{F}_2[G_K]$-module with splitting field $L := K(A)$.
- $[L : K]$ is odd.
- S contains all ramified places of L/K.
- $\Gamma := \mathrm{Gal}(L/K)$.

The main result of this paper, Theorem 3, is a generalization of [4, Theorem A]. Both of these results hold only for odd primes p, so it is natural to ask what happens when $p = 2$. In [4], the case $p = 2$ involves an exceptional situation.

Definition 3. *For a field K and a tame set S of primes of K, the pair (K, S) is called exceptional if $p = 2$ and one simultaneously has:*

(a) $\zeta_4 \notin K$,
(b) $\mathcal{O}_K^\times \cap -4K^4 \neq \emptyset$,
(c) S contains no real place, and for every $\mathfrak{p} \in S$ one has $\zeta_4 \in K_\mathfrak{p}$.

It is shown in [4, Theorem B] that if S is a set of tame primes of K and the situation is exceptional, then there exist infinitely many finite tame sets X such that

$$d_2 Б_S(K, \mathbb{F}_2) - 1 \leq d_2 Ш^2_{S\cup X,2}(K, \mathbb{F}_2) = d_2 Ш^2_{S\cup X}(K, \mathbb{F}_2) = d_2 Б_{S\cup X}(K, \mathbb{F}_2) \leq d_2 Б_S(K, \mathbb{F}_2).$$

If the situation is not exceptional, then the conclusion of [4, Theorem A] holds in this case too.

In this section we prove a generalization of this result:

Theorem 12. *(i) If (K, S) is not exceptional, or if the trivial module $\mathbb{F}_2$ is not in the decomposition of A as a direct sum of irreducible $\mathbb{F}_2[\Gamma]$-modules, then there exist infinitely many tame sets X of K such that*

$$Ш^2(L_{\tilde{S}\cup\tilde{X}}(p)/K, A) \overset{\simeq}{\hookrightarrow} Ш^2_{S\cup X}(K, A) \overset{\simeq}{\hookrightarrow} Б_{S\cup X}(K, A) \overset{\simeq}{\twoheadleftarrow} Б_S(K, A).$$

(ii) Let $\mathbb{F}_2$ be the trivial $\mathbb{F}_2[\Gamma]$-module, so $\mathbb{F}_2 \otimes A \simeq A$ as $\mathbb{F}_2[\Gamma]$-modules. If (K, S) is exceptional, then there exist infinitely many finite tame sets X such that either

$$Ш^2(L_{\tilde{S}\cup\tilde{X}}(p)/K, A) \overset{\simeq}{\hookrightarrow} Ш^2_{S\cup X}(K, A) \overset{\simeq}{\hookrightarrow} Б_{S\cup X}(K, A) \overset{\simeq}{\twoheadleftarrow} Б_S(K, A)$$

or

$$(\mathbb{F}_2 \otimes A)^\Gamma \oplus Ш^2(L_{\tilde{S}\cup\tilde{X}}(p)/K, A) \overset{\simeq}{\hookrightarrow} A^\Gamma \oplus Ш^2_{S\cup X}(K, A) \overset{\simeq}{\hookrightarrow} A^\Gamma \oplus Б_{S\cup X}(K, A) \overset{\simeq}{\twoheadleftarrow} Б_S(K, A).$$

Proof. The proof follows the same steps as the proof of Theorem 3, with the caveat that we need to use [4, Theorem B] instead of [4, Theorem A] in the construction of the tame set X' of primes of L.

Firstly, we claim that the situation is not exceptional for (K, S) if and only if it is not exceptional for $(L, \tilde{S})$. To this end, let us prove the converse. Since $\Gamma = \mathrm{Gal}(L/K)$ has odd order, then $\zeta_4 \notin K$ (resp. $\zeta_4 \in K_\mathfrak{p}$ for $\mathfrak{p} \in S$) if and only if $\zeta_4 \notin L$ (resp. $\zeta_4 \in L_\mathfrak{q}$, for $\mathfrak{q}|\mathfrak{p}$). Similarly, S contains no real place if and only if $\tilde{S}$ contains no real place. Finally, if $\mathcal{O}_K^\times \cap 4K^4 \neq \emptyset$, then clearly $\mathcal{O}_L^\times \cap -4L^4 \neq \emptyset$. On the other hand, if $-4a^4 \in \mathcal{O}_L^\times \cap -4L^4$ (for $a \in L$), then taking norms, we obtain

$$N_{L/K}(-4a^4) = -4\left(2^k N_{L/K}(a)\right)^4 \in \mathcal{O}_K^\times \cap -4K^4,$$

where $\#\Gamma = 2k+1$.

We prove *(i)* and *(ii)* simultaneously: If the situation is not exceptional for (K,S), then it is not exceptional for $(L,\tilde{S})$. Then by [4, Theorem B], there exist infinitely many sets X' of primes of L such that

$$Ш^2_{\tilde{S}\cup X',2}(L,\mathbb{F}_2) \overset{\simeq}{\hookrightarrow} Ш^2_{\tilde{S}\cup X'}(L,\mathbb{F}_2) \overset{\simeq}{\hookrightarrow} Б_{\tilde{S}\cup X'}(L,\mathbb{F}_2) \overset{\simeq}{\twoheadleftarrow} Б_{\tilde{S}}(L,\mathbb{F}_2).$$

The proof of the first part of *(i)* then proceeds exactly as the proof of Theorem 3. We prove the second part of *(i)* at the end.

To finish the proof of *(ii)*, we can therefore assume that the situation is exceptional for (K,S) and also $(L,\tilde{S})$. Apply [4, Theorem B] to construct infinitely many sets X' such that

$$d_2Б_{\tilde{S}}(L,\mathbb{F}_2)-1 \le d_2Ш^2_{\tilde{S}\cup X',2}(L,\mathbb{F}_2) = d_2Ш^2_{\tilde{S}\cup X'}(L,\mathbb{F}_2) = d_2Б_{\tilde{S}\cup X'}(L,\mathbb{F}_2) \le d_2Б_{\tilde{S}}(L,\mathbb{F}_2).$$

Just as in the proof of Theorem 3, these sets X' are not Γ-stable, so let $\tilde{X}$ be the Γ-orbit of X'. It follows that

$$d_2Б_{\tilde{S}}(L,\mathbb{F}_2)-1 \le d_2Ш^2_{\tilde{S}\cup \tilde{X},2}(L,\mathbb{F}_2) = d_2Ш^2_{\tilde{S}\cup \tilde{X}}(L,\mathbb{F}_2) = d_2Б_{\tilde{S}\cup \tilde{X}}(L,\mathbb{F}_2) \le d_2Б_{\tilde{S}}(L,\mathbb{F}_2),$$

so either

$$Ш^2_{\tilde{S}\cup\tilde{X},2}(L,\mathbb{F}_2) \overset{\simeq}{\hookrightarrow} Ш^2_{\tilde{S}\cup\tilde{X}}(L,\mathbb{F}_2) \overset{\simeq}{\hookrightarrow} Б_{\tilde{S}\cup\tilde{X}}(L,\mathbb{F}_2) \twoheadleftarrow Б_{\tilde{S}}(L,\mathbb{F}_2)$$

or

$$\mathbb{F}_2 \oplus Ш^2_{\tilde{S}\cup\tilde{X},2}(L,\mathbb{F}_2) \overset{\simeq}{\hookrightarrow} \mathbb{F}_2 \oplus Ш^2_{\tilde{S}\cup\tilde{X}}(L,\mathbb{F}_2) \overset{\simeq}{\hookrightarrow} \mathbb{F}_2 \oplus Б_{\tilde{S}\cup\tilde{X}}(L,\mathbb{F}_2) \overset{\simeq}{\twoheadleftarrow} Б_{\tilde{S}}(L,\mathbb{F}_2).$$

As A is an $\mathbb{F}_2[\Gamma]$-module, we have $Б_{\tilde{S}}(L,A) \simeq Б_{\tilde{S}}(L,\mathbb{F}_2)\otimes A$ (and similarly for $Б_{\tilde{S}\cup\tilde{X}}(L,A)$, $Ш^2_{\tilde{S}\cup\tilde{X}}(L,A)$ and $Ш^2_{\tilde{S}\cup\tilde{X},p}(L,A)$). So either

$$Ш^2_{\tilde{S}\cup\tilde{X},2}(L,A) \overset{\simeq}{\hookrightarrow} Ш^2_{\tilde{S}\cup\tilde{X}}(L,A) \overset{\simeq}{\hookrightarrow} Б_{\tilde{S}\cup\tilde{X}}(L,A) \overset{\simeq}{\twoheadleftarrow} Б_{\tilde{S}}(L,A)$$

or

$$(\mathbb{F}_2\otimes A) \oplus Ш^2_{\tilde{S}\cup\tilde{X},2}(L,A) \overset{\simeq}{\hookrightarrow} A \oplus Ш^2_{\tilde{S}\cup\tilde{X}}(L,A) \overset{\simeq}{\hookrightarrow} A \oplus Б_{\tilde{S}\cup\tilde{X}}(L,A) \overset{\simeq}{\twoheadleftarrow} Б_{\tilde{S}}(L,A).$$

Taking Γ-invariants, and denoting by S and X, respectively, the sets of primes of K below $\tilde{S}$ and $\tilde{X}$, we obtain that either

$$Ш^2(L_{\tilde{S}\cup\tilde{X}}(p)/K,A) \overset{\simeq}{\hookrightarrow} Ш^2_{S\cup X}(K,A) \overset{\simeq}{\hookrightarrow} Б_{S\cup X}(K,A) \overset{\simeq}{\twoheadleftarrow} Б_S(K,A)$$

or

$$A^\Gamma \oplus Ш^2(L_{\tilde{S}\cup\tilde{X}}(p)/K,A) \overset{\simeq}{\hookrightarrow} A^\Gamma \oplus Ш^2_{S\cup X}(K,A) \overset{\simeq}{\hookrightarrow} A^\Gamma \oplus Б_{S\cup X}(K,A) \overset{\simeq}{\twoheadleftarrow} Б_S(K,A),$$

which proves part *(ii)*.

To prove the second part of *(i)*, observe that $\dim A^\Gamma$ is equal to the multiplicity of the trivial representation in the decomposition of A. Thus, if A has no trivial modules in its decomposition, then $\dim A^\Gamma = 0$, and the conclusion follows. □

6. Examples

In [4] several examples are given where the composite $Ш^2_{\emptyset,2}(K,\mathbb{F}_2) \hookrightarrow Ш^2_{\emptyset}(K,\mathbb{F}_2) \hookrightarrow$ $Б_{\emptyset}(K,\mathbb{F}_2)$ is not surjective, but explicit sets S were given such that

$$Ш^2_{\emptyset,2}(K,\mathbb{F}_2) \hookrightarrow Б_{\emptyset}(K,\mathbb{F}_2) \simeq Б_S(K,\mathbb{F}_2) \overset{\simeq}{\hookleftarrow} Ш^2_S(K,\mathbb{F}_2) \overset{\simeq}{\hookleftarrow} Ш^2_{S,2}(K,\mathbb{F}_2).$$

In this section we give two examples: one for odd p and one for $p = 2$. We used MAGMA, [1], for our computations, and all code was run unconditionally, that is we did not assume the GRH.

Example 1. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{5})$, $p = 3$ and let A be the group $\mathbb{Z}/3\mathbb{Z}$ with nontrivial action of $\Gamma := \mathrm{Gal}(L/K)$. Note L/K is unramified outside 5. Let $S = \{5\}$, $T = \{5, 107\}$ and $V = \{5, 107, 197\}$ be sets of primes of $\mathbb{Q}$ and $\tilde{S}$, $\tilde{T}$ and $\tilde{V}$ are the corresponding sets of primes of L. There is only one prime in L above each rational prime of V.

For $\tilde{X} \in \{\tilde{S}, \tilde{T}, \tilde{V}\}$ we will study $L_{\tilde{X}}(3)$, the maximal pro-3 extension of L unramified outside $\tilde{X}$. As $\tilde{X}$ is Γ-stable, $L_{\tilde{X}}(3)/K$ is Galois.

A simple inflation restriction argument, using that $(\#\Gamma, 3) = 1$, gives, for $X \in \{S, T, V\}$, that

$$H^1(G_{K,X}, A) \xrightarrow{\simeq} H^1(G_{L,\tilde{X}}, A)^{\Gamma} = \mathrm{Hom}_{\Gamma}(G_{L,\tilde{X}}, A).$$

The 3-parts of the ray class groups are given below:

The 3-parts of ray class groups for given tame conductors

	S	T	V	$\tilde{S}$	$\tilde{T}$	$\tilde{V}$
K	0	0	0	-	-	-
L	-	-	-	0	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/27\mathbb{Z}$

The first row follows as none of the primes of V are 1 mod 3, and the second comes from MAGMA computations. We want to determine the $\mathrm{Gal}(L/K)$-action on the ray class groups over L for $\tilde{T}$ and $\tilde{V}$. That the first row is trivial implies the action of $\mathrm{Gal}(L/K)$ on the 3-parts of the ray class groups over L is multiplication by -1 so

$$\mathrm{Hom}(G_{L,\tilde{X}}, A) = \mathrm{Hom}_{\Gamma}(G_{L,\tilde{X}}, A) = H^1(G_{L,\tilde{X}}, A)^{\Gamma} = H^1(G_{K,X}, A)$$

and thus

$$\dim H^1(G_{K,T}, A) = \dim H^1(G_{L,\tilde{T}}, A) = 1 \text{ and } \dim H^1(G_{K,V}, A) = \dim H^1(G_{L,\tilde{V}}, A) = 1.$$

As $G_{K,V} \twoheadrightarrow G_{K,T}$ (call the kernel J) and the inflation map $H^1(G_{K,T}, A) \longrightarrow H^1(G_{K,V}, A)$ is an isomorphism, the latter half of the 5-term inflation-restriction sequence gives the top row of:

$$\begin{tikzcd} 0 \arrow[r] & H^1(J,A)^{G_{K,T}} \arrow[r] & H^2(G_{K,T},A) \arrow[r] \arrow[d] & H^2(G_{K,V},A) \arrow[d] \\ & & \oplus_{\mathfrak{q}\in T} H^2(G_{K_{\mathfrak{q}}},A) \arrow[r, hook] & \oplus_{\mathfrak{q}\in V} H^2(G_{K_{\mathfrak{q}}},A) \end{tikzcd}$$

From the second row of the table we have the 3-part of the ray class group of conductor $\tilde{V}$ properly surjects onto that of conductor $\tilde{T}$, giving a nontrivial element $\alpha \in H^1(J,A)^{G_{K,T}}$. Chasing α to $\oplus_{\mathfrak{q}\in V} H^2(G_{K_{\mathfrak{q}}},A)$ its image is zero, so its image in $\oplus_{\mathfrak{q}\in T} H^2(G_{K_{\mathfrak{q}}},A)$ is zero as well. Thus the image of α in $H^2(G_{K,T},A)$ actually lies in $Ш^2_T(K,A)$ so this latter group is nonzero.

It remains to show

(i) $\dim Б_S(K,A) = \dim Б_T(K,A) = 1$,
(ii) $Ш^2(L_{\tilde{S}}(3)/K, A) = 0$.

Once these are established, we will have shown that $\dim Ш^2(L_{\tilde{X}}(3)/K,A)$ *increases* as we change X from S to T and reaches its maximum of $\dim Б_S(K,A) = 1$.

(i) By Lemma 9*(iv)*, $Б_S(K,A) \simeq Б_S(L,A)^\Gamma$ and $Б_T(K,A) \simeq Б_T(L,A)^\Gamma$. Over L, the $\mathbb{F}_3[G_{L,\tilde{T}}]$-module A has trivial action and is just $\mathbb{F}_3$. Using the relation between $\dim H^1(G_{L,S},\mathbb{F}_p)$ and $\dim Б_S(L,\mathbb{F}_p)$ given in (3) in the Introduction and the table above, we have $\dim Б_S(L,A) = \dim Б_T(L,A) = 1$. Let U_L be the unit group of L and $\mathrm{Cl}_L[p]$ be the p-torsion in the class group of L. From (1), we see

$$0 \to (\mathrm{Cl}_L[3])^\vee \to Б_\emptyset(L,\mathbb{F}_3) \to (U_L/U_L^3)^\vee \to 0.$$

Using our knowledge that the class group of L is trivial, its unit group has rank 1, Γ acts on U_L/U_L^3 by -1 and that Γ acts on A by -1 as well, taking Γ-invariants gives $\dim Б_S(K,A) = \dim Б_T(K,A) = 1$.

(ii) From the table we see there are no 3-extensions of L unramified outside S so $L_{\tilde{S}} = L$. It follows that $Ш^2(L_{\tilde{S}}(3)/K,A) \simeq Ш^2_{\tilde{S},3}(L,A)^\Gamma = 0$.

Example 2. We adapt Example 1 of [4]. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) = \mathbb{Q}(\cos\frac{2\pi}{7})$, noting that L is the splitting field of the polynomial $x^3 + x^2 - 2x - 1$. This is the totally real subfield of $\mathbb{Q}(\zeta_7)$. Clearly $\Gamma := \mathrm{Gal}(L/K) \simeq \mathbb{Z}/3\mathbb{Z}$ and one can check that L has trivial class group. We set $p = 2$ and $A = \mathbb{F}_2 \oplus \mathbb{F}_2$ with a nontrivial action of Γ.

Lemma 13. *$\dim_{\mathbb{F}_2}(A \otimes_{\mathbb{F}_2} A)^\Gamma = 2$.*

Proof. Extend scalars to $\mathbb{F}_4$ which contains all the eigenvalues of Γ acting on A. Let $\psi : \Gamma \to \mathbb{F}_4^\times$ be a nontrivial character. It is an exercise to check $A \otimes_{\mathbb{F}_2} \mathbb{F}_4 \simeq \mathbb{F}_4(\psi) \oplus \mathbb{F}_4(\psi^{-1})$ so

$$\dim_{\mathbb{F}_2}(A \otimes_{\mathbb{F}_2} A)^\Gamma = \dim_{\mathbb{F}_4}\left[\left(\mathbb{F}_4(\psi) \oplus \mathbb{F}_4(\psi^{-1})\right) \otimes_{\mathbb{F}_4} \left(\mathbb{F}_4(\psi) \oplus \mathbb{F}_4(\psi^{-1})\right)\right]^\Gamma = 2$$

$\square$

Consider the following sets of primes of K and L below. In the sets of primes of L, the subscript "1" indicates the first prime of L above the rational prime as chosen by MAGMA.

$$\text{Primes of } K : S = \{7\},\ T = \{7, 181, 293\},\ \text{and } V = \{7, 181, 293, 307, 349\}.$$

$$\text{Primes of } L : S' = \{7_1\},\ T' = \{7_1, 181_1, 293_1\},\ V' = \{7_1, 181_1, 293_1, 307_1, 349_1\}.$$

The first row of the table below gives the 2-primary part of ray class groups of L with given tame conductor $X' \in \{\emptyset, S', T', V'\}$, as computed by MAGMA. The second row follows from the first row and (3) of the Introduction.

	$\emptyset$	S'	T'	V'
$RCG_{L,X'}[2^\infty]$	0	0	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
$\dim_{\mathbb{F}_2} Б_{X'}(L,\mathbb{F}_2)$	3	2	2	0
$\dim_{\mathbb{F}_2} Ш^2_{X',2}(L,\mathbb{F}_2)$	0	0	2	0

We now explain the third row: From the first row we see $L_\emptyset(2) = L_{S'}(2) = L$ so $G_{L,\emptyset}(2) = G_{L,S'}(2)$ is trivial which gives the first two entries of the third row. The fourth entry follows from the injection $Ш^2_{V',2}(L,\mathbb{F}_2) \hookrightarrow Б_{V'}(L,\mathbb{F}_2) = 0$. For the third entry, using inflation-restriction for the map $1 \to N \to G_{L,V'}(2) \twoheadrightarrow G_{L,T'}(2) \to 1$, the last two entries of the first row of the table and the method of Example 1, we have

$$H^1(N,\mathbb{F}_2)^{G_{L,T'}(2)} \hookrightarrow Ш^2_{T',2}(L,\mathbb{F}_2).$$

As

$$\begin{aligned}2 &= \dim_{\mathbb{F}_2}\left(\ker\left(RCG_{L,V'}[2^\infty] \twoheadrightarrow RCG_{L,T'}[2^\infty]\right) \otimes_{\mathbb{Z}} \mathbb{F}_2\right)\\ &\leq \dim_{\mathbb{F}_2} H^1(N,\mathbb{F}_2)^{G_{L,T'}(2)} \leq \dim_{\mathbb{F}_2} Ш^2_{T',2}(L,\mathbb{F}_2) \leq \dim_{\mathbb{F}_2} Б_{T'}(L,\mathbb{F}_2) = 2,\end{aligned}$$

we are done.

Let $\tilde{X}$ be the $\mathrm{Gal}(L/K)$-orbit of $X' \in \{S', T', V'\}$. We now justify the data in the table below.

	$\emptyset$	$\tilde{S}$	$\tilde{T}$	$\tilde{V}$
$\dim_{\mathbb{F}_2} Б_{\tilde{X}}(L,A)^\Gamma$	2	2	2	0
$\dim_{\mathbb{F}_2} Ш^2_{\tilde{X},2}(L,A)^\Gamma$	0	0	2	0

Since the class number of L is 1, we see $Б_\emptyset(L,\mathbb{F}_2)$ is the dual of U_L/U_L^2 where U_L is the unit group of L, which has rank 2 as L is totally real. Recalling $\{\pm 1\} \subset U_L$, one easily sees $U_L/U_L^2 \simeq \mathbb{F}_2 \oplus A$ as $\mathbb{F}_2[\Gamma]$-modules so $Б_\emptyset(L,\mathbb{F}_2) \simeq \mathbb{F}_2 \oplus A$ as well. Then

$$Б_\emptyset(L,A) \simeq Б_\emptyset(L,\mathbb{F}_2) \otimes_{\mathbb{F}_2} A \simeq A \oplus (A \otimes_{\mathbb{F}_2} A).$$

Taking Γ-invariants and using Lemma 13 gives the first entry of the first row. As 7 is totally ramified in L/K, we see $S' = \tilde{S}$ so $\dim_{\mathbb{F}_2} Б_{\tilde{S}}(L,\mathbb{F}_2) = 2$. This group is a Γ-stable quotient of $\mathbb{F}_2 \oplus A$ and must therefore be A, so

$$Б_{\tilde{S}}(L,A) = Б_{\tilde{S}}(L,\mathbb{F}_2) \otimes_{\mathbb{F}_2} A \simeq A \otimes_{\mathbb{F}_2} A,$$

and Lemma 13 gives the second entry of the first row. We know from the first table that $\dim_{\mathbb{F}_2} Б_{T'}(L,\mathbb{F}_2) = 2$ and Lemma 10 gives $\dim_{\mathbb{F}_2} Б_{\tilde{T}}(L,\mathbb{F}_2) = 2$. As a Γ-module this is again A, so tensoring with A and taking Γ-invariants gives the third entry of the first row. The fourth entry follows as $Б_{V'}(L,\mathbb{F}_2) = Б_{\tilde{V}}(L,\mathbb{F}_2) = 0$ from the first table.

The first two entries of the second row follow from the fact that $L_\emptyset(2) = L_{\tilde{S}}(2) = L$ so $\mathrm{Gal}(L_\emptyset(2)/K) = \mathrm{Gal}(L_{\tilde{S}}(2)/K) = \mathrm{Gal}(L/K) = \Gamma$. The fourth entry follows as $Ш^2_{\tilde{V},2}(L,A) \hookrightarrow Б_{\tilde{V}}(L,A) = 0$. The third entry comes from the fact that the isomorphism $Ш^2_{T',2}(L,\mathbb{F}_2) \overset{\simeq}{\hookrightarrow} Б_{T'}(L,\mathbb{F}_2)$ of 2-dimensional vector spaces induces, using Lemma 10, the Γ-equivariant isomorphism $Ш^2_{\tilde{T},2}(L,\mathbb{F}_2) \overset{\simeq}{\hookrightarrow} Б_{\tilde{T}}(L,\mathbb{F}_2)$ of 2-dimensional vector spaces. Both of these $\mathbb{F}_2[\Gamma]$-modules are A, so again, tensoring with A and taking Γ-invariants completes this table.

From the second and third columns, we have increased $Ш^2_{\tilde{X},2}(L,A)^\Gamma \simeq Ш^2(L_{\tilde{X}}(2)/K,A)$ as we increase X in size from S to T from the trivial group to $Б_{\tilde{T}}(L,A)^\Gamma \simeq Б_{\tilde{S}}(L,A)^\Gamma$, its maximal possible size.

References

1. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478
2. Laurent Clozel, Michael Harris, and Richard Taylor, *Automorphy for some l-adic lifts of automorphic mod l Galois representations*, Publ. Math. Inst. Hautes Études Sci. (2008), no. 108, 1–181, With Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras. MR 2470687
3. Georges Gras, *Class field theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003, From theory to practice, Translated from the French manuscript by Henri Cohen. MR 1941965

4. Farshid Hajir, Christian Maire, and Ravi Ramakrishna, *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. MR 4359923
5. Helmut Koch, *Galois theory of p-extensions*, second ed., Springer Monogr. Math., Springer-Verlag, Berlin, 2002. MR 1930372
6. John Labute, *Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$*, J. Reine Angew. Math. **596** (2006), 155–182. MR 2254811
7. Yuan Liu, *Presentations of Galois groups of maximal extensions with restricted ramification*, Algebra Number Theory **19** (2025), no. 5, 835–881. MR 4896734
8. Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR 2392026
9. Alexander Schmidt, *über pro-p-fundamentalgruppen markierter arithmetischer kurven*, J. Reine Angew. Math. **640** (2010), 203–235. MR 2629694
10. Jean-Pierre Serre, *Cohomologie galoisienne*, fifth ed., Lecture Notes in Mathematics, vol. 5, Springer-Verlag, Berlin, 1994. MR 1324577
11. Richard Taylor, *On icosahedral Artin representations. II*, Amer. J. Math. **125** (2003), no. 3, 549–566. MR 1981033

Department of Mathematics, Cornell University, Ithaca, USA
Email address: `ai324@cornell.edu` `rkr5@cornell.edu`