Algebra & Number Theory

Volume 19
2025
No. 5

Presentations of Galois groups of maximal extensions with restricted ramification

Yuan Liu

msp

ALGEBRA AND NUMBER THEORY 19:5 (2025)
https://doi.org/10.2140/ant.2025.19.835

Presentations of Galois groups of maximal extensions with restricted ramification

Yuan Liu

Motivated by the work of Lubotzky, we use Galois cohomology to study the difference between the number of generators and the minimal number of relations in a presentation of $G_S(k)$, the Galois group of the maximal extension of a global field k that is unramified outside a finite set S of places, as k varies among a certain family of extensions of a fixed global field Q. We define a group $\text{Б}_S(k, A)$, for each finite simple $G_S(k)$-module A, to generalize the work of Koch and Shafarevich on the pro-ℓ completion of $G_S(k)$. We prove that $G_S(k)$ always admits a balanced presentation when it is finitely generated. In the setting of the nonabelian Cohen–Lenstra heuristics, we prove that the unramified Galois groups studied by the Liu–Wood–Zureick-Brown conjecture always admit a balanced presentation in the form of the random group in the conjecture.

1. Introduction

For a global field k and a set S of primes of k, we denote by $G_S(k)$ the Galois group of the maximal extension of k that is unramified outside S. Determining whether $G_\varnothing(k)$ is finitely generated and finitely presented is a long-existing open question. It is well known by class field theory that the abelianization of $G_\varnothing(k)$ is finitely presented and, in particular, is finite when k is a number field. Golod and Shafarevich [1964] constructed the first infinite ℓ-class tower group of a number field, where the ℓ-class tower group of k is the pro-ℓ completion of $G_\varnothing(k)$ for a prime number ℓ. The minimal numbers of generators and relations, which are called the generator rank and relator rank, in presentations of a pro-ℓ group is determined by its group cohomology with coefficient $\mathbb{F}_\ell$. Using this idea, Koch [2002] employed Galois cohomology to give an exact formula for the generator rank and estimate the relator rank of the pro-ℓ completion of $G_S(k)$ when S is finite and $\ell \neq \mathrm{char}(k)$; and in particular, in such cases, the pro-ℓ completion of $G_S(k)$ is always finitely presented.

Recently the development on the nonabelian Cohen–Lenstra program pushes us to study canonical quotients of $G_\varnothing(k)$ beyond the pro-ℓ completion. Let Γ be a finite group, Q the global field $\mathbb{Q}$ or $\mathbb{F}_q(t)$, and $\mu(Q)$ the group of roots of unity of Q. For a Galois extension k/Q with $\mathrm{Gal}(k/Q) \simeq \Gamma$, define $k^\#$ to be the maximal unramified extension of k, that is split completely at places of k over ∞ and of order relatively prime to $|\mu(Q)||\Gamma|$ and $\mathrm{char}(Q)$ (if nonzero). Wood, Zureick-Brown and the author [Liu et al. 2024] constructed random group models to make conjectures on the distributions for some

MSC2020: 11R29, 11R32, 11R34.
Keywords: presentation of Galois groups, class groups, nonabelian Cohen–Lenstra heuristics.

families of canonical quotients $\mathrm{Gal}(k^{\#}/k)$ of $G_{\varnothing}(k)$ as k varies among all Γ-extensions of Q split completely at ∞. Because $\mathrm{Gal}(k^{\#}/k)$ has (supernatural) order prime to $|\Gamma|$, a homomorphic split of $\mathrm{Gal}(k^{\#}/Q) \twoheadrightarrow \mathrm{Gal}(k/Q)$ defines by conjugation a continuous Γ action on $\mathrm{Gal}(k^{\#}/k)$; and this action is *admissible* (see Definition 4.1). The set of all isomorphism classes of all admissible profinite Γ-groups is closed under taking Γ-equivariant quotients, and we can construct *the free admissible profinite* Γ*-group* $\mathcal{F}_n(\Gamma)$ *on* n *generators* (see Section 4 for its definition). For a profinite Γ-group G and a finite set $\mathcal{C}$ of isomorphism classes of finite Γ-groups, let $G^{\mathcal{C}}$ denote the *pro-*$\mathcal{C}$ *completion* of G with respect to $\mathcal{C}$ (the definition of pro-$\mathcal{C}$ completions is given in Section 5 and it is different from the one that is commonly used). The work [Liu et al. 2024] uses quotients of $\mathcal{F}_n(\Gamma)$ as $n \to \infty$ to construct a random group model; this model together with the conjectures implies a surprising phenomenon of the structure of $\mathrm{Gal}(k^{\#}/k)$ that was not known before: for any finite set $\mathcal{C}$ of finite Γ-groups, the following occur with probability 1.

(1) The pro-$\mathcal{C}$ completion $\mathrm{Gal}(k^{\#}/k)^{\mathcal{C}}$ is a finite group.

(2) There exists a finite integer n_0 depending on $\mathcal{C}$, Γ and k, such that for every $n \geq n_0$, $\mathrm{Gal}(k^{\#}/k)^{\mathcal{C}}$ can be presented as the quotient of $\mathcal{F}_n(\Gamma)^{\mathcal{C}}$ by $[r^{-1}\gamma(r)]_{r\in X,\,\gamma\in\Gamma}$ for some subset X of $\mathcal{F}_n(\Gamma)^{\mathcal{C}}$ of cardinality $n+1$. Here, the symbol $[r^{-1}\gamma(r)]_{r\in X,\,\gamma\in\Gamma}$ denotes the Γ-closed normal subgroup of $\mathcal{F}_n(\Gamma)^{\mathcal{C}}$ generated by $r^{-1}\gamma(r)$ for all $r \in X$ and $\gamma \in \Gamma$.

The statement in (2) implies that the deficiency (i.e., the difference between the minimal number of generators and the minimal number of relations) of $\mathrm{Gal}(k^{\#}/k)^{\mathcal{C}}$ has an upper bound depending only on the order of Γ. In this paper, we prove that both (1) and (2) hold for all Γ-extensions k/Q split completely above ∞, which strongly supports that the random group model in [Liu et al. 2024] is the right object to study.

Theorem 1.1. *Let* Γ *be a nontrivial finite group and* Q *be either* $\mathbb{Q}$ *or* $\mathbb{F}_q(t)$ *with* q *relatively prime to* $|\Gamma|$. *Let* $\mathcal{C}$ *be a finite set of isomorphism classes of finite* Γ*-groups all of whose orders are prime to* $|\mu(Q)||\Gamma|$ *and* $\mathrm{char}(Q)$ (*if nonzero*). *Then for a Galois extension* k/Q *with Galois group* Γ *that is split completely over* ∞, *we have the following isomorphism of* Γ*-groups* (Γ *acts on the left-hand side via* $\Gamma \simeq \mathrm{Gal}(k/Q)$):

$$\mathrm{Gal}(k^{\#}/k)^{\mathcal{C}} \simeq \mathcal{F}_n(\Gamma)^{\mathcal{C}}/[r^{-1}\gamma(r)]_{r\in X,\gamma\in\Gamma} \tag{1-1}$$

for some positive integer n *and some set* X *consisting of* $n+1$ *elements of* $\mathcal{F}_n(\Gamma)^{\mathcal{C}}$.

Let $G_{\varnothing,\infty}(k)$ denote the Galois group of the maximal unramified extension of k that is completely split at every place above ∞, and note that with the assumptions in Theorem 1.1 one has $\mathrm{Gal}(k^{\#}/k)^{\mathcal{C}} = G_{\varnothing,\infty}(k)^{\mathcal{C}}$. The method we develop in this paper in fact works for $G_S(k)^{\mathcal{C}}$ for any finite set S of primes of k and any global base field Q, so it can be used to study the presentation of Galois groups with restricted ramification. In the case that k is a function field and $\Gamma = 1$ (so $k = Q$), building on the theorem of Lubotzky [2001], Shusterman [2022] showed that $G_{\varnothing}(k)$ admits a finite presentation in which the number of relations is exactly the same as the number of generators (such a presentation is called a balanced presentation). Note that, in [Shusterman 2022], the fact that $G_{\varnothing}(k)$ is finitely generated follows by Grothendieck's result on the geometric fundamental group of a smooth projective curve defined over a finite field, but when k is

a number field, whether $G_\varnothing(k)$ is finitely generated or not is unknown. We prove an analogous result regarding the number field case.

Theorem 1.2. *Let k be a number field and S a finite set of places of k. If $G_S(k)$ is topologically generated by n elements, then it admits a finite presentation on n generators and $[k:\mathbb{Q}]+n$ relations.*

We also apply our methods to the situations that are not considered in Theorem 1.1. We study the presentation of the pro-ℓ completion of $G_{\varnothing,\infty}(k)$ for a Galois Γ-extension k/Q in two exceptional cases:

(i) Q is a number field not containing the ℓ-th roots of unity and we do not make any assumptions on the ramification of ∞ in k (Section 11.1).

(ii) Q is a global field containing the ℓ-th roots of unity (Section 11.2).

When considering the ℓ-parts of class groups, it has been known for a long time that the Cohen–Lenstra heuristics need to be corrected in these two cases (see [Cohen and Martinet 1987; Malle 2010]). In each of these two cases, we use our method to compute an upper bound for the deficiency of $G_{\varnothing,\infty}(k)$ at the pro-ℓ level, and then show why the Liu–Wood–Zureick-Brown conjecture doesn't work in these two exceptional cases. This computation of deficiencies also provides insights of how the random group model should be modified in these two cases.

1.1. ***Method of the proof.*** The bulk of this paper is devoted to establishing the techniques for proving Theorem 1.1. Motivated by [Lubotzky 2001], we first translate the question to understanding the Galois cohomology groups. In Section 3, we construct the *free profinite Γ-group $F_n(\Gamma)$ on n generators*, and, for a finitely generated profinite Γ-group G, we study the minimal number of relations of a presentation defined by a Γ-equivariant surjection $\pi: F_n(\Gamma)\twoheadrightarrow G$. The minimal number of relations is closely related to the multiplicities of the finite irreducible $G\rtimes\Gamma$-modules appearing as quotients of $\ker(\pi)$ (Definition 3.1). In Lemma 3.2, we show that for a finite simple $\mathbb{F}_\ell[G\rtimes\Gamma]$-module A with $\ell\nmid|\Gamma|$, the multiplicity of A can be computed by a formula involving $\dim_{\mathbb{F}_\ell} H^2(G\rtimes\Gamma,A)-\dim_{\mathbb{F}_\ell} H^1(G\rtimes\Gamma,A)$. So when restricted to the category of profinite Γ-groups whose order is prime to $|\Gamma|$, by using these multiplicities, we obtain formulas for the minimal number of relations of the presentation $F_n'(\Gamma)\twoheadrightarrow G'$, where $F_n'(\Gamma)$ and G' are the maximal pro-prime-to-$|\Gamma|$ quotients of $F_n(\Gamma)$ and G respectively (Propositions 3.4 and 3.7). In particular, the formulas provide an upper bound for the minimal number of relations of this presentation using $\dim_{\mathbb{F}_\ell} H^2(G,A)^\Gamma-\dim_{\mathbb{F}_\ell} H^1(G,A)^\Gamma$, where Γ acts on the cohomology groups by conjugation. These upper bound formulas set up the strategy of the proof of Theorem 1.1. Building upon it, we explore the multiplicities of *admissible presentations* $\mathcal{F}_n(\Gamma)\twoheadrightarrow G$ in Section 4 and the multiplicities of *pro-$\mathcal{C}$ presentations* in Section 5, where we obtain formulas that will be directly applied to the proof of Theorem 1.1. Then in Section 6, we define *the height of a group* and show in Proposition 6.3 that there is an upper bound for the heights of pro-$\mathcal{C}$ groups (not necessarily finitely generated) when $\mathcal{C}$ is a finite set. Then Theorem 6.4 proves the finiteness of $G_S(k)^{\mathcal{C}}$ when S is a finite set of primes of k and $\mathcal{C}$ is a finite set of finite groups, which confirms the phenomenon (1).

Therefore, in order to prove Theorem 1.1, we need to deal with the Galois cohomology groups. In a more general setting, assuming that Q is an arbitrary global field, that k/Q is a Galois extension with $\mathrm{Gal}(k/Q) \simeq \Gamma$, and that S is a finite set of primes of k, we want to understand

$$\delta_{k/Q,S}(A) := \dim_{\mathbb{F}_\ell} H^2(G_S(k), A)^\Gamma - \dim_{\mathbb{F}_\ell} H^1(G_S(k), A)^\Gamma \tag{1-2}$$

for all prime integers ℓ relatively prime to $|\Gamma|$ and $\mathrm{char}(Q)$, and all finite simple $\mathbb{F}_\ell[\mathrm{Gal}(k_S/Q)]$-modules A. In (1-2), the set S needs to be k/Q-closed to ensure that k_S/Q is Galois (see the definition of the *k/Q-closed* sets in Section 2), and the Γ action on the cohomology groups is defined via the conjugation by $\mathrm{Gal}(k/Q)$. In Section 7, we prove a generalized version of the global Euler–Poincaré characteristic formula (Theorem 7.1), from which we can compute $\delta_{k/Q,S}$ when S is nonempty and contains the primes above ∞ and ℓ if Q is a number field. The proof basically follows the original proof of the global Euler–Poincaré characteristic formula, but taking the Γ actions into account creates many technical difficulties.

In the work of Koch, when dealing with the case that $A = \mathbb{F}_\ell$ and S does not satisfy the assumptions in Theorem 7.1, the abelian group $\text{Б}_S(k)$ plays an important role in the computation of $\dim_{\mathbb{F}_\ell} H^i(G_S(k), \mathbb{F}_\ell)$ for $i = 1, 2$, and is defined to be the Pontryagin dual of the Kummer group

$$V_S(k) = \ker\Big(k^\times/k^{\times\ell} \to \prod_{\mathfrak{p}\in S} k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times\ell} \times \prod_{\mathfrak{p}\notin S} k_\mathfrak{p}^\times/U_\mathfrak{p} k_\mathfrak{p}^{\times\ell}\Big),$$

where $k_\mathfrak{p}$ is the completion of k at $\mathfrak{p}$ and $U_\mathfrak{p}$ is the group of units of $k_\mathfrak{p}$. In Definition 8.1, we define a group $\text{Б}_S(k, A)$ in a cohomological way as

$$\mathrm{coker}\Big(\prod_{\mathfrak{p}\in S} H^1(k_\mathfrak{p}, A) \times \prod_{\mathfrak{p}\notin S} H^1_{nr}(k_\mathfrak{p}, A) \to H^1(k, A')^\vee\Big),$$

in order to generalize Koch's work to compute $\delta_{k/Q,S}(A)$ by replacing the trivial module $\mathbb{F}_\ell$ with an arbitrary finite simple module A. The definition of $\text{Б}_S(k, A)$ agrees with that of $\text{Б}_S(k)$ when $A = \mathbb{F}_\ell$ (Proposition 8.3). However, Koch's argument does not directly apply to $\text{Б}_S(k, A)$, because it uses the Hasse principle for $\mathbb{F}_\ell$ but the Hasse principle for arbitrary global fields and arbitrary Galois modules has not been proven (the Hasse principle holds for k and A if the Shafarevich group $Ш^1(k, A)$ is trivial). In Section 8, we modify Koch's work to overcome this obstacle, and show that most properties of $\text{Б}_S(k)$ also hold for $\text{Б}_S(k, A)$. In particular, one example, clearly showing that the failure of the Hasse principle makes a difference, is that there is a natural embedding $Ш^2_S(k, A) \hookrightarrow \text{Б}_S(k, A)$ for $A = \mathbb{F}_\ell$ but not for arbitrary A (Proposition 8.5 and Remark 8.6). In Section 9, we explicitly compute $\delta_{k/Q,S}(A)$ for all S by applying the results from Sections 7 and 8, and then we prove Theorem 1.2. In Section 10, we give the proof of Theorem 1.1. Finally, in Section 11, we apply our methods to the exceptional cases (i) and (ii) of Theorem 1.1. The proof of Theorem 1.1 uses results from Section 3 to Section 9; and the proof of Theorem 1.2 uses results from Sections 3, 7, 8, and 9.

1.2. ***Previous works.*** For an odd prime ℓ, the Cohen–Lenstra heuristics [1984] give predictions of the distribution of ℓ-primary parts of the class groups $\mathrm{Cl}(k)$ as k varies over quadratic number fields. Friedman and Washington [1989] formulated an analogous conjecture for global function fields. The probability

measure used for the conjectural distributions in the Cohen–Lenstra heuristics matches the one defined by the random abelian group

$$\lim_{n\to\infty} \mathbb{Z}_\ell^{\oplus n}/(n+u \text{ random relations}), \tag{1-3}$$

where the random relations are taken with respect to the Haar measure, and u is chosen to be 0 and 1 respectively when k varies among imaginary quadratic fields and real quadratic fields. Ellenberg and Venkatesh [2010] theoretically explained the random group model (1-3) and the value of u, by viewing $\mathrm{Cl}(k)$ as the cokernel of the map sending the S-units of k to the group of fractional ideals of k generated by S with S running along an ascending sequence of finite sets of primes of k. Boston, Bush and Hajir [Boston et al. 2017; 2021] extended the Cohen–Lenstra heuristics to a nonabelian setting considering the distribution of ℓ-class tower groups (for odd ℓ). In their work, the probability measure in the heuristics is defined by a random pro-ℓ group generalizing (1-3), and the value of u (which is the deficiency in this setting) is obtained by applying Koch's argument. Notably, the moment versions of the function field analogs of the Cohen–Lenstra heuristics and the Boston–Bush–Hajir heuristics are both proven; see [Ellenberg et al. 2016; Boston and Wood 2017]. In [Liu et al. 2024], we constructed the random Γ-group

$$\lim_{n\to\infty} \mathcal{F}_n(\Gamma)/[r^{-1}\gamma(r)]_{r\in X,\gamma\in\Gamma}, \tag{1-4}$$

where X is a set of $n+u$ random elements of $\mathcal{F}_n(\Gamma)$. We showed that the moment proven in the function field case matches the moment of the probability measure defined by (1-4) exactly when $u=1$. With this evidence, we conjectured that the random group (1-4) gives the distribution of $\mathrm{Gal}(k^{\#}/k)$ in both the function field case and the number field case. Theorem 1.1 explains the theoretical reason behind $u=1$ in the Liu–Wood–Zureick-Brown conjecture.

Regarding the exceptional case (i), Cohen and Martinet [1987] provided a modification for the case that $Q=\mathbb{Q}$ and k/Q varies among imaginary Γ-extensions whose decomposition subgroup at ∞ is a fixed (conjugacy class of) subgroup of Γ. Wang and Wood [2021] proved some results about the probability measures described in the Cohen–Martinet heuristics. From these works, one can see that the decomposition subgroup Γ_∞ at ∞ of $k/\mathbb{Q}$ crucially affects the probability measures. In Lemma 11.1, we explicitly compute the upper bounds of multiplicities in a pro-ℓ admissible Γ-presentation of $G_\varnothing(k)(\ell)$, which shows how the multiplicities are determined by Γ_∞. Then in Corollary 11.2 and Remark 11.3, we prove that, when $k/\mathbb{Q}$ is an imaginary quadratic field, $G_\varnothing(k)(\ell)$ can be achieved by a random group model which defines a probability measure agreeing with the Boston–Bush–Hajir heuristics.

For the exceptional case (ii), when the base field Q contains the ℓ-th roots of unity, we give upper bounds for multiplicities in Lemma 11.4 and Corollary 11.5, which suggests that the distributions of $G_{\varnothing,\infty}(k)(\ell)$ should be different between the function field case and the number field case (Remark 11.6(2)). This difference is not surprising, as Malle [2010] observed that his conjecture regarding the class groups of number fields does not easily match the result for function fields. So the upper bounds obtained in Corollary 11.5 support Malle's observation. The phenomenon related to the presence of the roots of unity has been numerically computed in [Malle 2008; 2010], and the random matrices in this setting and their

relation with function field counting has been studied in [Katz and Sarnak 1999; Achter 2006; 2008; Garton 2015; Adam and Malle 2015]. A correction for roots of unity, provided with empirical evidence, is presented in [Wood 2019].

1.3. ***Other applications and further questions.*** We expect that the techniques established in this paper will have many interesting and important applications. For example, the author applies the results in this paper to the following work. In [Liu 2022], the exceptional case (ii) is studied, where the moment conjecture in the number field case is inspired by the computation of $\delta_{k/Q,\varnothing}(A)$ similar to Section 11.2. In [Liu 2024], the abelian group $\text{Б}_S(k, A)$ is used to study the embedding problems with restricted ramification, which will be crucial for the forthcoming work on the generalized Cohen–Lenstra–Martinet–Gerth conjectures.

There are many further questions we would like to understand. First, the techniques in this paper work for any finite set S of primes. So we would like to ask whether the random group models (in the abelian, pro-ℓ and pro-$\mathcal{C}$ versions) can also be applied to predict the distributions of $G_S(k)$ as k/Q varies among certain families of Γ-extensions. Secondly, the group $\text{Б}_S(k, A)$, which is the generalization of $\text{Б}_S(k)$ that we construct in Section 8, has its own interest, because it could be applied to extend our knowledge of $G_S(k)$ from the pro-ℓ completion to the whole group, and moreover, it bounds the Shafarevich group via (see Proposition 8.5)

$$\#Ш^2_S(k, A) \le \#\text{Б}_S(k, A). \tag{1-5}$$

We emphasize here that understanding when $\#Ш^2_\varnothing(k, A) = \#\text{Б}_\varnothing(k, A)$ holds can help us determine whether our upper bound of multiplicities is sharp or not (see how the inequality (1-5) is used in the proof of Proposition 9.4). Last but not least, the techniques established in Sections 3, 4 and 5, which use group cohomology to understand the presentation of a Γ-group, are purely group theoretical and independent of the number theory background, so we hope that they could have other interesting applications.

In this paper, we only study the maximal prime-to-$|\Gamma|$ quotient of $G_{\varnothing,\infty}(k)$ for a Galois Γ-extension k/Q, and one can see that this "prime-to-$|\Gamma|$" requirement is necessary in almost every crucial step. We would like to ask if the ideas of this paper can be generalized to the $|\Gamma|$-part of $G_{\varnothing,\infty}(k)$ too.

2. Notation and preliminaries

2.1. ***Profinite groups and modules.*** In this paper, groups are always profinite groups and subgroups are always closed subgroups. For a group G, a *G-group* is a group with a continuous G action. If $x_1, \dots$ are elements of a G-group H, we write $[x_1, \dots]$ for the closed normal G-subgroup of H topologically generated by $x_1, \dots$. If H is a G-group, then we write $H \rtimes G$ for the semidirect product induced by the G action on H, and its multiplication rule is given by $(h_1, g_1)(h_2, g_2) = (h_1 g_1(h_2), g_1 g_2)$ for $h_1, h_2 \in H$ and $g_1, g_2 \in G$. *Morphisms of G-groups* are G-equivariant group homomorphisms. We write $\simeq_G$ to represent isomorphism of G-groups, write Hom_G to represent the set of G-equivariant homomorphisms, and define G-subgroup and G-quotient accordingly. For a G-group H, we say a set of elements *G-generates* H if H is the smallest closed G-subgroup containing this set. We say that H is an *irreducible* G-group if it is a nontrivial G-group and has no proper, nontrivial normal G-subgroups. For a positive integer n, a *pro-n'*

group is a group such that every finite quotient has order relatively prime to n. The *pro-n' completion of G* is the inverse limit of all pro-n' quotients of G. For a prime ℓ, we denote the pro-ℓ and the pro-ℓ' completions of G by $G(\ell)$ and $G(\ell')$ respectively.

For a group G and a commutative ring R, we denote by $R[G]$ the completed R-group ring of G. We use the following notation of G-modules:

$$\begin{aligned}\mathrm{Mod}(G) &= \text{ the category of isomorphism classes of finite } G\text{-modules},\\ \mathrm{Mod}(R[G]) &= \text{ the category of isomorphism classes of finite } R[G]\text{-modules},\\ \mathrm{Mod}_n(G) &= \text{ the category of isomorphism classes of finite } \mathbb{Z}/n\mathbb{Z}[G]\text{-modules}.\end{aligned}$$

For a prime integer ℓ and a finite $\mathbb{F}_\ell[G]$-module A, we define $h_G(A)$ to be the $\mathbb{F}_\ell$-dimension of $\mathrm{Hom}_G(A, A)$. We consider the *Grothendieck group* $K_0'(R[G])$, which is the abelian group generated by the set $\{[A] \mid A \in \mathrm{Mod}(R[G])\}$ and the relations

$$[A] - [B] + [C] = 0$$

arising from each exact sequence $0 \to A \to B \to C \to 0$ of modules in $\mathrm{Mod}(R[G])$. For $A, B \in \mathrm{Mod}(R[G])$, the tensor product $A \otimes_R B$ endowed with the diagonal action of G is an element of $\mathrm{Mod}(R[G])$. Then $K_0'(R[G])$ becomes a ring by linear extensions of the product $[A][B] = [A \otimes_R B]$. If H is a subgroup of G, then the action of taking induced modules Ind_G^H defines a map from $K_0'(R[H])$ to $K_0'(R[G])$, which we will also denote by Ind_G^H.

Let ℓ denote a prime integer. If H is a pro-ℓ' subgroup of G, then it follows by the Schur–Zassenhaus theorem that $H^1(H, A) = 0$ for any $A \in \mathrm{Mod}_\ell(G)$, and hence taking the H-invariants is an exact functor on $\mathrm{Mod}_\ell(G)$. Moreover, when G is a pro-ℓ' group, $\mathrm{Mod}_\ell(G)$ is the free abelian group generated by the isomorphism classes of finite simple $\mathbb{F}_\ell[G]$-modules, and elements $[A]$ and $[B]$ of $K_0'(\mathbb{F}_\ell[G])$ are equal if and only if A and B are isomorphic as $\mathbb{F}_\ell[G]$-modules. For an abelian group A, we let $A^\vee$ denote the Pontryagin dual of A.

2.2. ***Galois groups and Galois cohomology.*** For a field k, we write $\bar{k}$ for a fixed choice of separable closure of k, and write G_k for the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$. For a finite G_k-module A, we let $A' = \mathrm{Hom}(A, \bar{k}^\times)$. Let k/Q be a finite Galois extension of global fields. When v is a prime of the field Q, we define $S_v(k)$ to be the set of all primes of k lying above v. Note that the function field $\mathbb{F}_q(t)$ has an infinite place defined by the valuation $|\cdot|_\infty := q^{\deg(\cdot)}$, but this infinite place is nonarchimedean. We define $S_\infty(k)$ to be the set of all archimedean places of k, so it is the empty set if k is a function field. For a number field k, we let $S_\mathbb{R}(k)$ and $S_\mathbb{C}(k)$ denote the set of all real archimedean places and the set of all imaginary archimedean places of k respectively. We let $G_{\varnothing,\infty}(k)$ denote the Galois group of the maximal unramified extension of k that is split completely at every prime above ∞. So if k is a number field, then $G_{\varnothing,\infty}(k)$ is $G_\varnothing(k)$. If k is a function field, then $G_{\varnothing,\infty}(k)$ is the quotient of $G_\varnothing(k)$ by the decomposition subgroups of k at primes above ∞.

Let S be a set of places of k. We let k_S denote the maximal extension of k that is unramified outside S, and denote $\mathrm{Gal}(k_S/k)$ by $G_S(k)$ or just G_S when the choice of k is clear. The set S is called *k/Q-closed*

if $S_v(k)$ either is contained in S or intersects emptily with S for any prime v of Q. When S is k/Q-closed, it is not hard to check by Galois theory that k_S is Galois over Q, and hence each element of $\mathrm{Gal}(k/Q)$ defines an outer automorphism of $G_S(k)$. We let

$$\mathbb{N}(S) = \{n \in \mathbb{N} \mid n \in \mathcal{O}_{k,S}^{\times}\},$$

where $\mathcal{O}_{k,S}^{\times}$ is the ring of S-integers of k. Explicitly, if k is a number field, then $\mathbb{N}(S)$ consists of the natural numbers such that $\mathrm{ord}_{\mathfrak{p}}(n) = 0$ for all $\mathfrak{p} \notin S$; and if k is a function field, then $\mathbb{N}(S)$ is the set of all natural numbers prime to $\mathrm{char}(k)$. For a group G, we define

$$\mathrm{Mod}_S(G) = \text{the category of finite } G\text{-modules whose order is in } \mathbb{N}(S).$$

In particular, if Q is a function field, then $\mathrm{Mod}_S(G)$ consists of modules of order prime to $\mathrm{char}(Q)$.

Let k be a global field, and $\mathfrak{p}$ a prime of k. The completion of k at $\mathfrak{p}$ is denoted by $k_{\mathfrak{p}}$, and the absolute Galois group and its inertia subgroup of $k_{\mathfrak{p}}$ are denoted by $\mathcal{G}_{\mathfrak{p}}(k)$ and $\mathcal{T}_{\mathfrak{p}}(k)$ respectively. When the choice of k is clear, we denote $\mathcal{G}_{\mathfrak{p}}(k)$ and $\mathcal{T}_{\mathfrak{p}}(k)$ by $\mathcal{G}_{\mathfrak{p}}$ and $\mathcal{T}_{\mathfrak{p}}$. Let k/Q be a Galois extension of global fields. For a prime v of Q and a prime $\mathfrak{p} \in S_v(k)$, the Galois group of $k_{\mathfrak{p}}/Q_v$, denoted by $\mathrm{Gal}_{\mathfrak{p}}(k/Q)$, is the decomposition subgroup of $\mathrm{Gal}(k/Q)$ at $\mathfrak{p}$. The subgroups $\mathrm{Gal}_{\mathfrak{p}}(k/Q)$ are conjugate to each other in $\mathrm{Gal}(k/Q)$ for all $\mathfrak{p} \in S_v(k)$, so we write $\mathrm{Gal}_v(k/Q)$ for a chosen representative of this conjugacy class. For a group G and an $A \in \mathrm{Mod}(G)$, we write $H^i(G, A)$ and $\widehat{H}^i(G, A)$ for the group cohomology and the Tate cohomology respectively. For a field k, we define $H^i(k, A) := H^i(G_k, A)$ and $\widehat{H}^i(k, A) := \widehat{H}^i(G_k, A)$. Let A be a module in $\mathrm{Mod}(G_Q)$, where G_Q is the absolute Galois group of Q. The Galois group $\mathrm{Gal}(k/Q)$ acts on $H^i(k, A)$ by conjugation. The conjugation map commutes with inflations, restrictions, cup products and connecting homomorphisms in a long exact sequence, and hence it is naturally compatible with spectral sequences and duality theorems used in the paper. For a prime v of Q, we consider the $\mathrm{Gal}(k/Q)$ action on $\bigoplus_{\mathfrak{p}\in S_v(k)} H^i(k_{\mathfrak{p}}, A)$ defined by the action on $\bigoplus_{\mathfrak{p}\in S_v(k)} H^i(k_{\mathfrak{p}}, \mathrm{Res}^{G_Q}_{\mathcal{G}_v(Q)} A)$. In other words, $\mathrm{Gal}(k/Q)$ acts on $\bigoplus_{\mathfrak{p}\in S_v(k)} H^i(k_{\mathfrak{p}}, A)$ by the permutation action on $S_v(k)$ and by the $\mathrm{Gal}_{\mathfrak{p}}(k/Q)$-conjugation on each summand. We similarly define the $\mathrm{Gal}(k/Q)$ action on the product when each of the local summands is $H^i(\mathcal{T}_{\mathfrak{p}}, A)$ or the unramified cohomology group $H^i_{nr}(k_{\mathfrak{p}}, A) := \mathrm{im}\big(H^i(\mathcal{G}_{\mathfrak{p}}/\mathcal{T}_{\mathfrak{p}}, A^{\mathcal{T}_{\mathfrak{p}}}) \xrightarrow{\inf} H^i(\mathcal{G}_{\mathfrak{p}}, A)\big)$. In particular, the product of restriction maps for v

$$H^i(k, A) \to \bigoplus_{\mathfrak{p}\in S_v(k)} H^i(k_{\mathfrak{p}}, A)$$

respects the $\mathrm{Gal}(k/Q)$ actions. Moreover, one can check that

$$\bigoplus_{\mathfrak{p}\in S_v(k)} H^i(k_{\mathfrak{p}}, A) \cong \mathrm{Ind}^{\mathrm{Gal}_{\mathfrak{q}}(k/Q)}_{\mathrm{Gal}(k/Q)} H^i(k_{\mathfrak{q}}, A)$$

as $\mathrm{Gal}(k/Q)$-modules for any $\mathfrak{q} \in S_v(k)$. The same statement holds for the Tate cohomology groups. For a set S of places of k, we use the following notation for Shafarevich groups:

$$Ш^i(k, A) = \ker\Big(H^i(k, A) \to \prod_{\mathfrak{p} \text{ all places}} H^i(k_{\mathfrak{p}}, A)\Big), \quad Ш^i_S(k, A) = \ker\Big(H^i(G_S(k), A) \to \prod_{\mathfrak{p}\in S} H^i(k_{\mathfrak{p}}, A)\Big),$$

and we set

$$\prod_{\mathfrak{p}\in S}{}' H^1(k_\mathfrak{p}, A) := \left\{ (f_\mathfrak{p})_{\mathfrak{p}\in S} \in \prod_{\mathfrak{p}\in S} H^1(k_\mathfrak{p}, A) \;\middle|\; f_\mathfrak{p} \text{ is unramified for all but finitely many primes in } S \right\}.$$

2.3. ***List of notation appearing in multiple sections.***

- $F_n(\Gamma)$: free profinite Γ-group on n generators (defined in Section 3).
- $F_n'(\Gamma)$: pro-$|\Gamma|'$ completion of $F_n(\Gamma)$.
- $\mathcal{F}_n(\Gamma)$: free admissible Γ-group on n generators (defined in Section 4).
- $m(\omega, \Gamma, H, A)$: multiplicity of A associated to a Γ-equivariant surjection ω to the Γ-group H (defined in Definition 3.1).
- $m(n, \Gamma, G, A)$: multiplicity of A associated to a pro-$|\Gamma|'$ Γ-equivariant surjection $F_n'(\Gamma) \to G$ (defined in Definition 3.6).
- $m_{\mathrm{ad}}(n, \Gamma, G, A)$: multiplicity of A associated to an admissible Γ-presentation $\mathcal{F}_n(\Gamma) \to G$ (defined in Definition 4.3).
- $m_{\mathrm{ad}}^{\mathcal{C}}(n, \Gamma, G, A)$: multiplicity of A associated to a level-$\mathcal{C}$ admissible Γ-presentation $\mathcal{F}_n(\Gamma)^{\mathcal{C}} \to G^{\mathcal{C}}$ (defined in Proposition 5.4).
- $\chi_{k/Q,S}(A)$: Euler characteristic (defined in Section 7).
- $\delta_{k/Q,S}(A) := \dim_{\mathbb{F}_\ell} H^2(G_S(k), A)^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell} H^1(G_S(k), A)^{\mathrm{Gal}(k/Q)}$ (defined in Definition 9.1).
- $\epsilon_{k/Q,S}(A)$: an invariant associated to the Galois module A (defined Proposition 9.4)

3. Presentations of finitely generated profinite Γ-groups

Let $F_n(\Gamma)$ denote the *free profinite* Γ*-group on* n *generators* defined in [Liu et al. 2024]. Explicitly, $F_n(\Gamma)$ is the free profinite group on $\{x_{i,\gamma} \mid i = 1, \ldots, n \text{ and } \gamma \in \Gamma\}$ together with a Γ-action defined by

$$\sigma(x_{i,\gamma}) = x_{i,\sigma\gamma} \quad \text{for all } \gamma \in \Gamma.$$

If G is a profinite Γ-group that is Γ-generated by $g_1, \ldots, g_n$, then there is a unique surjective Γ-equivariant homomorphism $F_n(\Gamma) \to G$ defined by sending x_{i,Id_Γ} to g_i for each i. So the universal property holds for $F_n(\Gamma)$, and that is why $F_n(\Gamma)$ is the free pro-Γ-group on n generators (namely, the generators are $x_{1,\mathrm{Id}_\Gamma}, \ldots, x_{n,\mathrm{Id}_\Gamma}$).

When the choice of Γ is clear, we will denote $F_n(\Gamma)$ simply by F_n. Let G be a finitely generated Γ-group. Then when n is sufficiently large, there exists a short exact sequence

$$1 \to N \to F_n \rtimes \Gamma \xrightarrow{\pi} G \rtimes \Gamma \to 1, \tag{3-1}$$

where π is defined by mapping Γ identically to Γ, and $\{x_{i,1_\Gamma}\}_{i=1}^n$ to a set of n elements of G that generates G under the Γ action. Note that (3-1) can be viewed as a presentation of the group G that is compatible with Γ actions, and we will call it a Γ-*presentation of* G. The minimal number of relations in

the presentation (3-1), which is one of the main objects studied in this paper, is related to the multiplicities of the irreducible $F_n \rtimes \Gamma$-quotients of N. We define the multiplicity as follows, and one can find that this quantity is similarly defined in [Lubotzky 2001; Liu and Wood 2020; Liu et al. 2024].

Definition 3.1. Given a short exact sequence $1 \to \ker\omega \to E \xrightarrow{\omega} H \to 1$ of Γ-groups, we let M be the intersection of all maximal proper $E \rtimes \Gamma$-normal subgroups of $\ker\omega$, and let $\bar{N} = \ker\omega/M$ and $\bar{E} = E/M$. Then one can show that $\bar{N}$ is a direct product of finite irreducible $\bar{E} \rtimes \Gamma$-groups. For any finite irreducible $\bar{E} \rtimes \Gamma$-group A, we define $m(\omega, \Gamma, H, A)$ to be the multiplicity of A appearing in $\bar{N}$. When the multiplicity is infinite, we let $m(\omega, \Gamma, H, A) = \infty$. When ω refers to the surjection $E \rtimes \Gamma \to H \rtimes \Gamma$ induced by the Γ-equivariant surjection $E \to H$, we use the notation $m(\omega, \Gamma, H, A)$ instead of $m(\omega|_E, \Gamma, H, A)$ for the sake of convenience.

Consider the short exact sequence (3-1). Let M be the intersection of all maximal proper $F_n \rtimes \Gamma$-normal subgroups of N, and define $R = N/M$ and $F = F_n/M$ (i.e., R and F are $\bar{N}$ and $\bar{E}$ in Definition 3.1) for the short exact sequence (3-1). Then we obtain a short exact sequence

$$1 \to R \to F \rtimes \Gamma \to G \rtimes \Gamma \to 1.$$

Note that $F \rtimes \Gamma$ acts on R by conjugation, and maps the factor $A^{m(\pi,\Gamma,G,A)}$ of R to itself. When A is abelian, then the conjugation action on A by elements in R is trivial, so the $F \rtimes \Gamma$ action on A factors through $G \rtimes \Gamma$, and hence A is a finite simple $G \rtimes \Gamma$-module.

Lemma 3.2. *Using the notation above, if A is a finite simple $G \rtimes \Gamma$-module such that* $\gcd(|\Gamma|, |A|) = 1$, *then*

$$m(\pi, \Gamma, G, A) = \frac{n \dim_{\mathbb{F}_\ell} A - \xi(A) + \dim_{\mathbb{F}_\ell} H^2(G \rtimes \Gamma, A) - \dim_{\mathbb{F}_\ell} H^1(G \rtimes \Gamma, A)}{h_{G\rtimes\Gamma}(A)},$$

where ℓ is the exponent of A and $\xi(A) := \dim_{\mathbb{F}_\ell} A^\Gamma/A^{G\rtimes\Gamma}$.

Remark 3.3. When Γ is the trivial group, the lemma is [Lubotzky 2001, Lemma 5.3]

Proof. Applying the inflation-restriction exact sequence to (3-1), we obtain

$$0 \to H^1(G \rtimes \Gamma, A^N) \to H^1(F_n \rtimes \Gamma, A) \to H^1(N, A)^{G\rtimes\Gamma} \to H^2(G \rtimes \Gamma, A^N) \to H^2(F_n \rtimes \Gamma, A). \quad (3\text{-}2)$$

Also by $\gcd(|A|, |\Gamma|) = 1$, the Hochschild–Serre spectural sequence $E^{ij} = H^i(\Gamma, H^j(F_n, A)) \Longrightarrow H^{i+j}(F_n \rtimes \Gamma, A)$ degenerates, so we have that

$$H^2(F_n \rtimes \Gamma, A) \cong H^2(F_n, A)^\Gamma,$$

which is trivial because F_n is a free profinite group. Note that N acts trivially on A, so

$$H^1(N, A)^{G\rtimes\Gamma} = \mathrm{Hom}_{F_n\rtimes\Gamma}(N, A) = \mathrm{Hom}_{G\rtimes\Gamma}(A^{m(\pi,\Gamma,G,A)}, A)$$

because A is a simple $\mathbb{F}_\ell[G \rtimes \Gamma]$-module and $m(\pi, \Gamma, G, A)$ is the maximal integer such that $A^{m(\pi,\Gamma,G,A)}$ is an $F_n \rtimes \Gamma$-equivariant quotient of N. Then it follows that

$$\dim_{\mathbb{F}_\ell} H^1(N, A)^{G\rtimes\Gamma} = m(\pi, \Gamma, G, A) \dim_{\mathbb{F}_\ell} \mathrm{Hom}_{G\rtimes\Gamma}(A, A).$$

Thus, by (3-2) it suffices to show $\dim_{\mathbb{F}_\ell} H^1(F_n \rtimes \Gamma, A) = n \dim_{\mathbb{F}_\ell} A - \xi(A)$.

Elements of $H^1(F_n \rtimes \Gamma, A)$ correspond to the A-conjugacy classes of homomorphic sections of $A \rtimes (F_n \rtimes \Gamma) \xrightarrow{\rho} F_n \rtimes \Gamma$. We write every element of $F_n \rtimes \Gamma$ in the form of (x, γ) for $x \in F_n$ and $\gamma \in \Gamma$, and similarly, write elements of $A \rtimes (F_n \rtimes \Gamma)$ as $(a; x, \gamma)$ for $a \in A$, $x \in F_n$ and $\gamma \in \Gamma$. Then ρ maps $(a; x, \gamma)$ to (x, γ) for any a, x and γ. Note that a section of ρ is completely determined by the images of $(x_{i,1_\Gamma}, 1)$ and $(1, \gamma)$ for $i = 1, \dots, n$ and $\gamma \in \Gamma$, where $x_{i,1_\Gamma}$'s are the Γ-generators of F_n defined at the beginning of this section. Since $\gcd(|A|, |\Gamma|) = 1$, we have $H^1(\Gamma, A) = 0$ by the Schur–Zassenhaus theorem, which implies that the restrictions of all the sections of ρ to the subgroup Γ are conjugate to each other by A. So we only need to study the A-conjugacy classes of sections of ρ which map $(1, \gamma)$ to $(1; 1, \gamma)$ for any $\gamma \in \Gamma$, and such sections are totally determined by the images of $(x_{i,1_\Gamma}, 1)$ for $i = 1, \dots, n$. Let s_1 and s_2 be two distinct sections of this type. Under the multiplication rule of semidirect product, the conjugation of $(a; x, \gamma)$ by an element $\alpha \in A$ is

$$\begin{aligned}(\alpha^{-1}; 1, 1)(a; x, \gamma)(\alpha; 1, 1) &= (\alpha^{-1} \cdot a \cdot (x, \gamma)(\alpha); x, \gamma) \\ &= (\alpha^{-1} \cdot (x, \gamma)(\alpha); 1, 1)(a; x, \gamma),\end{aligned}$$

where the last equality is because A is abelian. Therefore, because of the assumption that $s_1(1, \gamma) = s_2(1, \gamma) = (1; 1, \gamma)$ for any $\gamma \in \Gamma$, we see that s_1 and s_2 are A-conjugate if and only if there exists $\alpha \in A^\Gamma / A^{G \rtimes \Gamma}$ such that $s_2(x, \gamma) = (\alpha^{-1} \cdot (x, \gamma)(\alpha); 1, 1) s_1(x, \gamma)$ for any x, γ. So

$$\begin{aligned}\#\{A\text{-conjugacy classes of sections of } \rho\} &= |A^\Gamma / A^{G \rtimes \Gamma}|^{-1} \prod_{i=1}^{n} \#\rho^{-1}(x_{i,1_\Gamma}, 1) \\ &= |A^\Gamma / A^{G \rtimes \Gamma}|^{-1} |A|^n,\end{aligned}$$

which proves that $\dim_{\mathbb{F}_\ell} H^1(F_n \rtimes \Gamma, A) = n \dim_{\mathbb{F}_\ell} A - \dim_{\mathbb{F}_\ell}(A^\Gamma / A^{G \rtimes \Gamma})$. □

In this paper, instead of the Γ-presentations in the form of (3-1), we want to study the presentations of pro-$|\Gamma|'$ completions of Γ-groups. Recall that the pro-$|\Gamma|'$ completion of a group G is the inverse limit of all finite quotients of G whose order is prime to $|\Gamma|$. We denote the pro-$|\Gamma|'$ completions of $F_n(\Gamma)$ and G by $F_n'(\Gamma)$ and G' respectively, and write F_n' for $F_n'(\Gamma)$ when the choice of Γ is clear. Then F_n' and G' naturally obtain Γ actions from F_n and G, and we have a short exact sequence

$$1 \to N' \to F_n' \rtimes \Gamma \xrightarrow{\pi'} G' \rtimes \Gamma \to 1, \tag{3-3}$$

induced by (3-1), which will be called *a* $|\Gamma|'$-Γ-*presentation of* G'.

Proposition 3.4. *Use the notation above. Let A be a finite simple $G' \rtimes \Gamma$-module, and denote the exponent of A by ℓ. If ℓ divides $|\Gamma|$, then $m(\pi', \Gamma, G', A) = 0$. Otherwise,*

$$m(\pi', \Gamma, G', A) = \frac{n \dim_{\mathbb{F}_\ell} A - \xi(A) + \dim_{\mathbb{F}_\ell} H^2(G' \rtimes \Gamma, A) - \dim_{\mathbb{F}_\ell} H^1(G' \rtimes \Gamma, A)}{h_{G' \rtimes \Gamma}(A)} \tag{3-4}$$

$$\leq \frac{n \dim_{\mathbb{F}_\ell} A - \xi(A) + \dim_{\mathbb{F}_\ell} H^2(G, A)^\Gamma - \dim_{\mathbb{F}_\ell} H^1(G, A)^\Gamma}{h_{G \rtimes \Gamma}(A)}. \tag{3-5}$$

where in (3-5) A is viewed as a $G \rtimes \Gamma$-module via the surjection $G \rtimes \Gamma \to G' \rtimes \Gamma$. Moreover, the equality in (3-5) holds if $H^2(\ker(G \to G'), \mathbb{F}_\ell) = 0$.

Remark 3.5. We see from (3-5) that the multiplicity $m(\pi', \Gamma, G', A)$ depends on n, Γ, G and A, but not on the choice of the quotient map π'.

Proof. It is clear that if ℓ divides $|\Gamma|$, then $m(\pi', \Gamma, G', A) = 0$. For the rest of the proof, assume $\ell \nmid |\Gamma|$. We consider the commutative diagram

$$\begin{array}{ccc} F_n \rtimes \Gamma & \xrightarrow{\pi} & G \rtimes \Gamma \\ \downarrow{\scriptstyle \rho} & \searrow^{\varpi} & \downarrow{\scriptstyle \rho_G} \\ F_n' \rtimes \Gamma & \xrightarrow{\pi'} & G' \rtimes \Gamma \end{array}$$

where each of the vertical maps is taking the $|\Gamma|'$-completion of the first component in semidirect product. If U is a maximal proper $F_n' \rtimes \Gamma$-normal subgroup of $\ker \pi'$ such that $\ker \pi'/U \simeq_{G' \rtimes \Gamma} A$, then its full preimage $\rho^{-1}(U)$ in $F_n \rtimes \Gamma$ is a maximal proper $F_n \rtimes \Gamma$-normal subgroup of $\ker \varpi$ with $\ker \varpi / \rho^{-1}(U) \simeq_{G' \rtimes \Gamma} A$. So by definition of multiplicities, we have that $m(\pi', \Gamma, G, A) \le m(\varpi, \Gamma, G, A)$. On the other hand, because $\gcd(|A|, |\Gamma|) = 1$, if V is a maximal proper $F_n \rtimes \Gamma$-normal subgroup of $\ker \varpi$ with $\ker \varpi / V \simeq_{G' \rtimes \Gamma} A$, then $F_n \rtimes \Gamma \twoheadrightarrow (F_n/V) \rtimes \Gamma$ factors through ρ, and hence we have shown that $m(\pi', \Gamma, G, A) = m(\varpi, \Gamma, G, A)$. Because ϖ defines a Γ-presentation of G', by Lemma 3.2 we obtain the equality (3-4).

Let W denote $\ker \rho_G = \ker(G \to G')$. Because G' is the pro-$|\Gamma|'$ completion of G and $\ell \nmid |\Gamma|$, the pro-ℓ completion of W is trivial. So as W acts trivially on A, we have that $H^1(W, A) = 0$. Then by considering the Hochschild–Serre spectral sequence associated to

$$1 \to W \to G \rtimes \Gamma \to G' \rtimes \Gamma \to 1,$$

we see that

$$H^1(G' \rtimes \Gamma, A) \cong H^1(G \rtimes \Gamma, A) \quad \text{and} \quad H^2(G' \rtimes \Gamma, A) \hookrightarrow H^2(G \rtimes \Gamma, A).$$

where the latter embedding is an isomorphism if $H^2(W, A) = 0$. Note that $H^2(W, A) = H^2(W, \mathbb{F}_\ell)^{\oplus \dim_{\mathbb{F}_\ell} A}$ because W acts trivially on A.

Finally, since $\gcd(|A|, |\Gamma|) = 1$, we have that $H^i(\Gamma, A) = 0$ for any $i \ge 1$, and hence by the Hochschild–Serre spectral sequence of

$$1 \to G \to G \rtimes \Gamma \to \Gamma \to 1$$

we have that $H^i(G \rtimes \Gamma, A) \cong H^i(G, A)^\Gamma$ for any i. Therefore, we have

$$\dim_{\mathbb{F}_\ell} H^1(G' \rtimes \Gamma, A) = \dim_{\mathbb{F}_\ell} H^1(G, A)^\Gamma \quad \text{and} \quad \dim_{\mathbb{F}_\ell} H^2(G' \rtimes \Gamma) \le \dim_{\mathbb{F}_\ell} H^2(G, A)^\Gamma,$$

where the equality holds if $H^2(W, \mathbb{F}_\ell) = 0$. □

By Remark 3.5, we can define the multiplicities as follows.

Definition 3.6. Let Γ be a finite group, G' a finitely generated pro-$|\Gamma|'$ Γ-group, and A a finite irreducible $G' \rtimes \Gamma$-group. Assume that there exists a Γ-equivariant surjection $\pi' : F_n' \to G'$. We define $m(n, \Gamma, G', A)$ to be $m(\pi', \Gamma, G', A)$.

When A is abelian, $m(n, \Gamma, G', A)$ is bounded above by (3-5). The next proposition proves that the minimal number of relators in the presentation π' is determined by $m(n, \Gamma, G', A)$ for all abelian A.

Proposition 3.7. *Consider the short exact sequence (3-3). The minimal number of generators of* $\ker\pi'$ *as a closed normal* Γ*-subgroup of* F_n' *is*

$$\sup_{\ell\nmid|\Gamma|}\ \sup_{\substack{A:\,\text{finite simple}\\ \mathbb{F}_\ell[G'\rtimes\Gamma]\text{-modules}}}\left\lceil\frac{\dim_{\mathbb{F}_\ell}H^2(G'\rtimes\Gamma,A)-\dim_{\mathbb{F}_\ell}H^1(G'\rtimes\Gamma,A)-\xi(A)}{\dim_{\mathbb{F}_\ell}A}\right\rceil+n. \tag{3-6}$$

Moreover, this minimal number is

$$\sup_{\ell\nmid|\Gamma|}\ \sup_{\substack{A:\,\text{finite simple}\\ \mathbb{F}_\ell[G'\rtimes\Gamma]\text{-modules}}}\left\lceil\frac{\dim_{\mathbb{F}_\ell}H^2(G,A)^\Gamma-\dim_{\mathbb{F}_\ell}H^1(G,A)^\Gamma-\xi(A)}{\dim_{\mathbb{F}_\ell}A}\right\rceil+n \tag{3-7}$$

and the equality holds if $H^2(\ker(G\to G'),\mathbb{F}_\ell)=0$.

Proof. We let M be the intersection of all maximal proper $F_n'\rtimes\Gamma$-normal subgroups of $\ker\pi'$, and let $R=\ker\pi'/M$ and $F=F_n'/M$. Then R is isomorphic to a direct product of finite irreducible $F\rtimes\Gamma$-groups whose orders are coprime to $|\Gamma|$. A set of elements of $\ker\pi'$ generates $\ker\pi'$ as a normal subgroup of $F_n'\rtimes\Gamma$ if and only if their images generate R as a normal subgroup of $F\rtimes\Gamma$.

For positive integer m, r and a finite irreducible $F\rtimes\Gamma$-group A, by [Liu and Wood 2020, Corollaries 5.9 and 5.10], one can compute the probability that the $F\rtimes\Gamma$-closed group generated by r random elements of A^m is the whole A^m. Note that this probability is positive if and only if A^m can be generated by r elements as a $F\rtimes\Gamma$-group. It follows that the minimal number of elements generating A^m as an $F\rtimes\Gamma$-group is

$$\begin{cases}1 & \text{if } A \text{ is nonabelian,}\\ \left\lceil\dfrac{mh_{F\rtimes\Gamma}(A)}{\dim_{\mathbb{F}_\ell}A}\right\rceil & \text{if } A \text{ is abelian, where } \ell \text{ is the exponent of } A.\end{cases}$$

Recall that if A is an abelian simple factor appearing in R, then the $F\rtimes\Gamma$ action on A factors through $G'\rtimes\Gamma$, since the conjugation action of R on A is trivial. Therefore, by the argument above and [Liu and Wood 2020, Corollary 5.7], the minimal number of generators of R as an $F\rtimes\Gamma$-group is

$$\sup_{\ell\nmid|\Gamma|}\ \sup_{\substack{A:\,\text{finite simple}\\ \mathbb{F}_\ell[G'\rtimes\Gamma]\text{-modules}}}\left\lceil\frac{m(n,\Gamma,G',A)h_{G'\rtimes\Gamma}(A)}{\dim_{\mathbb{F}_\ell}A}\right\rceil.$$

Then the proposition follows by Proposition 3.4 and the fact that $h_{G\rtimes\Gamma}(A)=h_{G'\rtimes\Gamma}(A)$. □

To end this section. we give a lemma that will be used later.

Lemma 3.8. *Let* E, F *and* G *be* Γ*-groups such that there exist* Γ*-equivariant surjections* $\alpha: E\to F$, $\beta: F\to G$ *and a* Γ*-equivariant homomorphic section* $s: F\to E$ *of* α. *Let* $\pi=\beta\circ\alpha$.

Let A *be a finite simple* $G\rtimes\Gamma$*-module. Then* $m(\pi,\Gamma,G,A)=m(\alpha,\Gamma,F,A)+m(\beta,\Gamma,G,A)$.

Proof. We first show $m(\pi, \Gamma, G, A) \geq m(\alpha, \Gamma, F, A) + m(\beta, \Gamma, G, A)$. By definition, the map β factors through an extension $\widetilde{G}$ of G satisfying the exact sequence

$$1 \to A^{m(\beta,\Gamma,G,A)} \to \widetilde{G} \to G \to 1.$$

Denote the composition of α and the quotient map $F \to \widetilde{G}$ by $\rho_1 : E \to \widetilde{G}$. Similarly, π factors through an extension $\widetilde{F}$ of F with kernel $A^{m(\alpha,\Gamma,F,A)}$. Because the section s identifies E as the semidirect product $\ker\alpha \rtimes s(F)$, we see that $\widetilde{F}$ has to be isomorphic to the semidirect product $A^{m(\alpha,\Gamma,F,A)} \rtimes F$. Note that the action of $F \rtimes \Gamma$ on A factors through $G \rtimes \Gamma$ (and similarly, factors through $\widetilde{G} \rtimes \Gamma$). So by composing with the surjection β, we have a Γ-equivariant quotient map

$$\rho_2 : E \to A^{m(\alpha,\Gamma,F,A)} \rtimes G.$$

Because ρ_2 factors through $A^{m(\alpha,\Gamma,F,A)} \rtimes \widetilde{G}$, we have the following fiber product diagram of Γ-equivariant quotients of E:

$$\begin{array}{ccc} A^{m(\alpha,\Gamma,F,A)} \rtimes \widetilde{G} = E/\ker\rho_1 \cap \ker\rho_2 & \twoheadrightarrow & \widetilde{G} = E/\ker\rho_1 \\ \downarrow & & \downarrow \\ A^{m(\alpha,\Gamma,F,A)} \rtimes G = E/\ker\rho_2 & \twoheadrightarrow & G = E/\ker\rho_1 \ker\rho_2 \end{array}$$

So the diagram shows $m(\pi, \Gamma, G, A) \geq m(\alpha, \Gamma, F, A) + m(\beta, \Gamma, G, A)$.

Let $\mathcal{S}$ be the set of all maximal proper $E \rtimes \Gamma$-normal subgroups U of $\ker\pi$ with $\ker\pi/U \simeq_{G\rtimes\Gamma} A$. To prove the equality in the lemma, it suffices to show that, for each $U \in \mathcal{S}$,

$$\ker\rho_1 \cap \ker\rho_2 = \ker\rho_1 \cap \ker\rho_2 \cap U, \tag{3-8}$$

because (3-8) together with the preceding paragraph implies that $\cap_{U\in\mathcal{S}} U = \ker\rho_1 \cap \ker\rho_2$.

Let $U \in \mathcal{S}$. If $\ker\alpha \subset U$, then $\alpha(U)$ is a maximal proper $F \rtimes \Gamma$-normal subgroup of $\ker\beta$ such that $\ker\beta/\alpha(U) \simeq_{G\rtimes\Gamma} A$, so $\ker\rho_1 \subset U$ and therefore (3-8) holds. Otherwise, $\ker\alpha \not\subset U$. Then $\ker\alpha/(\ker\alpha \cap U) \simeq_{G\rtimes\Gamma} (\ker\alpha \cdot U)/U = \ker\pi/U \simeq_{G\rtimes\Gamma} A$ and similarly $\ker\rho_1/(\ker\rho_1 \cap U) \simeq_{G\rtimes\Gamma} A$, and we have the quotient map

$$E/\ker\alpha \cap U \simeq A \rtimes F \to E/\ker\rho_1 \cap U \simeq A \rtimes \widetilde{G}.$$

The domain of this quotient map is a quotient of $\widetilde{F}$ and the target is a quotient of $E/(\ker\rho_1 \cap \ker\rho_2)$. Then we see that $\ker\rho_1 \cap U \supset \ker\rho_1 \cap \ker\rho_2$; thus we prove (3-8) in this case. □

4. Presentations of finitely generated profinite admissible Γ-groups

We first recall the definition of the admissible Γ-groups and the free admissible Γ-groups in [Liu et al. 2024].

Definition 4.1. A profinite Γ-group G is called *admissible* if it is Γ-generated by elements $\{g^{-1}\gamma(g) \mid g \in G, \gamma \in \Gamma\}$ and is of order prime to $|\Gamma|$.

Recall that for each positive integer n, we defined F_n' to be the pro-$|\Gamma|'$ completion of F_n. We set $y_{i,\gamma}$ to be the image in F_n' of the generators $x_{i,\gamma}$ of F_n, and therefore F_n' is the free pro-$|\Gamma|'$ group on $\{y_{i,\gamma} \mid i = 1, \dots, n \text{ and } \gamma \in \Gamma\}$, where $\sigma \in \Gamma$ acts on F_n' by $\sigma(y_{i,\gamma}) = y_{i,\sigma\gamma}$. We fix a generating set $\{\gamma_1, \dots, \gamma_d\}$ of the finite group Γ throughout the paper. We set $y_i := y_{i,\mathrm{id}_\Gamma}$ and define $\mathcal{F}_n(\Gamma)$ to be the closed Γ-subgroup of F_n' that is generated as a Γ-subgroup by the elements

$$\{y_i^{-1}\gamma_j(y_i) \mid i = 1, \dots, n \text{ and } j = 1, \dots, d\}.$$

We will denote $\mathcal{F}_n(\Gamma)$ by $\mathcal{F}_n$ when the choice of Γ is clear. The following is a list of properties of $\mathcal{F}_n(\Gamma)$ proven in [Liu et al. 2024, Lemma 3.1, Corollary 3.8 and Lemma 3.9]:

(1) $\mathcal{F}_n$ is an admissible Γ-group and it does not depend on the choice of the generating set $\{\gamma_1, \dots, \gamma_d\}$.

(2) There is a Γ-equivariant quotient map $\rho_n : F_n' \to \mathcal{F}_n$ such that the composition of the inclusion $\mathcal{F}_n \subset F_n'$ with ρ_n is the identity map on $\mathcal{F}_n$.

(3) Define a set function for any Γ-group G

$$Y : G \to G^d, \quad g \mapsto (g^{-1}\gamma_1(g), g^{-1}\gamma_2(g), \dots, g^{-1}\gamma_d(g)).$$

Then the function

$$Y(G)^n \to \mathrm{Hom}_\Gamma(\mathcal{F}_n, G)$$

taking $(Y(g_1), \dots, Y(g_n))$ to the restriction of the map $F_n' \to G$ with $y_i \mapsto g_i$ is a bijection.

Let G be an admissible Γ-group with a Γ-presentation defined by $F_n \rtimes \Gamma \xrightarrow{\pi} G \rtimes \Gamma$ such that the reduced map $F_n' \rtimes \Gamma \xrightarrow{\pi'} G \rtimes \Gamma$ satisfies that

$$G \text{ is } \Gamma\text{-generated by coordinates of } Y(y_i), \quad i = 1, \dots, n. \tag{4-1}$$

Under the condition (4-1), the restriction of π' to the admissible subgroup $\mathcal{F}_n$ of F_n' is surjective, so π' that factors through the quotient map $\rho_n : F_n' \to \mathcal{F}_n$ in (2) above. We let $\pi_{\mathrm{ad}} = \pi'|_{\mathcal{F}_n \rtimes \Gamma}$ and obtain a short exact sequence

$$1 \to N \to \mathcal{F}_n \rtimes \Gamma \xrightarrow{\pi_{\mathrm{ad}}} G \rtimes \Gamma \to 1, \tag{4-2}$$

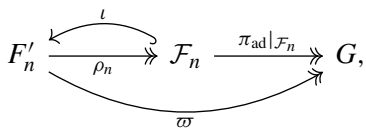
and we call it an *admissible Γ-presentation of G*.

Similarly to the previous section, we are interested in the multiplicities of the simple factors appearing as the quotients of N.

Lemma 4.2. *Let G be an admissible Γ-group with an admissible Γ-presentation (4-2) and A a finite simple $G \rtimes \Gamma$-module with* $\gcd(|A|, |\Gamma|) = 1$. *Then*

$$m(\pi_{\mathrm{ad}}, \Gamma, G, A) = m(n, \Gamma, G, A) - m(n, \Gamma, \mathcal{F}_n, A).$$

Proof. We let $\rho_n : F_n' \to \mathcal{F}_n$ be the quotient map described in property (2). Let ϖ be the composition of the following Γ-equivariant surjections and then ϖ defines a $|\Gamma|'$-Γ-presentation of G. Let $\iota : \mathcal{F}_n \to F_n'$ be the natural embedding. Then we have the diagram



The lemma follows by Lemma 3.8. □

Definition 4.3. Let G be a Γ-group with an admissible Γ-presentation (4-2). For a finite simple $G \rtimes \Gamma$-module A with $\gcd(|A|, |\Gamma|) = 1$, we define $m_{\mathrm{ad}}(n, \Gamma, G, A)$ to be $m(\pi_{\mathrm{ad}}, \Gamma, G, A)$. By Lemma 4.2, $m_{\mathrm{ad}}(n, \Gamma, G, A) = m(n, \Gamma, G, A) - m(n, \Gamma, \mathcal{F}_n, A)$ does not depend on the choice of π_{ad}.

Lemma 4.4. *Let A be a finite simple $\mathcal{F}_n \rtimes \Gamma$-module such that* $\gcd(|A|, |\Gamma|) = 1$. *Then*

$$\dim_{\mathbb{F}_\ell} H^1(\mathcal{F}_n \rtimes \Gamma, A) = n \dim_{\mathbb{F}_\ell}(A/A^\Gamma) - \xi(A).$$

Proof. We use the idea in the proof of Lemma 3.2. Elements of $H^1(\mathcal{F}_n \rtimes \Gamma, A)$ correspond to the A-conjugacy classes of homomorphic sections of $A \rtimes (\mathcal{F}_n \rtimes \Gamma) \xrightarrow{\rho} \mathcal{F}_n \rtimes \Gamma$. We use (g, γ) to represent elements of $\mathcal{F}_n \rtimes \Gamma$, and $(a; g, \gamma)$ to represent elements of $A \rtimes (\mathcal{F}_n \rtimes \Gamma)$. Again, by the Schur–Zassenhaus theorem, we only need to count the A-conjugacy classes of sections of ρ that maps $(1; 1, \gamma)$ to $(1, \gamma)$. In other words, we only need to study the A-conjugacy classes of Γ-equivariant sections of $A \rtimes \mathcal{F}_n \to \mathcal{F}_n$.

By property (3) of $\mathcal{F}_n$, there is a bijection $Y(A \rtimes \mathcal{F}_n)^n \to \mathrm{Hom}_\Gamma(\mathcal{F}_n, A \rtimes \mathcal{F}_n)$ taking $(Y(g_1), \dots, Y(g_n))$ to the restriction of the map $F_n' \to A \rtimes \mathcal{F}_n$ with $y_i \mapsto g_i$. For a Γ-equivariant section s of $A \rtimes \mathcal{F}_n \to \mathcal{F}_n$, the elements $s(y_i^{-1}\gamma_j(y_i))$ in $A \rtimes \mathcal{F}_n$ must map to $y_i^{-1}\gamma_j(y_i) \in \mathcal{F}_n$ for each $i = 1, \dots, n$ and $j = 1, \dots, d$. Therefore, the Γ-equivariant sections of $A \rtimes \mathcal{F}_n \to \mathcal{F}_n$ are in one-to-one correspondence with elements in $Y(A \rtimes \mathcal{F}_n)^n$ which map to $(Y(y_1), \dots, Y(y_n)) \in Y(\mathcal{F}_n)^n$ under the natural quotient map $A \rtimes \mathcal{F}_n \to \mathcal{F}_n$ on each component.

Let's consider $Y(y_i)$ and its preimages in $Y(A \rtimes \mathcal{F}_n)$. Note that there is also a natural embedding $Y(\mathcal{F}_n) \hookrightarrow Y(A \rtimes \mathcal{F}_n)$ defined by the obvious section of split extension $A \rtimes \mathcal{F}_n \twoheadrightarrow \mathcal{F}_n$. So we can fix a $g \in A \rtimes \mathcal{F}_n$ such that $Y(g)$ is the image of $Y(y_i)$ under this embedding, and then $Y(g)$ is a preimage of $Y(y_i)$ under φ, where φ is the quotient map $(A \rtimes \mathcal{F}_n)^d \to \mathcal{F}_n^d$. The self-bijection

$$(A \rtimes \mathcal{F}_n)^d \to (A \rtimes \mathcal{F}_n)^d, \quad (a_1, \dots, a_d) \mapsto (ga_1\gamma_1(g)^{-1}, \dots, ga_d\gamma_d(g)^{-1})$$

maps $Y(A \rtimes \mathcal{F}_n)$ to itself and $\varphi^{-1}(Y(y_i))$ to A^d. Thus,

$$\#Y(A \rtimes \mathcal{F}_n) \cap \varphi^{-1}(Y(y_i)) = \#Y(A \rtimes \mathcal{F}_n) \cap A^d = \#Y(A) = |A/A^\Gamma|,$$

where the second equality above uses [Liu et al. 2024, Lemma 3.4] and the last uses [Liu et al. 2024, Lemma 3.5]. So we've shown that there are $|A/A^\Gamma|$ elements in $Y(A \rtimes \mathcal{F}_n)$ mapping to $Y(y_i)$, and it follows that the number of Γ-equivariant sections of $A \rtimes \mathcal{F}_n \to \mathcal{F}_n$ is $|A/A^\Gamma|^n$.

Finally, recall that two sections s_1, s_2 of $A \rtimes (\mathcal{F}_n \rtimes \Gamma) \to \mathcal{F}_n \rtimes \Gamma$ are A-conjugate if and only if $s_1(g,\gamma) = (\alpha^{-1} \cdot (g,\gamma)(\alpha); 1, 1)s_1(g,\gamma)$ for some $\alpha \in A^\Gamma / A^{\mathcal{F}_n \rtimes \Gamma}$, by the computation in the proof of Lemma 3.2. Therefore,

$$\#H^1(\mathcal{F}_n \rtimes \Gamma, A) = \frac{|A/A^\Gamma|^n}{|A^\Gamma / A^{\mathcal{F}_n \rtimes \Gamma}|}. \qquad \square$$

Corollary 4.5. *Under the assumptions in Lemma 4.2, we have*

$$m_{\mathrm{ad}}(n, \Gamma, G, A) = m(n, \Gamma, G, A) - \frac{n \dim_{\mathbb{F}_\ell} A^\Gamma}{h_{G \rtimes \Gamma}(A)}.$$

Proof. By Proposition 3.4 and Lemma 4.4, we have

$$m(n, \Gamma, \mathcal{F}_n, A) = \frac{n \dim_{\mathbb{F}_\ell} A^\Gamma + \dim_{\mathbb{F}_\ell} H^2(\mathcal{F}_n, A)^\Gamma}{h_{G \rtimes \Gamma}(A)}.$$

Note that, forgetting the Γ-action, $\mathcal{F}_n$ is a projective profinite group, because by definition it is a closed subgroup of the free pro-$|\Gamma|'$ group F_n'. So $H^2(\mathcal{F}_n, A) = 0$, and then the corollary follows immediately by Lemma 4.2. $\square$

We point out in the next lemma that A^Γ is strictly smaller than A when $G \rtimes \Gamma$ acts nontrivially on A.

Lemma 4.6. *If G is an admissible Γ-group and A is a $G \rtimes \Gamma$-group such that Γ acts trivially on A, then $G \rtimes \Gamma$ acts trivially on A.*

Proof. The $G \rtimes \Gamma$ action on A induces a group homomorphism $G \rtimes \Gamma \to \mathrm{Aut}(A)$. So it suffices to show that Γ is not contained in any proper normal subgroup of $G \rtimes \Gamma$. Suppose M is a proper normal subgroup containing Γ. Then $B := (G \rtimes \Gamma)/M$ is a Γ-quotient of G and Γ acts trivially on B. However, G is admissible, so is generated by elements $g^{-1}\gamma(g)$ for $g \in G$ and $\gamma \in \Gamma$. Then the images of all $g^{-1}\gamma(g)$ in the Γ-quotient B generate B but each of these images is 1, and hence we obtain the contradiction. $\square$

5. Presentations of finitely generated profinite Γ-groups of level $\mathcal{C}$

Let $\mathcal{C}$ be a set of isomorphism classes of finite Γ-groups. The *variety of Γ-groups generated by $\mathcal{C}$* is defined to be the smallest set $\bar{\mathcal{C}}$ of isomorphism classes of Γ-groups containing $\mathcal{C}$ that is closed under taking finite direct products, Γ-quotients and Γ-subgroups. For a given Γ-group G, we define the pro-$\mathcal{C}$ completion of G to be

$$G^{\mathcal{C}} = \varprojlim_M G/M,$$

where the inverse limit runs over all closed normal Γ-subgroups M of G such that the Γ-group G/M is contained in $\bar{\mathcal{C}}$. We call a Γ-group G *level $\mathcal{C}$* if $G^{\mathcal{C}} = G$.

We want to emphasize that we do not require $\bar{\mathcal{C}}$ to be closed under taking group extensions, and it is different from most of works in the literature about completions of groups. For example, if we set $\mathcal{C}$ to be the set containing only the group $\mathbb{Z}/\ell\mathbb{Z}$ with the trivial Γ action, then $G^{\mathcal{C}}$ is the maximal quotient of G that is isomorphic to a direct product of $\mathbb{Z}/\ell\mathbb{Z}$ on which Γ acts trivially. If we want $G^{\mathcal{C}}$ to give us

the pro-ℓ completion of G, then we need to let $\mathcal{C}$ contain all the finite Γ-groups of order a power of ℓ. Similarly, $G^{\mathcal{C}}$ is the pro-$|\Gamma|'$ completion of G if $\mathcal{C}$ consists of all finite Γ-groups of order prime to $|\Gamma|$.

Lemma 5.1. *Let F, G be Γ-groups and $\omega : F \to G$ a Γ-equivariant surjection. Let $\mathcal{C}$ be a set of isomorphism classes of finite Γ-groups, and φ the pro-$\mathcal{C}$ completion map $F \to F^{\mathcal{C}}$. Then we have the following commutative diagram of Γ-equivariant surjections*:

$$\begin{array}{ccc} F & \xrightarrow{\omega} & G \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \alpha} \\ F^{\mathcal{C}} & \xrightarrow{\omega^{\mathcal{C}}} & G^{\mathcal{C}} \end{array}$$

where $\omega^{\mathcal{C}}$ is the quotient map by $\varphi(\ker\omega)$.

Proof. By the set-up, $\operatorname{im}\omega^{\mathcal{C}}$ naturally fits into the right-lower position of this diagram, so it's enough to show that $\operatorname{im}\omega^{\mathcal{C}} \simeq G^{\mathcal{C}}$. First, $\operatorname{im}\omega^{\mathcal{C}}$ is a quotient of G and a quotient of $F^{\mathcal{C}}$, so it is of level $\mathcal{C}$ and hence is a quotient of $G^{\mathcal{C}}$. On the other hand, we consider the natural pro-$\mathcal{C}$ completion map $\alpha : G \to G^{\mathcal{C}}$, and the composition $\alpha \circ \omega : F \to G^{\mathcal{C}}$. Because $G^{\mathcal{C}}$ is of level $\mathcal{C}$, it follows that $\ker(\alpha\circ\omega) \supseteq \ker\varphi$. Also, because $\ker\omega \subseteq \ker(\alpha\circ\omega)$, we have that $\operatorname{im}(\alpha\circ\omega) = G^{\mathcal{C}}$ is a quotient of $F/(\ker\omega\ker\varphi) = (F/\ker\varphi)/(\ker\omega/\ker\omega\cap\ker\varphi) = F^{\mathcal{C}}/\ker\omega^{\mathcal{C}} = \operatorname{im}\omega^{\mathcal{C}}$. So we have proved that $\operatorname{im}\omega^{\mathcal{C}} \simeq G^{\mathcal{C}}$. □

Definition 5.2. For any Γ-equivariant surjection $\omega : F \to G$, we define the pro-$\mathcal{C}$ completion of ω to be $\omega^{\mathcal{C}} : F^{\mathcal{C}} \to G^{\mathcal{C}}$ in Lemma 5.1.

Corollary 5.3. *Under the assumptions in Lemma 5.1, for any finite simple $G^{\mathcal{C}} \rtimes \Gamma$-module A, we have $m(\omega^{\mathcal{C}}, \Gamma, G^{\mathcal{C}}, A) \le m(\omega, \Gamma, G, A)$.*

Proof. By definition of $\omega^{\mathcal{C}}$, $\ker\omega^{\mathcal{C}}$ is the quotient of $\ker\omega$ by $\ker\omega\cap\ker\varphi$, and we denote this quotient map by $\phi : \ker\omega \to \ker\omega^{\mathcal{C}}$. If N is a maximal proper $F^{\mathcal{C}} \rtimes \Gamma$-normal subgroup of $\ker\omega^{\mathcal{C}}$ such that $\ker\omega^{\mathcal{C}}/N \simeq A$ as $G^{\mathcal{C}} \rtimes \Gamma$-modules, then its preimage $\phi^{-1}(N)$ in F is a maximal proper $F \rtimes \Gamma$-normal subgroup of $\ker\omega$ with $\ker\omega/\phi^{-1}(N) \simeq A$. The corollary follows by the definition of the multiplicity. □

Proposition 5.4. *Let G be an admissible Γ-group, $\mathcal{C}$ a set of isomorphism classes of finite Γ-groups and A a finite simple $G^{\mathcal{C}} \rtimes \Gamma$-module with $\gcd(|A|, |\Gamma|) = 1$. Then, for a fixed positive integer n such that there exists an admissible Γ-presentation of G as (4-2), the multiplicity $m(\pi_{\mathrm{ad}}^{\mathcal{C}}, \Gamma, G^{\mathcal{C}}, A)$ does not depend on the choice of π_{ad}, and so we denote $m(\pi_{\mathrm{ad}}^{\mathcal{C}}, \Gamma, G^{\mathcal{C}}, A)$ by $m_{\mathrm{ad}}^{\mathcal{C}}(n, \Gamma, G, A)$. Then*

$$m_{\mathrm{ad}}^{\mathcal{C}}(n, \Gamma, G, A) \le m_{\mathrm{ad}}(n, \Gamma, G, A).$$

Moreover, if $m_{\mathrm{ad}}(n, \Gamma, G, A)$ is finite, then the equality holds for sufficiently large $\mathcal{C}$.

Proof. Since A is finite, we can find a finite set $\mathcal{C}_1 \subset \mathcal{C}$ of isomorphism classes of finite Γ-groups such that the map $G^{\mathcal{C}} \rtimes \Gamma \to \mathrm{Aut}(A)$ induced by the $G^{\mathcal{C}} \rtimes \Gamma$ action on A factors through $G^{\mathcal{C}_1} \rtimes \Gamma$, and hence A is a simple $G^{\mathcal{C}_1} \rtimes \Gamma$-module. Let $\mathcal{C}_1 \subset \mathcal{C}_2 \subset \cdots$ be an ascending sequence of finite sets of isomorphism classes

of finite Γ-groups with $\cup \mathcal{C}_i = \mathcal{C}$. For each $i \le j$, we have that $m(\pi_{\mathrm{ad}}^{\mathcal{C}_i}, \Gamma, G^{\mathcal{C}_i}, A) \le m(\pi_{\mathrm{ad}}^{\mathcal{C}_j}, \Gamma, G^{\mathcal{C}_j}, A) \le m(\pi_{\mathrm{ad}}^{\mathcal{C}}, \Gamma, G^{\mathcal{C}}, A)$ by Corollary 5.3, and hence

$$m(\pi_{\mathrm{ad}}^{\mathcal{C}}, \Gamma, G^{\mathcal{C}}, A) = \lim_{i \to \infty} m(\pi_{\mathrm{ad}}^{\mathcal{C}_i}, \Gamma, G^{\mathcal{C}_i}, A).$$

Since $\mathcal{C}_i$ is a finite set of Γ-groups, [Liu et al. 2024, Remark 4.9] shows that the multiplicity $m(\pi_{\mathrm{ad}}^{\mathcal{C}_i}, \Gamma, G^{\mathcal{C}_i}, A)$ does not depend on the choice of π_{ad}. So we obtained that $m(\pi_{\mathrm{ad}}^{\mathcal{C}}, \Gamma, G^{\mathcal{C}}, A)$ also does not depend on the choice of π_{ad}. The inequality in the proposition follows by $m(\pi_{\mathrm{ad}}^{\mathcal{C}}, \Gamma, G^{\mathcal{C}}, A) \le m(\pi_{\mathrm{ad}}, \Gamma, G, A)$.

The last statement in the proposition then automatically follows because

$$m_{\mathrm{ad}}(n, \Gamma, G, A) = \sup_{\substack{\mathcal{D}\text{: finite set} \\ \text{of } \Gamma\text{-groups}}} m_{\mathrm{ad}}^{\mathcal{D}}(n, \Gamma, G, A). \qquad \square$$

6. The heights of pro-$\mathcal{C}$ groups

Definition 6.1. For a finite group H, we define $\mathfrak{h}(H)$ to be the smallest integer n such that there exists a length-n sequence of normal subgroups of H,

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = H,$$

where H_{i+1}/H_i is isomorphic to a direct product of minimal normal subgroups of H/H_i. We define the height of H to be

$$\hat{\mathfrak{h}}(H) = \max\{\mathfrak{h}(U) \mid U \text{ is a subquotient of } H\}.$$

For a profinite group H, the height is defined as

$$\hat{\mathfrak{h}}(H) = \sup_{\substack{U\text{: finite} \\ \text{quotient of } H}} \hat{\mathfrak{h}}(U).$$

Lemma 6.2. *Let G and H be two finite groups. Then $\hat{\mathfrak{h}}(G \times H) = \max\{\hat{\mathfrak{h}}(G), \hat{\mathfrak{h}}(H)\}$.*

Proof. Note that a subquotient of G or H is a subquotient of $G \times H$, so $\hat{\mathfrak{h}}(G \times H) \ge \max\{\hat{\mathfrak{h}}(G), \hat{\mathfrak{h}}(H)\}$. It suffices to show that $\mathfrak{h}(U) \le \max\{\hat{\mathfrak{h}}(G), \hat{\mathfrak{h}}(H)\}$ for any subquotient U of $G \times H$. Each subquotient U of $G \times H$ is a quotient of a subgroup V of $G \times H$. Then because a sequence of normal subgroups of V induces a sequence of normal subgroups of U, and a minimal normal subgroup is mapped to a product of minimal normal subgroups or the trivial subgroup under any quotient map. We see that $\mathfrak{h}(U) \le \mathfrak{h}(V)$, so we only need to show that $\mathfrak{h}(V) \le \max\{\hat{\mathfrak{h}}(G), \hat{\mathfrak{h}}(H)\}$ for any subgroup $V \subset G \times H$.

We let Proj_G and Proj_H be the projections mapping $G \times H$ to G and H respectively, and denote $V_G = \mathrm{Proj}_G(V)$ and $V_H = \mathrm{Proj}_H(V)$. Then $\mathrm{Proj}_G \times \mathrm{Proj}_H$ maps V injectively into $V_G \times V_H$. Let n denote $\max\{\hat{\mathfrak{h}}(G), \hat{\mathfrak{h}}(H)\}$, and then there exists a sequence

$$1 \lhd V_{G,1} \times V_{H,1} \lhd V_{G,2} \times V_{H,2} \lhd \cdots \lhd V_{G,n} \times V_{H,n} = V_G \times V_H.$$

of normal subgroups of $V_G \times V_H$ of length n, where $\{V_{*,i}\}$ for $* = G$ or H is a sequence of normal subgroups of V_* such that $V_{*,i+1}/V_{*,i}$ is a direct product of minimal normal subgroups of $V_*/V_{*,i}$.

Assume that A is a minimal normal subgroup of $V_G \times V_H$ contained in $V_{G,1} \times V_{H,1}$ such that $A \cap V \neq 1$. Since V is a subgroup of $V_G \times V_H$, we have that $A \cap V$ is normal in V. Then $\mathrm{Proj}_G \times \mathrm{Proj}_H$ sends $A \cap V$ to a normal subgroup of $V_G \times V_H$ that is contained in $\mathrm{Proj}_G \times \mathrm{Proj}_H(A) \subset V_{G,1} \times V_{H,1}$. We see that $A \cap V$ is A, because $A \cap V \neq 1$ and A is minimal normal in $V_G \times V_H$. In particular, $A \cap V$ is a minimal normal subgroup of V, because otherwise Proj_G would map a minimal normal subgroup of V contained in $A \cap V$ to a normal subgroup of V_G that is properly contained in A which contradicts to the assumption that A is minimal normal. Thus, we have shown that $V \cap (V_{G,1} \times V_{H,1})$ is a direct product of minimal normal subgroups of V. Then by induction on i, we see that $\{V_i := V \cap (V_{G,i} \times V_{H,i})\}_{i=1}^n$ forms a sequence of normal subgroups of V such that V_{i+1}/V_i is a direct product of minimal normal subgroups of V/V_i, and hence $\mathfrak{h}(V) \leq \max\{\hat{\mathfrak{h}}(G), \hat{\mathfrak{h}}(H)\}$. □

Proposition 6.3. *Let Γ be a finite group and $\mathcal{C}$ a finite set of isomorphism classes of finite Γ-groups. For any Γ-group G, we have that $\hat{\mathfrak{h}}(G^{\mathcal{C}})$ is at most*

$$\hat{\mathfrak{h}}_{\mathcal{C}} := \max\{\hat{\mathfrak{h}}(H) \mid H \in \mathcal{C}\}.$$

Proof. By definition of $\hat{\mathfrak{h}}(G^{\mathcal{C}})$, it suffices to prove $\hat{\mathfrak{h}}(G) \leq \hat{\mathfrak{h}}_{\mathcal{C}}$ for any $G \in \overline{\mathcal{C}}$. So we just need to show that the three actions,

(1) taking Γ-quotients,

(2) taking Γ-subgroups, and

(3) taking finite direct products,

do not produce groups with larger value of $\hat{\mathfrak{h}}$. For the first two actions, it is obvious that if H is a Γ-quotient or a Γ-subgroup of G, then it is a quotient or a subgroup of G by forgetting the Γ actions, and hence $\hat{\mathfrak{h}}(H) \leq \hat{\mathfrak{h}}(G)$ by definition of heights. The last action follows by Lemma 6.2. □

We finish this section by applying Proposition 6.3 to prove the following number theory theorem.

Theorem 6.4. *Let k/Q be a Galois global field extension with $\mathrm{Gal}(k/Q) \simeq \Gamma$ and S a finite k/Q-closed set of places of k. Let $\mathcal{C}$ be a finite set of isomorphism classes of finite Γ-groups. Then $G_S(k)^{\mathcal{C}}$ is a finite group.*

Proof. By Proposition 6.3, we have that

$$h := \hat{\mathfrak{h}}(G_S(k)^{\mathcal{C}}) \leq \hat{\mathfrak{h}}_{\mathcal{C}}$$

is finite. So there exists a sequence of normal subgroups of $G_S(k)^{\mathcal{C}}$,

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_h = G_S(k)^{\mathcal{C}},$$

such that H_{i+1}/H_i is isomorphic to a direct product of minimal normal subgroups of H_h/H_i. Note that each of the minimal normal subgroups is a (not necessarily finite) direct product of isomorphic finite simple groups. So, for each i, H_{i+1}/H_i as a group is a direct product of finite simple groups. On the other hand, $G_S(k)^{\mathcal{C}}$ is a quotient of $G_S(k)$, so is the Galois group of an extension of k that is unramified outside S. Therefore, H_{i+1}/H_i is the Galois group of an extension K_i/K_{i+1} of some intermediate fields between k_S and k. We denote by S_i the set of primes of K_i lying above S.

For a prime $\mathfrak{P}$ of K_i, the local absolute Galois group $\mathcal{G}_{\mathfrak{P}}(K_i)$ is finitely generated, so there are finitely many Galois extensions of $(K_i)_{\mathfrak{P}}$ having a fixed Galois group. Then for a simple group E, there exists an integer $N_{E,\mathfrak{P}}(K_i)$ for each $\mathfrak{P} \in S_i$, such that any Galois extension of $(K_i)_{\mathfrak{P}}$ whose Galois group is a subgroup of E has discriminant at most $N_{E,\mathfrak{P}}(K_i)$. Let $N_{E,S}(K_i)$ denote the product $\prod_{\mathfrak{P}\in S_i} N_{E,\mathfrak{P}}(K_i)$. By the Hermite-Minkowski theorem (see [Goss 1996, Theorem 8.23.5(3)] for the function field version of this theorem), for each finite simple group E, there are only finitely many extensions of K_i that have Galois group E and of discriminant at most $N_{E,S}(K_i)$. Therefore, there are finitely many extensions of K_i that are of Galois group E and unramified outside S_i.

Since $\mathcal{C}$ is finite, there are only finitely many simple groups that appear as composition factors of groups in $\bar{\mathcal{C}}$ (see [Liu and Wood 2020, Corollary 6.12]). Now we consider the tower of extensions K_i. Note that $K_h = k$ and $\mathrm{Gal}(K_{h-1}/K_h) \simeq H_h/H_{h-1}$. By the above argument, we conclude that H_h/H_{h-1} is a direct product of finite simple groups, that there are finitely many choices of these finite simple groups, and that for each of them there are finitely many copies of this simple group appearing in H_h/H_{h-1}. So we obtain that H_h/H_{h-1} is finite, and hence K_{h-1} is a finite extension of k. By induction, we see that H_{i+1}/H_i is finite for each $i = h-1, \ldots, 0$, and it follows that $G_S(k)^{\mathcal{C}}$ is finite. □

7. A generalized version of global Euler–Poincaré characteristic formula

Throughout this section, we let k/Q be a finite Galois extension of global fields, and S be a *finite nonempty* k/Q-closed set of primes of k such that $S_\infty(k) \subseteq S$. For each $A \in \mathrm{Mod}(\mathrm{Gal}(k_S/Q))$, we define

$$\chi_{k/Q,S}(A) = \frac{\#H^2(G_S(k), A)^{\mathrm{Gal}(k/Q)} \#H^0(G_S(k), A)^{\mathrm{Gal}(k/Q)}}{\#H^1(G_S(k), A)^{\mathrm{Gal}(k/Q)}},$$

where $\mathrm{Gal}(k/Q)$ acts on $H^i(G_S(k), A)$ by conjugation. We will prove the following theorem.

Theorem 7.1. *Use the assumption at the beginning of this section. If $A \in \mathrm{Mod}_S(\mathrm{Gal}(k_S/Q))$ has order prime to $[k : Q]$, then*

$$\chi_{k/Q,S}(A) = \#\Big(\bigoplus_{v\in S_\infty(Q)} \widehat{H}^0(Q_v, A')\Big) \Big/ \#\Big(\bigoplus_{v\in S_\infty(Q)} H^0(Q_v, A')\Big).$$

Remark 7.2. (1) If k is a function field, then the theorem says that $\chi_{k/Q,S}(A) = 1$ since $S_\infty(k) = \varnothing$.

(2) When $k = Q$, the theorem is exactly the global Euler–Poincaré characteristic formula [Neukirch et al. 2008, Theorem (8.7.4)].

(3) When Q is a number field, a similar result is proven in [Clozel et al. 2008, Lemma 2.3.3].

7.1. *Preparation for the proof.*

Lemma 7.3. *Let G be a profinite group and U an open normal subgroup of G. Let H be an open subgroup of G and V denote $U \cap H$. Then H/V is naturally a subgroup of G/U, and for an H-module A we have*

$$H^i(U, \mathrm{Ind}_G^H A) \cong \mathrm{Ind}_{G/U}^{H/V} H^i(V, A)$$

as G/U-modules for each $i \geq 0$.

Proof. Under the quotient map $G \twoheadrightarrow G/U$, H/V is the image of H, so it is a subgroup of G/U. Then

$$\mathrm{Ind}_G^H A = \mathrm{Ind}_G^{UH} \mathrm{Ind}_{UH}^H A = \bigoplus_{\sigma \in G/UH} \sigma(\mathrm{Ind}_{UH}^H A),$$

where we denote by $\sigma(\mathrm{Ind}_{UH}^H A)$ the $\sigma UH\sigma^{-1}$-module, whose underlying group is $\mathrm{Ind}_{UH}^H A$ and the action of $\tau \in \sigma UH\sigma^{-1}$ is given by $a \mapsto \sigma^{-1}\tau\sigma a$. So

$$\begin{aligned} H^i(U, \mathrm{Ind}_G^H A) &= \bigoplus_{\sigma \in G/UH} H^i(U, \sigma(\mathrm{Ind}_{UH}^H A)) \\ &= \bigoplus_{\sigma \in G/UH} \sigma_* H^i(U, \mathrm{Ind}_{UH}^H A) \\ &= \mathrm{Ind}_{G/U}^{H/V} H^i(U, \mathrm{Ind}_{UH}^H A), \end{aligned} \tag{7-1}$$

where the second equality follows by $U \trianglelefteq G$ and the definition of the conjugation action σ_* on cohomology groups, and the last equality is because the quotient map $G \to G/U$ maps a set of representatives of G/UH to a set of representatives of $(G/U)/(H/V)$. Since A is an H-module, UH acts on $\mathrm{Ind}_U^V A$, and moreover, it follows by $V = H \cap U$ that $\mathrm{Ind}_U^V A = \mathrm{Ind}_{UH}^H A$ as UH-modules. So we have the following identity of H/V-modules:

$$H^i(U, \mathrm{Ind}_{UH}^H A) = H^i(U, \mathrm{Ind}_U^V A) \cong H^i(V, A), \tag{7-2}$$

where the last isomorphism follows by Shapiro's lemma. The lemma follows from (7-1) and (7-2). □

For the rest of this section, we assume S is a nonempty k/Q-closed set of primes of k containing S_∞ and let $G = \mathrm{Gal}(k_S/Q)$ and $U = G_S(k)$. For each open subgroup H of $\mathrm{Gal}(k_S/Q)$ we let $V = U \cap H$ and K be the fixed field of V, and define a map

$$\varphi_{H,S} : \mathrm{Mod}(H) \to K_0'(\mathbb{Z}[H/V]),$$

$$A \mapsto [H^0(V, A)] - [H^1(V, A)] + [H^2(V, A)] - \Big[\bigoplus_{\mathfrak{P} \in S_\infty(K)} \widehat{H}^0(K_{\mathfrak{P}}, A')\Big]^\vee + \Big[\bigoplus_{\mathfrak{P} \in S_\infty(K)} H^0(K_{\mathfrak{P}}, A')\Big]^\vee,$$

where H/V acts on $\bigoplus_{\mathfrak{P} \in S_\infty(K)} H^0(K_{\mathfrak{P}}, A')$ (similarly on Tate cohomology) by its permutation action on $S_\infty(K)$ and by the $\mathrm{Gal}_{\mathfrak{P}}(K/Q) \cap H$ on each summand, and the Pontryagin dual is taking on the classes of $K_0'(\mathbb{Z}[H/V])$.

Lemma 7.4. *Using the notation above, we have the following isomorphisms of G/U-modules for any $A \in \mathrm{Mod}(H)$:*

$$\bigoplus_{\mathfrak{p} \in S_\infty(k)} H^0(k_{\mathfrak{p}}, \mathrm{Ind}_G^H A) \cong \mathrm{Ind}_{G/U}^{H/V} \bigoplus_{\mathfrak{P} \in S_\infty(K)} H^0(K_{\mathfrak{P}}, A), \tag{7-3}$$

$$\bigoplus_{\mathfrak{p} \in S_\infty(k)} \widehat{H}^0(k_{\mathfrak{p}}, \mathrm{Ind}_G^H A) \cong \mathrm{Ind}_{G/U}^{H/V} \bigoplus_{\mathfrak{P} \in S_\infty(K)} \widehat{H}^0(K_{\mathfrak{P}}, A). \tag{7-4}$$

Proof. It suffices to fix a $v \in S_\infty(Q)$ and prove (7-3) and (7-4) for places above v. For each $\mathfrak{p} \in S_v(k)$, $\mathrm{Ind}_G^H A$ as a $\mathcal{G}_v(Q)$-module has the following canonical decomposition (see [Neukirch et al. 2008, §1.5, Example 5]):

$$\mathrm{Res}_{\mathcal{G}_v}^G \mathrm{Ind}_G^H A = \bigoplus_{\sigma \in \mathcal{G}_v \backslash G/H} \mathrm{Ind}_{\mathcal{G}_v}^{\mathcal{G}_v \cap \sigma H \sigma^{-1}} \sigma \, \mathrm{Res}^H_{\sigma^{-1}\mathcal{G}_v\sigma \cap H} A. \tag{7-5}$$

If v splits completely in k/Q, then $\mathrm{Gal}_v(k/Q) = 1$ and $\mathcal{G}_\mathfrak{p}(k) = \mathcal{G}_v(Q)$. So we have the following identities of $\mathrm{Gal}_v(k/Q)$-modules:

$$\begin{aligned} H^0(k_\mathfrak{p}, \mathrm{Ind}_G^H A) &= \bigoplus_{\sigma \in \mathcal{G}_v \backslash G/H} H^0(\mathcal{G}_v \cap \sigma H \sigma^{-1}, \sigma \,\mathrm{Res}^H_{\sigma^{-1}\mathcal{G}_v\sigma \cap H} A) \\ &= \bigoplus_{\sigma \in \mathcal{G}_v \backslash G/H} \sigma_* H^0(\sigma \mathcal{G}_v \sigma^{-1} \cap H, \mathrm{Res}^H_{\sigma^{-1}\mathcal{G}_v\sigma \cap H} A), \end{aligned} \tag{7-6}$$

where the first equality uses (7-5) and Shapiro's lemma, and the second follows by definition of the conjugation action on cohomology groups. We let L denote the fixed field of H. Then, the set $\{\sigma \mathcal{G}_\mathfrak{p} \sigma^{-1} \cap H \mid \sigma \in \mathcal{G}_\mathfrak{p} \backslash G/H\}$ is exactly the set $\{\mathcal{G}_w(L) \mid w \in S_v(L)\}$. Therefore, we have the identity of abelian groups (hence of $\mathrm{Gal}_v(k/Q)$-modules since $\mathrm{Gal}_v(k/Q) = 1$)

$$H^0(k_\mathfrak{p}, \mathrm{Ind}_G^H A) = \bigoplus_{w \in S_v(L)} H^0(L_w, A),$$

and hence

$$\bigoplus_{\mathfrak{p} \in S_v(k)} H^0(k_\mathfrak{p}, \mathrm{Ind}_G^H A) = \mathrm{Ind}_{G/U}^1 \Big(\bigoplus_{w \in S_v(L)} H^0(L_w, A) \Big) \tag{7-7}$$

because the $\mathrm{Gal}(k/Q)$-action on this direct sum is determined by its permutation action on places above v. On the other hand, because $K = kL$, the assumption that v splits completely in k/Q implies that w splits completely in K for any $w \in S_v(L)$ and then we obtain

$$\bigoplus_{\mathfrak{P} \in S_v(K)} H^0(K_\mathfrak{P}, A) = \mathrm{Ind}_{H/V}^1 \Big(\bigoplus_{w \in S_v(L)} H^0(L_w, A) \Big). \tag{7-8}$$

Thus, (7-7) and (7-8) prove (7-3) in this case. The isomorphism in (7-4) can be proven using the exactly same argument.

Otherwise, v is ramified in k/Q, so $\mathrm{Gal}_v(k/Q) \simeq \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_\mathfrak{p}(k) = 1$ and $\mathcal{G}_\mathfrak{P}(K) = 1$ for each $\mathfrak{p} \in S_v(k)$ and $\mathfrak{P} \in S_v(K)$. Then (7-4) automatically follows because of $\widehat{H}^0(k_\mathfrak{p}, \mathrm{Ind}_G^H A) = \widehat{H}^0(K_\mathfrak{P}, A) = 0$. The set of right cosets G/H naturally acts on $S_v(L)$, and moreover, for any $w \in S_v(L)$ and $\sigma_1, \sigma_2 \in G/H$, $\sigma_1^{-1}\sigma_2$ is contained in $\mathcal{G}_w(L) \subset \mathrm{Gal}(K/L)$ if and only if $\sigma_1(w) = \sigma_2(w)$. So by (7-5), we have the following identities of $\mathrm{Gal}_\mathfrak{p}(k/Q)$-modules:

$$H^0(k_\mathfrak{p}, \mathrm{Ind}_G^H A) = \mathrm{Res}^G_{\mathcal{G}_v(Q)} \mathrm{Ind}_G^H A = \bigoplus_{w \in S_\mathbb{R}(L)} A_w \oplus \bigoplus_{w \in S_\mathbb{C}(L)} (A_w \oplus \tau A_w),$$

where $A_w := \mathrm{Res}^H_{\mathcal{G}_w(L)} A$ and τ denotes the nontrivial element in $\mathrm{Gal}_v(k/Q)$. So we have the following identity of $\mathrm{Gal}(k/Q)$-modules:

$$\bigoplus_{\mathfrak{p} \in S_v(k)} H^0(k_\mathfrak{p}, \mathrm{Ind}_G^H A) = \bigoplus_{w \in S_\mathbb{R}(L)} \mathrm{Ind}^{\mathrm{Gal}_v(k/Q)}_{\mathrm{Gal}(k/Q)} A_w \oplus \bigoplus_{w \in S_\mathbb{C}(L)} \mathrm{Ind}^1_{\mathrm{Gal}(k/Q)} A_w. \tag{7-9}$$

Finally, because $w \in S_v(L)$ is imaginary if and only if $\mathrm{Gal}_w(K/L) = 1$, we have

$$\begin{aligned}\mathrm{Ind}_{G/U}^{H/V}\bigoplus_{\mathfrak{P}\in S_v(K)} H^0(K_{\mathfrak{P}}, A) &= \mathrm{Ind}_{G/U}^{H/V}\Big(\bigoplus_{w\in S_v(L)}\bigoplus_{\mathfrak{P}\in S_w(K)} A_w\Big)\\ &= \mathrm{Ind}_{G/U}^{H/V}\Big(\bigoplus_{w\in S_{\mathbb{R}}(L)} \mathrm{Ind}_{\mathrm{Gal}(K/L)}^{\mathrm{Gal}_w(K/L)} A_w \oplus \bigoplus_{w\in S_{\mathbb{C}}(L)} \mathrm{Ind}_{\mathrm{Gal}(K/L)}^{1} A_w\Big)\\ &= \bigoplus_{w\in S_{\mathbb{R}}(L)} \mathrm{Ind}_{\mathrm{Gal}(k/Q)}^{\mathrm{Gal}_v(k/Q)} A_w \oplus \bigoplus_{w\in S_{\mathbb{C}}(L)} \mathrm{Ind}_{\mathrm{Gal}(k/Q)}^{1} A_w. \end{aligned} \tag{7-10}$$

Thus, (7-3) follows by (7-9) and (7-10). □

The corollary below immediately follows by Lemmas 7.3, 7.4 and the fact $\mathrm{Ind}_G^H A' = (\mathrm{Ind}_G^H A)'$.

Corollary 7.5. *For any open subgroup H of G and $A \in \mathrm{Mod}(H)$, we have*

$$\varphi_{G,S}(\mathrm{Ind}_G^H A) \simeq \mathrm{Ind}_{G/U}^{H/V} \varphi_{H,S}(A).$$

Lemma 7.6. *The map $\varphi_{G,S}$ is additive on short exact sequences of modules in* $\mathrm{Mod}_S(G)$.

Proof. Denote $G_S(k)$ by G_S. Let $0 \to A_1 \to A_2 \to A_3 \to 0$ be an exact sequence of finite modules in $\mathrm{Mod}_S(G)$. By considering the associated long exact sequence of group cohomology, we have the following identity of elements in $K_0'(\mathbb{Z}[\mathrm{Gal}(k/Q)])$:

$$\sum_{i=0}^{2}\sum_{j=1}^{3}(-1)^{i+j+1}[H^i(G_S, A_j)] = \sum_{i=3}^{4}\sum_{j=1}^{3}(-1)^{i+j}[H^i(G_S, A_j)] + [\delta H^4(G_S, A_3)], \tag{7-11}$$

where δ denotes the connecting map $H^i \to H^{i+1}$ (or $\widehat{H}^i \to \widehat{H}^{i+1}$ for Tate cohomology groups) in the long exact sequence. By [Neukirch et al. 2008, Theorem (8.6.10)(ii)], for $i \geq 3$ and any j, the restriction map $H^i(G_S, A_j) \to \bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)} H^i(k_{\mathfrak{p}}, A_j)$ is an isomorphism. Note that for $\mathfrak{p} \in S_{\mathbb{R}}(k)$, we have $\mathcal{G}_{\mathfrak{p}}(k) = \mathbb{Z}/2\mathbb{Z}$, so by [Neukirch et al. 2008, Propositions (1.7.1) and (1.7.2)] we have

$$\begin{aligned}\sum_{i=3}^{4}\sum_{j=1}^{3}(-1)^{i+j}[H^i(G_S, A_j)] &= \sum_{i=3}^{4}\sum_{j=1}^{3}(-1)^{i+j}\Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)} H^i(k_{\mathfrak{p}}, A_j)\Big]\\ &= \sum_{\mathfrak{p}\in S_{\mathbb{R}}(k)}\sum_{i=-1}^{0}\sum_{j=1}^{3}(-1)^{i+j}[\widehat{H}^i(k_{\mathfrak{p}}, A_j)] = 0.\end{aligned}$$

So (7-11) gives

$$\begin{aligned}\sum_{i=0}^{2}\sum_{j=1}^{3}(-1)^{i+j+1}[H^i(G_S, A_j)] &= [\delta H^4(G_S, A_3)]\\ &= \Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)} \delta H^4(k_{\mathfrak{p}}, A_3)\Big] = \Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)} \delta \widehat{H}^0(k_{\mathfrak{p}}, A_3)\Big]\\ &= \Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)} \ker(\widehat{H}^1(k_{\mathfrak{p}}, A_1) \to \widehat{H}^1(k_{\mathfrak{p}}, A_2))\Big]\\ &= \Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)} \mathrm{coker}(\widehat{H}^1(k_{\mathfrak{p}}, A_2') \to \widehat{H}^1(k_{\mathfrak{p}}, A_1'))\Big]^{\vee}\\ &= \Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)} \delta \widehat{H}^1(k_{\mathfrak{p}}, A_1')\Big]^{\vee},\end{aligned} \tag{7-12}$$

where the fourth and last equalities use the long exact sequence of Tate cohomology groups, and the fifth uses the local duality theorem [Neukirch et al. 2008, Theorem (7.2.17)]. On the other hand, again by [Neukirch et al. 2008, Propositions (1.7.1) and (1.7.2)], the long exact sequence induced by

$$0 \to A_3' \to A_2' \to A_1' \to 0 \tag{7-13}$$

implies

$$\begin{aligned}\sum_{j=1}^{3}(-1)^{j+1}\Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)}\widehat{H}^0(k_{\mathfrak{p}}, A_j')\Big] &= \sum_{j=1}^{3}(-1)^{j+1}\Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)}\widehat{H}^1(k_{\mathfrak{p}}, A_j')\Big]\\ &= \sum_{j=1}^{3}(-1)^{j+1}\Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)}H^0(k_{\mathfrak{p}}, A_j')\Big] + \Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)}\delta H^1(k_{\mathfrak{p}}, A_1')\Big], \end{aligned}\tag{7-14}$$

where the last equality follows by the long exact sequence of group cohomology induced by (7-13). Therefore, combining (7-12) and (7-14), we obtain

$$\varphi_{G,S}(A_1) - \varphi_{G,S}(A_2) + \varphi_{G,S}(A_3) = 0. \qquad \square$$

Lemma 7.7. *If $\ell \in \mathbb{N}(S)$ is a prime, then we have the following identities of elements in $K_0'(\mathbb{F}_\ell[\mathrm{Gal}(K/Q)])$ for any Galois extension K of Q with $k(\mu_\ell) \subset K \subset k_S$:*

$$\begin{aligned}&[H^0(\mathrm{Gal}(k_S/K), \mu_\ell)] = [\mu_\ell],\\ &[H^1(\mathrm{Gal}(k_S/K), \mu_\ell)] = [\mathcal{O}_{K,S}^\times/\ell] + [\mathrm{Cl}_S(K)[\ell]],\\ &[H^2(\mathrm{Gal}(k_S/K), \mu_\ell)] = [\mathrm{Cl}_S(K)/\ell] - [\mathbb{F}_\ell] + \Big[\bigoplus_{\mathfrak{P}\in S\setminus S_\infty(K)}\mathbb{F}_\ell\Big] + \Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)}\widehat{H}^0(\mathcal{G}_{\mathfrak{P}}, \mathbb{F}_\ell)\Big],\end{aligned}$$

where $\mathrm{Cl}_S(K)$ is the S-class group of K, $\mathrm{Cl}_S(K)[\ell]$ is the ℓ-torsion subgroup of $\mathrm{Cl}_S(K)$, and $\mathcal{O}_{K,S}^\times/\ell$ and $\mathrm{Cl}_S(K)/\ell$ denote the maximal exponent-ℓ quotients of $\mathcal{O}_{K,S}^\times$ and $\mathrm{Cl}_S(K)$ respectively.

Proof. The lemma follows directly from the claims (i)–(iii) in the proof of [Neukirch et al. 2008, Theorem 8.7.4]. Though the proof of those claims only shows these identities when each terms are treated as Grothendieck group elements of $\mathrm{Gal}(K/k)$-modules, one can check that the ideas there work generally for the base field Q instead of k. $\square$

Proof of Theorem 7.1. For any G-module A and $v \in S_\infty(Q)$,

$$\bigoplus_{\mathfrak{p}\in S_v(k)} H^0(k_{\mathfrak{p}}, A') \cong \mathrm{Ind}_{\mathrm{Gal}(k/Q)}^{\mathrm{Gal}_{\mathfrak{p}}(k/Q)} H^0(k_{\mathfrak{p}}, A')$$

as $\mathrm{Gal}(k/Q)$-modules, where $\mathfrak{p}$ on the right-hand side is an arbitrarily chosen place in $S_v(k)$. So by Shapiro's lemma, we have

$$\Big(\bigoplus_{\mathfrak{p}\in S_v(k)} H^0(k_{\mathfrak{p}}, A')\Big)^{\mathrm{Gal}(k/Q)} \cong H^0(k_{\mathfrak{p}}, A')^{\mathrm{Gal}_{\mathfrak{p}}(k/Q)} = H^0(Q_v, A'). \tag{7-15}$$

If $\mathrm{Gal}_{\mathfrak{p}}(k/Q)=\mathbb{Z}/2\mathbb{Z}$, then $\widehat{H}^0(k_{\mathfrak{p}}, A')=\widehat{H}^0(Q_v, A')=0$ because $|A'|$ has to be odd as $\gcd(|A|, [k:Q])=1$. If $\mathrm{Gal}_{\mathfrak{p}}(k/Q)=1$, then $\widehat{H}^0(k_{\mathfrak{p}}, A')=\widehat{H}^0(Q_v, A')$. So

$$\Big(\bigoplus_{\mathfrak{p}\in S_v(k)} \widehat{H}^0(k_{\mathfrak{p}}, A')\Big)^{\mathrm{Gal}(k/Q)} \cong \widehat{H}^0(k_{\mathfrak{p}}, A')^{\mathrm{Gal}_{\mathfrak{p}}(k/Q)} = \widehat{H}^0(Q_v, A'). \tag{7-16}$$

Note that for any $M \in \mathrm{Mod}(\mathrm{Gal}(k/Q))$, we have $(M^\vee)^{\mathrm{Gal}(k/Q)} = \mathrm{Hom}_{\mathrm{Gal}(k/Q)}(M, \mathbb{Q}/\mathbb{Z}) \simeq M_{\mathrm{Gal}(k/Q)}$. When M has order prime to $[k:\mathbb{Q}]$, $M^{\mathrm{Gal}(k/\mathbb{Q})}$ and $M_{\mathrm{Gal}(k/\mathbb{Q})}$ are isomorphic. So the $\mathrm{Gal}(k/Q)$-invariants of

$$\Big(\bigoplus_{\mathfrak{p}\in S_v(k)} H^0(k_{\mathfrak{p}}, A')\Big)^\vee \quad \text{and} \quad \Big(\bigoplus_{\mathfrak{p}\in S_v(k)} \widehat{H}^0(k_{\mathfrak{p}}, A')\Big)^\vee$$

are $H^0(Q_v, A')$ and $\widehat{H}^0(Q_v, A')$ respectively.

We let R denote the ring $\prod_{p\nmid[k:Q]} \mathbb{Z}_p$. Let $\Theta : K_0'(R[\mathrm{Gal}(k/Q)]) \to \mathbb{Z}$ be the map defined by sending the class $[A]$ to the size of $A^{\mathrm{Gal}(k/Q)}$, which is a group homomorphism because taking $\mathrm{Gal}(k/Q)$-invariants is an exact functor in the category of $R[\mathrm{Gal}(k/Q)]$-modules. So we want to show that $\Theta\circ\varphi_{G,S}$ is the zero map when restricted to modules in $\mathrm{Mod}_S(\mathrm{Gal}(k_S/Q))$ with order prime to $[k:Q]$. By Lemma 7.6 we just need to show

$$\Theta\circ\varphi_{G,S}(K_0'(\mathbb{F}_\ell[\mathrm{Gal}(E/Q)])) = 0 \tag{7-17}$$

for any prime integer $\ell \in \mathbb{N}(S)$ with $\ell \nmid [k:Q]$ and any finite extension E of k that is Galois over Q. Because the codomain of the map Θ is free, (7-17) is equivalent to the vanishing of $\Theta\circ\varphi_{G,S}$ on the torsion-free part of $K_0'(\mathbb{F}_\ell[\mathrm{Gal}(E/Q)])$. Note that, by [Neukirch et al. 2008, Lemma (7.3.4)], the $\mathbb{Q}$-linear space $K_0'(\mathbb{F}_\ell[\mathrm{Gal}(E/Q)])\otimes_{\mathbb{Z}}\mathbb{Q}$ is generated by classes in the form of $\mathrm{Ind}_{\mathrm{Gal}(E/Q)}^{\overline{C}} A$, where $\overline{C}$ runs over all cyclic subgroups of $\mathrm{Gal}(E/Q)$ of order prime to ℓ and A runs over classes of $K_0'(\mathbb{F}_\ell[\overline{C}])$. For such $\overline{C}$ and A, we denote by C the full preimage of $\overline{C}$ in $G=\mathrm{Gal}(k_S/Q)$, and then by Corollary 7.5 and $\mathrm{Ind}_{\mathrm{Gal}(E/Q)}^{\overline{C}} A = \mathrm{Ind}_G^C A$, we have that $\Theta\circ\varphi_{G,S}(\mathrm{Ind}_G^C A)=0$ if and only if $\Theta\circ\varphi_{C,S}(A)=0$. By setting G to be C, U to be $C\cap U$, Q to be $(k_S)^C$ and k to be $(k_S)^{C\cap U}$, we finally reduce the problem to the statement that we will prove in the rest of this section:

$$\begin{aligned}&\Theta\circ\varphi_{G,S}(A)=0 \text{ for all } A\in \mathrm{Mod}_\ell(G) \text{ such that } k(A)/Q \text{ is}\\ &\quad\text{a cyclic extension of } Q \text{ of order relatively prime to } \ell.\end{aligned} \tag{7-18}$$

We let $K=k(A, \mu_\ell)$. So under the assumption in (7-18), we have that $\mathrm{Gal}(K/Q)$ is an abelian group of order relatively prime to ℓ, in which case the Hochschild–Serre spectral sequence for the group extension

$$1 \to \mathrm{Gal}(k_S/K) \to \mathrm{Gal}(k_S/k) \to \mathrm{Gal}(K/k) \to 1$$

and the module A degenerates, and then for each $i\geq 0$ we have that

$$H^i(\mathrm{Gal}(k_S/k), A) \cong H^i(\mathrm{Gal}(k_S/K), A)^{\mathrm{Gal}(K/k)}. \tag{7-19}$$

We first consider the module $A = \mu_\ell$, then $K = k(\mu_\ell)$ and we let $\overline{G} = \mathrm{Gal}(K/Q)$. As $\ell \nmid \mathrm{Gal}(K/Q)$, in both the number field case (by [Neukirch et al. 2008, Corollary (8.7.3)]) and the function field case (by a standard argument using the divisor group), we have that

$$[\mathcal{O}_{K,S}^{\times}/\ell] = \Big[\bigoplus_{\mathfrak{P}\in S(K)} \mathbb{F}_\ell\Big] + [\mu_\ell] - [\mathbb{F}_\ell]$$

in $K_0'(\mathbb{F}_\ell[\overline{G}])$. Then since $[\mathrm{Cl}_S(K)[\ell]] = [\mathrm{Cl}_S(K)/\ell]$ as they are the kernel and the cokernel of the map $\mathrm{Cl}_S(K) \xrightarrow{\times\ell} \mathrm{Cl}_S(K)$, by Lemma 7.7 we have

$$\sum_{i=0}^{2}(-1)^i[H^i(\mathrm{Gal}(k_S/K), \mu_\ell)] = \Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)} \widehat{H}^0(K_\mathfrak{P}, \mathbb{F}_\ell)\Big] - \Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)} H^0(K_\mathfrak{P}, \mathbb{F}_\ell)\Big], \tag{7-20}$$

and hence $\varphi_{G,S}(\mu_\ell) = 0$ follows easily by (7-19) and by the arguments in the first paragraph of this subsection. Thus $\Theta \circ \varphi_{G,S}(\mu_\ell) = 0$.

For a general finite module $A \in \mathrm{Mod}_\ell(G)$, we again let $K = k(A, \mu_\ell)$ and $\overline{G} = \mathrm{Gal}(K/Q)$. We define

$$\chi : \mathrm{Mod}_\ell(\overline{G}) \to K_0'(\mathbb{F}_\ell[\overline{G}]), \quad M \mapsto \sum_{i=0}^{2}(-1)^i[H^i(\mathrm{Gal}(k_S/K), M)].$$

Because A and μ_ℓ are both trivial $\mathrm{Gal}(k_S/K)$-modules, the pairing

$$\mu_\ell \times \mathrm{Hom}(A', \mathbb{F}_\ell) \to \mathrm{Hom}(A', \mu_\ell) = A, \quad (\zeta, f) \mapsto (x \mapsto \zeta^{f(x)})$$

defines $\overline{G}$-isomorphisms via the cup product

$$H^i(\mathrm{Gal}(k_S/K), \mu_\ell) \otimes_{\mathbb{Z}} \mathrm{Hom}(A', \mathbb{F}_\ell) \xrightarrow{\sim} H^i(\mathrm{Gal}(k_S/K), A).$$

So we have $\chi(A) = [A'^\vee]\chi(\mu_\ell)$, and hence by (7-20) we have

$$\chi(A) = [A'^\vee]\Big(\Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)} \widehat{H}^0(K_\mathfrak{P}, \mathbb{F}_\ell)\Big] - \Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)} H^0(K_\mathfrak{P}, \mathbb{F}_\ell)\Big]\Big).$$

If Q is a function field, then (7-18) follows immediately after taking the $\overline{G}$-invariants on both sides above.

For the rest of the proof we consider the number field case. Let $S_\infty^-(Q)$ be the set of archimedean places of Q lying below the imaginary places of K if $\ell = 2$, and be the set $S_\infty(Q)$ if ℓ is odd. One can check by definition of $\widehat{H}^0$ that for any module $M \in \mathrm{Mod}_\ell(\overline{G})$ (for example, $M = A'$ and $M = \mathbb{F}_\ell$), we have

$$\Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)} \widehat{H}^0(K_\mathfrak{P}, M)\Big] - \Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)} H^0(K_\mathfrak{P}, M)\Big] = \sum_{v\in S_\infty^-(Q)} -[\mathrm{Ind}_{\overline{G}}^{\overline{G}_v} M],$$

where the group $\overline{G}_v$ is the decomposition subgroup $G_v(K/Q)$. Also, note that $(\mathrm{Ind}_{\overline{G}}^{\overline{G}_v} \mathbb{F}_\ell) \otimes_{\mathbb{Z}} M \cong \mathrm{Ind}_{\overline{G}}^{\overline{G}_v} M$ for any $M \in \mathrm{Mod}_\ell(\overline{G})$ and that

$$(\mathrm{Ind}_{\overline{G}}^{\overline{G}_v} M)^{\overline{G}} = H^0(\overline{G}, \mathrm{Ind}_{\overline{G}}^{\overline{G}_v} M) = H^0(\overline{G}_v, M) = M^{\overline{G}_v}.$$

So we have

$$\begin{aligned}\Theta\circ\varphi_{G,\ell}(A) &= \#\Big(\sum_{i=0}^{2}(-1)^i[H^i(G_S(k),A)] - \Big[\bigoplus_{\mathfrak{p}\in S_\infty(k)}\widehat{H}^0(k_\mathfrak{p},A')\Big]^\vee + \Big[\bigoplus_{\mathfrak{p}\in S_\infty(k)}H^0(k_\mathfrak{p},A')\Big]^\vee\Big)^{\mathrm{Gal}(k/Q)}\\ &= \#\Big(\chi(A) - \Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)}\widehat{H}^0(K_\mathfrak{P},A')\Big]^\vee + \Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)}H^0(K_\mathfrak{P},A')\Big]^\vee\Big)^{\overline{G}}\\ &= \sum_{v\in S_\infty^-(Q)}\#\big(-[A'^\vee][\mathrm{Ind}_{\overline{G}}^{\overline{G}_v}\mathbb{F}_\ell] + [\mathrm{Ind}_{\overline{G}}^{\overline{G}_v}A']^\vee\big)^{\overline{G}}\\ &= \sum_{v\in S_\infty^-(Q)}\#\big(-[\mathrm{Ind}_{\overline{G}}^{\overline{G}_v}A'^\vee] + [\mathrm{Ind}_{\overline{G}}^{\overline{G}_v}A']^\vee\big)^{\overline{G}} = 0,\end{aligned}$$

completing the proof of Theorem 7.1. □

8. Definition and properties of $Б_S(k, A)$

Throughout this section, we assume that k/Q is a finite Galois extension of global fields, and that S is a k/Q-closed set of primes of k (not necessarily nonempty or containing S_∞).

Let $\mathfrak{p}$ be a prime of the global field k. We let $\mathcal{G}_\mathfrak{p} = \mathcal{G}_\mathfrak{p}(k)$ and $\mathcal{T}_\mathfrak{p} = \mathcal{T}_\mathfrak{p}(k)$. Recall that for a $\mathcal{G}_\mathfrak{p}$-module A of order not divisible by $\mathrm{char}(k)$, the unramified cohomology group is defined to be

$$H^i_{nr}(k_\mathfrak{p},A) = \mathrm{im}(H^i(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}, A^{\mathcal{T}_\mathfrak{p}}) \to H^i(k_\mathfrak{p},A)),$$

where the map is the inflation map. Then we consider the following homomorphism of cohomology groups:

$$\prod_{\mathfrak{p}\in S}H^1(k_\mathfrak{p},A)\times\prod_{\mathfrak{p}\notin S}H^1_{nr}(k_\mathfrak{p},A)\hookrightarrow\prod_{\mathfrak{p}}H^1(k_\mathfrak{p},A)\xrightarrow{\sim}\prod_{\mathfrak{p}}H^1(k_\mathfrak{p},A')^\vee\to H^1(k,A')^\vee. \tag{8-1}$$

The first map is the natural embedding of cohomology groups. The second map is an isomorphism because of the local Tate duality theorem [Neukirch et al. 2008, Theorems 7.2.6 and 7.2.17]. The last map is defined by the Pontryagin dual of the product of restriction map $H^1(k,A')\to H^1(k_\mathfrak{p},A')$ for each prime $\mathfrak{p}$ of k. In particular, the restriction of the composition of the last two maps in (8-1) to the restricted product is the map

$$\prod_{\mathfrak{p}}{}'H^1(k_\mathfrak{p},A)\to H^1(k,A')^\vee$$

used in the long exact sequence of Poitou–Tate [Neukirch et al. 2008, (8.6.10)(i)]. Here the restricted product $\prod'_\mathfrak{p}H^1(k_\mathfrak{p},A)$ is the subgroup of $\prod_\mathfrak{p}H^1(k_\mathfrak{p},A)$ consisting of all $(x_\mathfrak{p})$ such that $x_\mathfrak{p}\in H^1_{nr}(k_\mathfrak{p},A)$ for almost all $\mathfrak{p}$.

Definition 8.1. For a global field k, a set S of primes of k, and $A\in\mathrm{Mod}(G_k)$ of order not divisible by $\mathrm{char}(k)$, we define

$$Б_S(k,A) = \mathrm{coker}\Big(\prod_{\mathfrak{p}\in S}H^1(k_\mathfrak{p},A)\times\prod_{\mathfrak{p}\notin S}H^1_{nr}(k_\mathfrak{p},A)\to H^1(k,A')^\vee\Big),$$

where the map is the composition of maps in (8-1).

Remark 8.2. (1) When A is a finite G_Q-module and S is k/Q-closed, the maps in (8-1) are compatible with the conjugation action of $\mathrm{Gal}(k/Q)$ on cohomology groups, so $\text{Б}_S(k, A)$ is naturally a $\mathrm{Gal}(k/Q)$-module.

(2) Using the language of the Selmer groups, $\text{Б}_S(k, A)$ is the Pontryagin dual of the Selmer group of the Galois module A' consisting of elements of $H^1(k, A')$ that have images inside the subgroup

$$\prod_{\mathfrak{p}\in S} 1 \times \prod_{\mathfrak{p}\notin S} \ker(H^1(k_\mathfrak{p}, A') \to H^1_{nr}(k_\mathfrak{p}, A)^\vee) \subset \prod_{\mathfrak{p}} H^1(k_\mathfrak{p}, A').$$

under the product of local restriction maps.

Proposition 8.3. *If $A = \mathbb{F}_\ell$ is the trivial G_k-module with $\ell \neq \mathrm{char}(k)$, then $\text{Б}_S(k, \mathbb{F}_\ell)$ is the Pontryagin dual of the Kummer group*

$$V_S(k, \ell) = \ker\Big(k^\times/k^{\times\ell} \to \prod_{\mathfrak{p}\in S} k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times\ell} \times \prod_{\mathfrak{p}\notin S} k_\mathfrak{p}^\times/U_\mathfrak{p} k_\mathfrak{p}^{\times\ell}\Big).$$

Proof. By the class field theory, we have

$$H^1(k, \mu_\ell) \cong k^\times/k^{\times\ell}, \quad H^1(k_\mathfrak{p}, \mu_\ell) \cong k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times\ell}, \quad \text{and} \quad H^1_{nr}(k_\mathfrak{p}, \mathbb{F}_\ell)^\vee \cong k_\mathfrak{p}^\times/U_\mathfrak{p} k_\mathfrak{p}^{\times\ell}.$$

Then the proposition follows directly from Definition 8.1. □

The following lemma is a generalization of [Neukirch et al. 2008, Lemma(10.7.4)(i)]

Lemma 8.4. *Let k/Q be a finite Galois extension of global fields, $T \supseteq S$ be k/Q-closed sets of primes of k, and $A \in \mathrm{Mod}(\mathrm{Gal}(k_S/Q))$ be of order not divisible by* $\mathrm{char}(k)$. *Then we have the following exact sequence that is compatible with the conjugation by* $\mathrm{Gal}(k/Q)$:

$$H^1(G_S(k), A) \hookrightarrow H^1(G_T(k), A) \to \bigoplus_{\mathfrak{p}\in T\setminus S} H^1(\mathcal{T}_\mathfrak{p}(k), A)^{\mathcal{G}_\mathfrak{p}(k)} \to \text{Б}_S(k, A) \twoheadrightarrow \text{Б}_T(k, A).$$

Proof. We consider the commutative diagram

$$\begin{array}{ccccc}
 & & Ш^1(k, A) & & \\
 & \swarrow & \downarrow & & \\
H^1(G_S, A) & \hookrightarrow & H^1(k, A) & \to & H^1(G_{k_S}, A)^{G_S} \\
 & & \downarrow & & \downarrow \\
\prod'_{\mathfrak{p}\in S} H^1(k_\mathfrak{p}, A) \times \prod_{\mathfrak{p}\notin S} H^1_{nr}(k_\mathfrak{p}, A) & \hookrightarrow & \prod'_{\mathfrak{p}} H^1(k_\mathfrak{p}, A) & \twoheadrightarrow & \bigoplus_{\mathfrak{p}\notin S} H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}} \\
\downarrow & & \downarrow & & \\
H^1(k, A')^\vee & = & H^1(k, A')^\vee & & \\
\downarrow & & \downarrow & & \\
\text{Б}_S(k, A) & & Ш^2(k, A') & &
\end{array}$$

The exactnesses of the second row and the third row follow from the Hochschild–Serre spectral sequence, and last arrow in the third row is surjective because of the fact that $H^2_{nr}(\mathcal{G}_\mathfrak{p}, A) = 0$ as $\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p} \simeq \widehat{\mathbb{Z}}$ when $\mathfrak{p}$

is nonarchimedean and 1 when $\mathfrak{p}$ is archimedean. The exact sequence of the first column follows from the definition of $Ш_S(k, A)$, and the second column follows from the long exact sequence of Poitou–Tate [Neukirch et al. 2008, (8.6.10)]. The right vertical map is injective since G_{k_S} is generated by the inertia groups of primes outside S.

We consider the map $H^1(k, A) \to \bigoplus_{\mathfrak{p}\notin S} H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}}$ in the diagonal of the square diagram on the right. Since $H^1(G_S, A)$ is the kernel of this map and $Ш^1(k, A)$ is contained in this kernel, the top dashed arrow exists and is injective. Then by diagram chasing, we have an exact sequence

$$Ш^1(k, A) \hookrightarrow H^1(G_S, A) \to \prod_{\mathfrak{p}\in S}{}' H^1(k_\mathfrak{p}, A) \times \prod_{\mathfrak{p}\notin S} H^1_{nr}(k_\mathfrak{p}, A) \to H^1(k, A')^\vee \twoheadrightarrow Ь_S(k, A). \tag{8-2}$$

We apply the snake lemma to the diagram

$$\begin{array}{ccc}
\prod_{\mathfrak{p}\in S}{}' H^1(k_\mathfrak{p}, A) \times \prod_{\mathfrak{p}\notin S} H^1_{nr}(k_\mathfrak{p}, A) & \longrightarrow & H^1(k, A')^\vee \\
\big\downarrow & & \big\| \\
\prod_{\mathfrak{p}\in T}{}' H^1(k_\mathfrak{p}, A) \times \prod_{\mathfrak{p}\notin T} H^1_{nr}(k_\mathfrak{p}, A) & \longrightarrow & H^1(k, A')^\vee \\
\big\downarrow & & \\
\bigoplus_{\mathfrak{p}\in T\setminus S} H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}} & &
\end{array}$$

where the horizontal map above is from (8-2), and we obtain the exact sequence

$$\frac{H^1(G_S, A)}{Ш^1(k, A)} \hookrightarrow \frac{H^1(G_T, A)}{Ш^1(k, A)} \to \bigoplus_{\mathfrak{p}\in T\setminus S} H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}} \to Ь_S(k, A) \twoheadrightarrow Ь_T(k, A).$$

Note that the inflation map $H^1(G_S, A) \hookrightarrow H^1(G_T, A)$ maps the submodule $Ш^1(k, A)$ to itself, because $Ш^1(k, A)$ is the kernel of $H^1(G_*, A) \to \prod_\mathfrak{p} H^1(k_\mathfrak{p}, A)$ for $* = S, T$. Therefore we proved the exact sequence in the lemma, and it is naturally compatible with the conjugation action by $\mathrm{Gal}(k/Q)$. □

Proposition 8.5. *Let k/Q be a finite Galois extension of global fields and S a k/Q-closed set of primes of k. Then for any $A \in \mathrm{Mod}(\mathrm{Gal}(k_S/Q))$ of order not divisible by* $\mathrm{char}(k)$, *we have the following inequality of elements in $K_0'(\mathrm{Gal}(k/Q))$:*

$$[Ш^2_S(k, A)] \le [Ь_S(k, A)].$$

Proof. We consider the commutative diagram

$$\begin{array}{ccccccc}
H^1(G_S, A) \hookrightarrow H^1(k, A) \to H^1(k_S, A)^{G_S} & \xrightarrow{\alpha} & H^2(G_S, A) & \xrightarrow{\beta} & H^2(k, A) \\
& & \big\downarrow{\scriptstyle \rho_S} & & \big\downarrow{\scriptstyle \rho} \\
& & \prod_{\mathfrak{p}\in S} H^2(k_\mathfrak{p}, A) & \hookrightarrow & \prod_\mathfrak{p} H^2(k_\mathfrak{p}, A)
\end{array} \tag{8-3}$$

where the first row is the Hochschild–Serre long exact sequence of $1 \to G_{k_S} \to G_k \to G_S \to 1$. Because $\operatorname{im}\alpha = \ker\beta \subseteq \ker\rho\circ\beta = \ker\rho_S = Ш^2_S(k, A)$, we have an exact sequence

$$H^1(G_S, A) \hookrightarrow H^1(k, A) \to H^1(G_{k_S}, A)^{G_S} \to Ш^2_S(k, A) \twoheadrightarrow \beta(Ш^2_S(k, A)).$$

Comparing this exact sequence to Lemma 8.4 using $T = \{\text{all primes}\}$, we have

$$\begin{array}{ccccccc} H^1(k, A) & \longrightarrow & H^1(k_S, A)^{G_S} & \longrightarrow & Ш^2_S(k, A) & \twoheadrightarrow & \beta(Ш^2_S(k, A)) \\ \| & & \downarrow & & & & \\ H^1(k, A) & \longrightarrow & \bigoplus_{\mathfrak{p}\notin S} H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}} & \longrightarrow & Б_S(k, A) & \twoheadrightarrow & Б_{\{\text{all primes}\}}(k, A) \end{array}$$

So by the vertical injection above, we have $\ker\beta \hookrightarrow N := \ker(Б_S(k, A) \to Б_{\{\text{all primes}\}}(k, A))$. By the diagram in (8-3), we have $\beta(\ker\rho_S) \subseteq \ker\rho$, which means $\beta(Ш^2_S(k, A)) \subseteq Ш^2(k, A)$. Also, note that by Definition 8.1 and the Poitou–Tate duality we have $Б_{\{\text{all primes}\}}(k, A) = Ш^1(k, A')^\vee \cong Ш^2(k, A)$. Then we consider the two short exact sequence

$$0 \to \ker\beta \to Ш^2_S(k, A) \to \beta(Ш^2_S(k, A)) \to 0,$$
$$0 \to N \to Б_S(k, A) \to Б_{\{\text{all primes}\}}(k, A) \to 0,$$

Because $\ker\beta \hookrightarrow N$, $\beta(Ш^2_S(k, A)) \hookrightarrow Б_{\{\text{all primes}\}}(k, A)$ and every map respects the conjugation action by $\mathrm{Gal}(k/Q)$, we have the desired inequality $[Ш^2_S(k, A)] \le [Б_S(k, A)]$. □

Remark 8.6. When $A = \mathbb{F}_\ell$ is the trivial module, then $Б_{\{\text{all primes}\}}(k, \mathbb{F}_\ell)$ vanishes [Neukirch et al. 2008, Proposition 9.1.12(ii)], so there is an embedding $Ш^2_S(k, \mathbb{F}_\ell) \hookrightarrow Б_S(k, \mathbb{F}_\ell)$. However, for an arbitrary A, Proposition 8.5 does not give such an embedding.

Lemma 8.7. *Let k be a global field and S a set of primes of k containing $S_\infty(k)$. Then for any $A \in \mathrm{Mod}_S(G_S(k))$ of order not divisible by* $\mathrm{char}(k)$, *we have* $Ш^1_S(k, A') \cong Б_S(k, A)^\vee$.

Proof. We consider the commutative diagram

$$\begin{array}{ccc} \prod_\mathfrak{p} H^1(k_\mathfrak{p}, A') & \longrightarrow & \prod_{\mathfrak{p}\in S} H^1(k_\mathfrak{p}, A') \times \prod_{\mathfrak{p}\notin S} H^1(\mathcal{T}_\mathfrak{p}, A')^{\mathcal{G}_\mathfrak{p}} \\ \downarrow\sim & & \downarrow\sim \\ \prod_\mathfrak{p} H^1(k_\mathfrak{p}, A)^\vee & \longrightarrow & \prod_{\mathfrak{p}\in S} H^1(k_\mathfrak{p}, A)^\vee \times \prod_{\mathfrak{p}\notin S} H^1_{nr}(k_\mathfrak{p}, A)^\vee \end{array}$$

where the two vertical arrows are isomorphisms by the Tate local duality theorem and its consequence that $H^1(\mathcal{T}_\mathfrak{p}, A')^{\mathcal{G}_\mathfrak{p}} \xrightarrow{\sim} H^1_{nr}(k_\mathfrak{p}, A)^\vee$ when A is unramified at $\mathfrak{p}$ and $\#\mathrm{tor}(A)$ is prime to the characteristic

of the residue field of $k_\mathfrak{p}$ (see the proof of [Neukirch et al. 2008, Theorem 7.2.15]). Then by definition, we have

$$\begin{aligned}\text{Б}_S(k, A)^\vee &= \ker\Big(H^1(k, A') \to \prod_{\mathfrak{p}\in S} H^1(k_\mathfrak{p}, A)^\vee \times \prod_{\mathfrak{p}\notin S} H^1_{nr}(k_\mathfrak{p}, A)^\vee\Big)\\ &= \ker\Big(H^1(k, A') \to \prod_{\mathfrak{p}\in S} H^1(k_\mathfrak{p}, A') \times \prod_{\mathfrak{p}\notin S} H^1(\mathcal{T}_\mathfrak{p}, A')^{\mathcal{G}_p}\Big).\end{aligned}$$

So by applying the snake lemma to the commutative diagram

$$\begin{array}{ccccc}
Ш^1_S(k, A') & \hookrightarrow & H^1(G_S, A') & \longrightarrow & \prod_{\mathfrak{p}\in S} H^1(k_\mathfrak{p}, A') \\
 & & \downarrow & & \downarrow \\
\text{Б}_S(k, A)^\vee & \hookrightarrow & H^1(k, A') & \longrightarrow & \prod_{\mathfrak{p}\in S} H^1(k_\mathfrak{p}, A') \times \prod_{\mathfrak{p}\notin S} H^1(\mathcal{T}_\mathfrak{p}, A')^{\mathcal{G}_\mathfrak{p}} \\
 & & \downarrow & & \downarrow \\
 & & H^1(k_S, A')^{G_S} & \hookrightarrow & \prod_{\mathfrak{p}\notin S} H^1(\mathcal{T}_\mathfrak{p}, A')^{\mathcal{G}_\mathfrak{p}}
\end{array}$$

we obtain the desired isomorphism $Ш^1_S(k, A') \xrightarrow{\sim} \text{Б}_S(k, A)^\vee$. □

Corollary 8.8. *For any set S of primes of a global field k and any $A \in \mathrm{Mod}(G_S(k))$ of order not divisible by* $\mathrm{char}(k)$, *we have that $\text{Б}_S(k, A)$ is finite.*

Proof. Define $T = S \cup S_\infty(k) \cup S_{|A|}(k)$. By applying Lemma 8.4, we have

$$\bigoplus_{\mathfrak{p}\in T\setminus S} H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}} \to \text{Б}_S(k, A) \twoheadrightarrow \text{Б}_T(k, A). \tag{8-4}$$

Since $A \in \mathrm{Mod}_T(G_T)$, by Lemma 8.7 and [Neukirch et al. 2008, Theorem 8.6.4], we have that $\text{Б}_T(k, A)^\vee \cong Ш^1_T(k, A')$ is finite. Also note that $H^1(k_\mathfrak{p}, A)$ is finite [Neukirch et al. 2008, Theorem 7.1.8(iv)] and $H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}}$ is a quotient of $H^1(k_\mathfrak{p}, A)$. Thus, the direct product $\prod_{\mathfrak{p}\in T\setminus S} H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}}$ is finite, and hence the corollary follows by (8-4). □

9. Determination of $\delta_{k/Q,S}(A)$

Definition 9.1. Let k/Q be a finite Galois extension of global fields, S a finite k/Q-closed set of primes of k, $\ell \neq \mathrm{char}(k)$ a prime integer not dividing $[k : Q]$, and $A \in \mathrm{Mod}_\ell(\mathrm{Gal}(k_S/Q))$. We define

$$\delta_{k/Q,S}(A) = \dim_{\mathbb{F}_\ell} H^2(G_S(k), A)^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell} H^1(G_S(k), A)^{\mathrm{Gal}(k/Q)}.$$

We will use the notation and assumption in Definition 9.1 throughout this section. When $\ell \in \mathbb{N}(S)$ and $S_\infty(k) \subset S$, by Theorem 7.1, we have our first case for which $\delta_{k/Q,S}(A)$ can be determined.

Proposition 9.2. *Assume $\ell \in \mathbb{N}(S)$ and $S \supset S_\infty(k)$ is nonempty. Then*

$$\delta_{k/Q,S}(A) = \sum_{v\in S_\infty(Q)} \big(\dim_{\mathbb{F}_\ell} \widehat{H}^0(Q_v, A') - \dim_{\mathbb{F}_\ell} H^0(Q_v, A')\big) - \dim_{\mathbb{F}_\ell} A^{\mathrm{Gal}(k_S/Q)}.$$

So in this section, we will consider the cases that are not covered by Proposition 9.2. In Section 9.1, we will deal with the case that Q is a function field and $S = \varnothing$, and obtain a formula for $\delta_{k/Q,\varnothing}(A)$ (Proposition 9.3). Then in Section 9.2, we will give an upper bound of $\delta_{k/Q,S}(A)$ when k is a number field with $S_\ell(k) \cup S_\infty(k) \not\subset S$ (Proposition 9.4). In Section 9.2, we will prove Theorem 1.2 by setting $k = Q$ and applying Propositions 9.2 and 9.4.

9.1. *Function field case with $S = \varnothing$.*

Proposition 9.3. *Assume k and Q are function fields. Let $g = g(k)$ be the genus of the curve corresponding to k.*

(1) *If $g = 0$, then $\delta_{k/Q,\varnothing}(A) = -\dim_{\mathbb{F}_\ell} A_{\mathrm{Gal}(k_\varnothing/Q)}$.*

(2) *If $g > 0$, then $\delta_{k/Q,\varnothing}(A) = \dim_{\mathbb{F}_\ell}(A')^{\mathrm{Gal}(k_\varnothing/Q)} - \dim_{\mathbb{F}_\ell} A^{\mathrm{Gal}(k_\varnothing/Q)}$.*

Proof. When $g = 0$, we have $G_\varnothing(k) \cong \widehat{\mathbb{Z}}$ by [Neukirch et al. 2008, Corollary 10.1.3(i)]. So $H^2(G_\varnothing, A) = 0$ as $\widehat{\mathbb{Z}}$ has cohomological dimension 1 and $H^1(G_\varnothing, A) \cong A_{G_\varnothing}$ by [Neukirch et al. 2008, Proposition 1.7.7(i)]. Then we see that

$$\delta_{k/Q,\varnothing}(A) = -\dim_{\mathbb{F}_\ell}(A_{G_\varnothing})^{\mathrm{Gal}(k/Q)} = -\dim_{\mathbb{F}_\ell}(A_{G_\varnothing})_{\mathrm{Gal}(k/Q)} = -\dim_{\mathbb{F}_\ell} A_{\mathrm{Gal}(k_\varnothing/Q)},$$

where the second equality uses $\ell \nmid [k : Q]$, so we proved (1).

For the rest, we assume $g > 0$. Let κ be the finite field of constants of k and $C = \mathrm{Gal}(\bar{\kappa}/\kappa) \cong \widehat{\mathbb{Z}}$. Then there exists an exact sequence, for each j,

$$H^j(G_\varnothing(k\bar{\kappa}), A)^C \hookrightarrow H^j(G_\varnothing(k\bar{\kappa}), A) \xrightarrow{\mathrm{Frob}-1} H^j(G_\varnothing(k\bar{\kappa}), A) \twoheadrightarrow H^j(G_\varnothing(k\bar{\kappa}), A)_C, \tag{9-1}$$

where Frob is the Frobenius action on the cohomology groups defined by conjugation. Note that $\mathrm{Gal}(k\bar{\kappa}/Q)$ acts on cohomology groups in (9-1), and

$$1 \to C \cong \mathrm{Gal}(k\bar{\kappa}/k) \to \mathrm{Gal}(k\bar{\kappa}/Q) \to \mathrm{Gal}(k/Q) \to 1$$

is a central group extension because $\mathrm{Gal}(k/Q)$ acts trivially on the generator Frob of C. So the map Frob -1 in (9-1) respects the $\mathrm{Gal}(k\bar{\kappa}/Q)$ actions. It follows that $H^j(G_\varnothing(k\bar{\kappa}), A)^C$ and $H^j(G_\varnothing(k\bar{\kappa}), A)_C$ are in the same class in $K_0'(\mathbb{F}_\ell[\mathrm{Gal}(k\bar{\kappa}/Q)])$, and hence they are in the same class in $K_0'(\mathbb{F}_\ell[\mathrm{Gal}(k/Q)])$. Because $\ell \nmid [k : Q]$ implies $\mathbb{F}_\ell[\mathrm{Gal}(k/Q)]$ is semisimple, we have

$$H^j(G_\varnothing(k\bar{\kappa}), A)^C \simeq H^j(G_\varnothing(k\bar{\kappa}), A)_C \tag{9-2}$$

as $\mathrm{Gal}(k/Q)$-modules. Therefore, as C is cyclic,

$$\begin{aligned} H^1(C, H^j(G_\varnothing(k\bar{\kappa}), A)) &\simeq \widehat{H}^{-1}(C, H^j(G_\varnothing(k\bar{\kappa}), A)) \simeq H^j(G_\varnothing(k\bar{\kappa}), A)_C \\ &\simeq H^0(C, H^j(G_\varnothing(k\bar{\kappa}), A)) \end{aligned} \tag{9-3}$$

as $\mathrm{Gal}(k/Q)$-modules. Then we consider the Hochschild–Serre spectral sequence

$$E_2^{ij} = H^i(C, H^j(G_\varnothing(k\bar{\kappa}), A)) \Rightarrow H^{i+j}(G_\varnothing(k), A).$$

As C has cohomological dimension 1, $E_2^{ij} = 0$ for each $i > 1$, and hence by [Neukirch et al. 2008, Lemma 2.1.3(ii)] we have the following exact sequence for every $j \geq 1$:

$$H^1(C, H^{j-1}(G_\varnothing(k\bar{k}), A)) \hookrightarrow H^j(G_\varnothing(k), A) \twoheadrightarrow H^0(C, H^j(G_\varnothing(k\bar{k}), A)). \tag{9-4}$$

Note that $G_\varnothing(k)$ has strict cohomological ℓ-dimension 3 by [Neukirch et al. 2008, Corollary 10.1.3(ii)]. Then as $\ell \nmid [k : Q]$, taking $\mathrm{Gal}(k/Q)$-invariants is exact on (9-4), and by computing the alternating sum of (9-4) for $j = 1, 2, 3$ and applying (9-3), we have

$$\begin{aligned}\sum_{j=1}^{3} (-1)^j \dim_{\mathbb{F}_\ell} H^j(G_\varnothing(k), A)^{\mathrm{Gal}(k/Q)} &= -\dim_{\mathbb{F}_\ell} H^1(C, H^0(G_\varnothing(k\bar{k}), A))^{\mathrm{Gal}(k/Q)} \\ &= -\dim_{\mathbb{F}_\ell} H^0(C, H^0(G_\varnothing(k\bar{k}), A))^{\mathrm{Gal}(k/Q)} \\ &= -\dim_{\mathbb{F}_\ell} H^0(\mathrm{Gal}(k_\varnothing/Q), A).\end{aligned}$$

Also, [Neukirch et al. 2008, Corollary 10.1.3(ii)] shows that $G_\varnothing(k)$ is a Poincaré group of dimension 3 with dualizing module μ, so we have a functorial isomorphism $H^3(G_\varnothing(k), A) \cong H^0(G_\varnothing(k), A')^\vee$. Combining the above computations, we see that

$$\begin{aligned}\delta_{k/Q,\varnothing}(A) &= \dim_{\mathbb{F}_\ell}(H^0(G_\varnothing(k), A')^\vee)^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell} H^0(\mathrm{Gal}(k_\varnothing/Q), A) \\ &= \dim_{\mathbb{F}_\ell} H^0(G_\varnothing(k), A')^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell} H^0(\mathrm{Gal}(k_\varnothing/Q), A) \\ &= \dim_{\mathbb{F}_\ell}(A')^{\mathrm{Gal}(k_\varnothing/Q)} - \dim_{\mathbb{F}_\ell} A^{\mathrm{Gal}(k_\varnothing/Q)},\end{aligned}$$

where the second equality is because the $\mathrm{Gal}(k/Q)$-invariants of M and $M^\vee$ have the same dimension for any $M \in \mathrm{Mod}_\ell(\mathrm{Gal}(k/Q))$. □

9.2. *Number field case with $S_\ell \cup S_\infty \not\subset S$.*

Proposition 9.4. *Assume k and Q are number fields. Let $T = S \cup S_\ell(k) \cup S_\infty(k)$. Then*

$$\delta_{k/Q,S}(A) \leq \log_\ell(\chi_{k/Q,T}(A)) + \dim_{\mathbb{F}_\ell}(A')^{\mathrm{Gal}(k_T/Q)} - \dim_{\mathbb{F}_\ell} A^{\mathrm{Gal}(k_S/Q)} + \epsilon_{k/Q,S}(A),$$

where $\epsilon_{k/Q,S}(A) = -\sum_{v\in I} \log_\ell \|\#A\|_v$[1] *with*

$$I = \{v \in S_\ell(Q) \text{ such that } S_v(k) \not\subset S\}.$$

In particular, when $S = \varnothing$, the equality holds if and only if $Ш^2_\varnothing(k, A)$ and $Б_\varnothing(k, A)$ are in the same class of $K_0'(\mathbb{F}_\ell[\mathrm{Gal}(k/Q)])$.

Remark 9.5. For an arbitrary S, the equality holds if and only if the equalities in (9-5) hold. So when $S \neq \varnothing$, if the equality holds then $[Ш^2_\varnothing(k, A)] = [Б_\varnothing(k, A)]$, but the converse is false.

Proof. First of all, by definition of $Ш^2_S$ and Proposition 8.5, we have the following inequalities of elements in $K_0'(\mathbb{F}_\ell[\mathrm{Gal}(k/Q)])$:

$$[H^2(G_S, A)] \leq [Ш^2_S(k, A)] + \Big[\bigoplus_{\mathfrak{p}\in S} H^2(k_\mathfrak{p}, A)\Big] \leq [Б_S(k, A)] + \Big[\bigoplus_{\mathfrak{p}\in S} H^2(k_\mathfrak{p}, A)\Big]. \tag{9-5}$$

[1] $\|x\|_v = q^{-\mathrm{ord}_v(x)}$ where q is the cardinality of the residue field of v and ord_v is the additive valuation with value group $\mathbb{Z}$.

By applying Lemma 8.4, we have

$$[\text{Ш}_S(k,A)]-[H^1(G_S,A)]=[\text{Ш}_T(k,A)]-[H^1(G_T,A)]+\Big[\bigoplus_{\mathfrak{p}\in T\setminus S}H^1(\mathcal{T}_\mathfrak{p},A)^{\mathcal{G}_\mathfrak{p}}\Big]. \tag{9-6}$$

Since T contains $S_\ell(k)\cup S_\infty(k)$, it follows that $[\text{Ш}_T(k,A)]=[\text{Ш}^2_T(k,A)]$ by Lemma 8.7 and the Poitou–Tate duality theorem. Also, note that the long exact sequence of Poitou–Tate [Neukirch et al. 2008, (8.6.10)] induces an exact sequence

$$\text{Ш}^2_T(k,A)\hookrightarrow H^2(G_T,A)\to\bigoplus_{\mathfrak{p}\in T}H^2(k_\mathfrak{p},A)\twoheadrightarrow H^0(G_T,A')^\vee.$$

Therefore

$$[\text{Ш}_T(k,A)]=[H^2(G_T,A)]+[H^0(G_T,A')^\vee]-\Big[\bigoplus_{\mathfrak{p}\in T}H^2(k_\mathfrak{p},A)\Big]. \tag{9-7}$$

Combining (9-5), (9-6) and (9-7), we have

$$\begin{aligned}&[H^2(G_S,A)]-[H^1(G_S,A)]\\&\quad\le[H^2(G_T,A)]-[H^1(G_T,A)]+[H^0(G_T,A')^\vee]+\Big[\bigoplus_{\mathfrak{p}\in T\setminus S}H^1(\mathcal{T}_\mathfrak{p},A)^{\mathcal{G}_\mathfrak{p}}\Big]-\Big[\bigoplus_{\mathfrak{p}\in T\setminus S}H^2(k_\mathfrak{p},A)\Big].\end{aligned}$$

The dimension of $\mathrm{Gal}(k/Q)$-invariants of the left-hand side above is $\delta_{k/Q,S}(A)$. On the right-hand side, the dimension of $\mathrm{Gal}(k/Q)$-invariants of $[H^2(G_T,A)]-[H^1(G_T,A)]$ is

$$\log_\ell(\chi_{k/Q,T}(A))-\dim_{\mathbb{F}_\ell}H^0(G_T,A)^{\mathrm{Gal}(k/Q)}=\log_\ell(\chi_{k/Q,T}(A))-\dim_{\mathbb{F}_\ell}A^{\mathrm{Gal}(k_S/Q)}$$

by the definition of $\chi_{k/Q,T}$ and the assumption that A is a $\mathrm{Gal}(k_S/Q)$-module. Also,

$$\dim_{\mathbb{F}_\ell}(H^0(G_T,A')^\vee)^{\mathrm{Gal}(k/Q)}=\dim_{\mathbb{F}_\ell}H^0(G_T,A')^{\mathrm{Gal}(k/Q)}=\dim_{\mathbb{F}_\ell}(A')^{\mathrm{Gal}(k_T/Q)}.$$

So to prove the inequality in the proposition, it suffices to show

$$\epsilon_{k/Q,S}(A)=\dim_{\mathbb{F}_\ell}\Big(\bigoplus_{\mathfrak{p}\in T\setminus S}H^1(\mathcal{T}_\mathfrak{p},A)^{\mathcal{G}_\mathfrak{p}}\Big)^{\mathrm{Gal}(k/Q)}-\dim_{\mathbb{F}_\ell}\Big(\bigoplus_{\mathfrak{p}\in T\setminus S}H^2(k_\mathfrak{p},A)\Big)^{\mathrm{Gal}(k/Q)}. \tag{9-8}$$

We first consider $v\in S_\infty(Q)$ such that $S_v(k)\not\subset S$. Since $\mathcal{T}_\mathfrak{p}(k)=\mathcal{G}_\mathfrak{p}(k)$, we know that $H^1(\mathcal{T}_\mathfrak{p},A)^{\mathcal{G}_\mathfrak{p}}=H^1(k_\mathfrak{p},A)$ for each $\mathfrak{p}\in S_v(k)$. For $i=1,2$, we have

$$\Big(\bigoplus_{\mathfrak{p}\in S_v(k)}H^i(k_\mathfrak{p},A)\Big)^{\mathrm{Gal}(k/Q)}=\big(\mathrm{Ind}_{\mathrm{Gal}(k/Q)}^{\mathrm{Gal}_\mathfrak{p}(k/Q)}H^i(k_\mathfrak{p},A)\big)^{\mathrm{Gal}(k/Q)}=H^i(k_\mathfrak{p},A)^{\mathrm{Gal}_\mathfrak{p}(k/Q)}=H^i(Q_v,A),$$

where the second equality uses Shapiro's lemma and the last one follows by the assumption that $\ell\nmid[k:Q]$ and the same argument for (7-15). Therefore

$$\begin{aligned}\dim_{\mathbb{F}_\ell}\Big(\bigoplus_{\mathfrak{p}\in S_v(k)}H^1(\mathcal{T}_\mathfrak{p},A)^{\mathcal{G}_\mathfrak{p}}\Big)^{\mathrm{Gal}(k/Q)}-\dim_{\mathbb{F}_\ell}\Big(\bigoplus_{\mathfrak{p}\in S_v(k)}H^2(k_\mathfrak{p},A)\Big)^{\mathrm{Gal}(k/Q)}\\=\dim_{\mathbb{F}_\ell}H^1(Q_v,A)-\dim_{\mathbb{F}_\ell}H^2(Q_v,A),\end{aligned}$$

which always equals 0 since Q_v is a cyclic group [Neukirch et al. 2008, Proposition 1.7.6].

Finally, we consider $v \in S_\ell(Q)$ such that $S_v(k) \not\subset S$. Because $\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}$ is procyclic, we have that $H^1(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}, A) \cong A_{\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}}$; and by the same argument from (9-1) to (9-2), we have an isomorphism $H^1(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}, A) \simeq A^{\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}} = A^{\mathcal{G}_\mathfrak{p}}$ that is compatible with the conjugation action by $\mathrm{Gal}_\mathfrak{p}(k/Q)$. So we see that

$$\begin{aligned}\dim_{\mathbb{F}_\ell}\Big(\bigoplus_{\mathfrak{p}\in S_\mathfrak{p}(k)} H^1(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}, A)\Big)^{\mathrm{Gal}(k/Q)} &= \dim_{\mathbb{F}_\ell}\big(\mathrm{Ind}_{\mathrm{Gal}(k/Q)}^{\mathrm{Gal}_\mathfrak{p}(k/Q)} H^1(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}, A)\big)^{\mathrm{Gal}(k/Q)}\\ &= \dim_{\mathbb{F}_\ell} H^1(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}, A)^{\mathrm{Gal}_\mathfrak{p}(k/Q)}\\ &= \dim_{\mathbb{F}_\ell} A^{\mathcal{G}_\mathfrak{p}(Q)}. \end{aligned} \tag{9-9}$$

Therefore, we compute

$$\begin{aligned}&\dim_{\mathbb{F}_\ell}\Big(\bigoplus_{\mathfrak{p}\in S_v(k)} H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}}\Big)^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell}\Big(\bigoplus_{\mathfrak{p}\in S_v(k)} H^2(k_\mathfrak{p}, A)\Big)^{\mathrm{Gal}(k/Q)}\\ &\quad= \dim_{\mathbb{F}_\ell}\Big(\bigoplus_{\mathfrak{p}\in S_v(k)} H^1(k_\mathfrak{p}, A)\Big)^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell}\Big(\bigoplus_{\mathfrak{p}\in S_v(k)} H^2(k_\mathfrak{p}, A)\Big)^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell} A^{\mathcal{G}_v(Q)}\\ &\quad= \dim_{\mathbb{F}_\ell} H^1(k_\mathfrak{p}, A)^{\mathrm{Gal}_\mathfrak{p}(k/Q)} - \dim_{\mathbb{F}_\ell} H^2(k_\mathfrak{p}, A)^{\mathrm{Gal}_\mathfrak{p}(k/Q)} - \dim_{\mathbb{F}_\ell} A^{\mathcal{G}_v(Q)}\\ &\quad= \dim_{\mathbb{F}_\ell} H^1(Q_v, A) - \dim_{\mathbb{F}_\ell} H^2(Q_v, A) - \dim_{\mathbb{F}_\ell} A^{\mathcal{G}_v(Q)}\\ &\quad= -\log_\ell \|\#A\|_v.\end{aligned}$$

The first equality above uses (9-9) and the exact sequence $H^1(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}, A) \hookrightarrow H^1(k_\mathfrak{p}, A) \twoheadrightarrow H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}}$, the second uses the Shapiro's lemma, the third uses the assumption that $\ell \nmid [k : Q]$, and the last uses the Tate's local Euler–Poincaré characteristic formula [Neukirch et al. 2008, Theorem 7.3.1]. We have proved (9-8).

When $S = \varnothing$, we have $Ш^2_\varnothing(k, A) = H^2(G_\varnothing, A)$, so the first inequality in (9-5) is an equality, and hence we have the last statement in the proposition. □

Proof of Theorem 1.2. We apply the above results to the case $k = Q$. Let $G = G_S(k)$. Let A be a finite simple G-module and ℓ denote the exponent of A. Since $\widehat{H}^0(k_\mathfrak{p}, A')$ is naturally a quotient of $H^0(k_\mathfrak{p}, A')$ for each $\mathfrak{p} \in S_\infty(k)$, we have $\log_\ell \chi_{k/k,T}(A) \le 0$ for $T = S \cup S_\ell(k) \cup S_\infty(k)$. When $S \supset S_\ell(k) \cup S_\infty(k)$, applying Proposition 9.2 to the case $k = Q$, we have $\delta_{k/k,S}(A) \le 0$. It follows by definition of $\epsilon_{k/k,S}(A)$ in Proposition 9.4 that $\epsilon_{k/k,S}(A) \le [k : \mathbb{Q}] \dim_{\mathbb{F}_\ell} A$. Also, note that, when $S \not\supset S_\ell(k) \cup S_\infty(k)$ and $A \not\simeq \mu_\ell$, we have $\dim_{\mathbb{F}_\ell}(A')^{G_T(k)} - \dim_{\mathbb{F}_\ell} A^{G_S(k)} \le 0$. When $S \not\supset S_\ell(k) \cup S_\infty(k)$ and $A = \mu_\ell$ (assume $\mu_\ell \not\simeq \mathbb{F}_\ell$), we have $\dim_{\mathbb{F}_\ell}(A')^{G_T(k)} - \dim_{\mathbb{F}_\ell} A^{G_S(k)} = 1$ but $\log_\ell \chi_{k/k,T}(A) \le -1$. So in both cases, Proposition 9.4 shows that $\delta_{k/k,S}(A) \le [k : \mathbb{Q}] \dim_{\mathbb{F}_\ell} A$, and hence the theorem follows by Proposition 3.7. □

10. Proof of Theorem 1.1

In this section, we will prove Theorem 1.1. We assume that Γ is a nontrivial finite group, $Q = \mathbb{Q}$ or $\mathbb{F}_q(t)$ with $\gcd(q, |\Gamma|) = 1$, and let k/Q be a Galois extension with $\mathrm{Gal}(k/Q) \simeq \Gamma$. By Theorem 6.4, $G_\varnothing(k)^\mathcal{C}$ is a finite Γ-group when $\mathcal{C}$ is finite, so for a sufficiently large n there is a Γ-presentation $F_n(\Gamma) \to G_\varnothing(k)^\mathcal{C}$. In Section 10.1, we construct a finitely generated Γ-quotient G of $G_\varnothing(k)$ such that $G^\mathcal{C} \simeq G_\varnothing(k)^\mathcal{C}$ as Γ-groups. With the help of the group G, we employ the cohomology of $G_\varnothing$ to

compute the multiplicities in a pro-$\mathcal{C}$ admissible Γ-presentation of $G_\varnothing(k)^{\mathcal{C}}$. In Section 10.2, we compute the multiplicities $m^{\mathcal{C}}_{\mathrm{ad}}(n, \Gamma, G_\varnothing(k)^{\mathcal{C}}, A)$, and then compute the multiplicities $m^{\mathcal{C}}_{\mathrm{ad}}(n, \Gamma, G_{\varnothing,\infty}(k)^{\mathcal{C}}, A)$ for a finite simple $G_{\varnothing,\infty}(k)^{\mathcal{C}} \rtimes \Gamma$-module A. Using these multiplicities, finally in Section 10.3, we show that the kernel of a pro-$\mathcal{C}$ admissible Γ-presentation $\mathcal{F}_n(\Gamma)^{\mathcal{C}} \to G_{\varnothing,\infty}(k)^{\mathcal{C}}$ can be normally generated by elements $\{r^{-1}\gamma(r)\}_{r\in X,\gamma\in\Gamma}$ with X a subset of $\mathcal{F}_n(\Gamma)$ of cardinality $n+1$.

Note that in Theorem 1.1, k/Q is assumed to be split completely at ∞, and the Γ-groups in $\mathcal{C}$ are of order prime to $|\mu(Q)|$, $|\Gamma|$ and $\mathrm{char}(Q)$. However, in the proof, we do not use these assumptions until Section 10.2. So right now, we only assume that k/Q is a Galois field extension with $\mathrm{Gal}(k/Q) \simeq \Gamma$ and that $\mathcal{C}$ is a finite set of isomorphism classes of finite Γ-groups of order prime to $|\Gamma|$.

10.1. ***Construction of a specific finitely generated quotient of $G_\varnothing(k)$.*** Because $G_\varnothing(k)^{\mathcal{C}}$ is finite, when n is sufficiently large, there exists a Γ-equivariant surjection $\pi : F_n(\Gamma) \to G_\varnothing(k)^{\mathcal{C}}$, where $F_n(\Gamma)$ is the free profinite Γ-group defined in Section 3. Then π factors through $\pi^{\mathcal{C}} : F_n(\Gamma)^{\mathcal{C}} \to G_\varnothing(k)^{\mathcal{C}}$ as defined in Definition 5.2.

Lemma 10.1. *Use the notation above. If A is a finite simple $G_\varnothing(k)^{\mathcal{C}} \rtimes \Gamma$-module with*

$$m(\pi^{\mathcal{C}}, \Gamma, G_\varnothing(k)^{\mathcal{C}}, A) > 0,$$

then $A \rtimes G_\varnothing(k)^{\mathcal{C}} \in \bar{\mathcal{C}}$.

Proof. We denote $G_\varnothing(k)^{\mathcal{C}}$ by G_0 for convenience purposes. If $m(\pi^{\mathcal{C}}, \Gamma, G_0, A) > 0$, then there is a Γ-group extension

$$1 \to A \to H \xrightarrow{\varpi} G_0 \to 1$$

such that H is a quotient of $F_n^{\mathcal{C}}$, and so $H \in \bar{\mathcal{C}}$. We let E be the fiber product $H \times_{G_0} H$ defined by ϖ, i.e., $E = \{(x, y) \in H \times H \mid \varpi(x) = \varpi(y)\}$. Note that E is a subgroup of $H \times H$, so is in $\bar{\mathcal{C}}$. There is a natural diagonal embedding $H \hookrightarrow E$ mapping x to (x, x), and a normal subgroup $\{(a, 1) \mid a \in A\}$ of E that is isomorphic to A. From this, one can check that the diagonal subgroup H and the normal subgroup A are disjoint and they generate E, so $E \simeq A \rtimes H$ where the H action on A factors through $\varpi(H) = G_0$. So by taking the quotient map ϖ on the subgroup H of E, we obtain that $A \rtimes G_0$ is a quotient of E, and therefore we proved the lemma. □

Now we fix a finite simple $G_\varnothing(k)^{\mathcal{C}} \rtimes \Gamma$-module A with $m(\pi^{\mathcal{C}}, \Gamma, G_\varnothing(k)^{\mathcal{C}}, A) > 0$, and construct the desired quotient of $G_\varnothing(k)$ for A. We let φ_0 denote the quotient map $G_\varnothing(k) \to G_\varnothing(k)^{\mathcal{C}}$, and again let G_0 denote $G_\varnothing(k)^{\mathcal{C}}$. We define G_1 to be the quotient of $G_\varnothing(k)$ satisfying the following Γ-group extension:

$$1 \to A^{m(\varphi_0,\Gamma,G_0,A)} \to G_1 \xrightarrow{\varpi_0} G_0 \to 1. \tag{10-1}$$

By definition of the multiplicities, G_1 is well-defined. Since G_1 is a quotient of $G_\varnothing(k)$, we have that $G_1^{\mathcal{C}}$ is exactly G_0. Then we claim that the extension (10-1) is "completely nonsplit" (that is, if a subgroup of G_1 maps surjectively onto G_0, then it has to be G_1 itself). Indeed, if it's not completely nonsplit, then G_1 has a Γ-quotient isomorphic to $A \rtimes G_0$, and hence by Lemma 10.1 we have $A \rtimes G_0 \in \bar{\mathcal{C}}$, which contradicts that $G_1^{\mathcal{C}} = G_0$.

Similarly, we define $G_2, G_3, \dots$ to be the Γ-quotients of $G_\varnothing(k)$ inductively via

$$1 \to A^{m(\varphi_i,\Gamma,G_i,A)} \to G_{i+1} \xrightarrow{\varpi_i} G_i \to 1,$$

where the map φ_i is the quotient map $G_\varnothing(k) \to G_i$. Using the argument in the previous paragraph, we see that each of these group extensions is completely nonsplit, and $G_i^{\mathcal{C}} = G_0$ for each i. Then we take the inverse limit

$$G := \varprojlim_i G_i.$$

Then the profinite group G is the maximal extension of G_0 in $G_\varnothing(k)$ that can be obtained via group extensions by A.

Lemma 10.2. (1) *A subset of G is a generator set if and only if its image in G_0 generates G_0.*

(2) *The map $\pi : F_n(\Gamma) \to G_0$ defined at the beginning of this subsection factors through G.*

(3) *Let φ be the natural quotient map $G_\varnothing(k) \to G$ defined by inverse limit of φ_i. Then*

$$\mathrm{Hom}_{G\rtimes\Gamma}((\ker\varphi)^{ab}, A) = 0.$$

Proof. The group extension $\varpi_i : G_{i+1} \to G_i$ is completely nonsplit, so any lift of a generator set of G_i is a generator set of G_{i+1}. So we have (1) by taking inverse limit, and then (2) follows.

Note that G acts on the abelianization $(\ker\varphi)^{ab}$ of $\ker\varphi$ by conjugation. Suppose that

$$\mathrm{Hom}_{G\rtimes\Gamma}((\ker\varphi)^{ab}, A) \neq 0.$$

Then it means that φ factors through a Γ-equivariant group extension H of G by a kernel A. However, G does not have such a group extension in $G_\varnothing(k)$ by definition. So we proved (3). □

10.2. ***Determination of the multiplicity of A.*** We continue to use notation and assumptions given previously in this section. In particular, we remind the reader that A is a fixed finite simple $G_\varnothing(k)^{\mathcal{C}} \rtimes \Gamma$-module where $\Gamma \simeq \mathrm{Gal}(k/Q)$, and G depends on A. The goal of this subsection is to compute the multiplicity of A in an admissible Γ-presentation of $G_{\varnothing,\infty}(k)^{\mathcal{C}}$. The Γ-group G plays a very important role in this computation.

Lemma 10.3. *Let ℓ be the exponent of A and assume that $\ell \neq \mathrm{char}(Q)$ is prime to $|\Gamma|$. Then*

$$\dim_{\mathbb{F}_\ell} H^2(G, A)^\Gamma - \dim_{\mathbb{F}_\ell} H^1(G, A)^\Gamma \leq \delta_{k/Q,\varnothing}(A).$$

Proof. We consider the Γ-equivariant short exact sequence

$$1 \to M \to G_\varnothing(k) \xrightarrow{\varphi} G \to 1.$$

By the Hochschild–Serre exact sequence, we have

$$0 \to H^1(G, A) \to H^1(G_\varnothing(k), A) \to H^1(M, A)^G \to H^2(G, A) \to H^2(G_\varnothing(k), A), \tag{10-2}$$

which is compatible with the conjugation action by Γ. Since M acts trivially on A, we see that $H^1(M, A)^{G\rtimes\Gamma} = \mathrm{Hom}_{G\rtimes\Gamma}(M^{ab}, A) = 0$ by Lemma 10.2(3). So by taking the Γ-invariants on (10-2) and

computing the dimensions, we have that

$$\dim_{\mathbb{F}_\ell} H^2(G,A)^\Gamma - \dim_{\mathbb{F}_\ell} H^1(G,A)^\Gamma \le \dim_{\mathbb{F}_\ell} H^2(G_\varnothing(k),A)^\Gamma - \dim_{\mathbb{F}_\ell} H^1(G_\varnothing(k),A)^\Gamma = \delta_{k/Q,\varnothing}(A). \quad \square$$

Starting from now, we assume that $\mathcal{C}$ is a finite set of isomorphism classes of finite Γ-groups all of whose orders are prime to $|\Gamma|$, char Q and $|\mu(Q)|$. Let $\widehat{\pi}$ denote the Γ-equivariant surjective map $F_n(\Gamma) \to G$ used in Lemma 10.2(2). Then the pro-$\mathcal{C}$ completion of $\widehat{\pi}$ is $\pi^{\mathcal{C}} : F_n^{\mathcal{C}} \twoheadrightarrow G_\varnothing(k)^{\mathcal{C}}$. If $Q = \mathbb{Q}$, then $G_\varnothing(k)^{\mathcal{C}}$ is exactly $G_{\varnothing,\infty}(k)^{\mathcal{C}}$. If Q is a function field, then $k_\varnothing/k$ is not split completely at primes over ∞. Instead, $G_{\varnothing,\infty}(k)$ is the Γ-quotient of $G_\varnothing(k)$ obtained via modulo the decomposition subgroup $\mathrm{Gal}_{\mathfrak{p}}(k_\varnothing/k)$ of one prime $\mathfrak{p}$ of k above ∞ (because Γ acts transitively on all the primes of k above ∞). Since this decomposition subgroup $\mathrm{Gal}_{\mathfrak{p}}(k_\varnothing/k)$ is isomorphic to $\widehat{\mathbb{Z}}$ and G is a quotient of $G_\varnothing(k)$, we can define g_n to be an element of G that is the image of one generator of $\mathrm{Gal}_{\mathfrak{p}}(k_\varnothing/k)$. In other words, denoting $G^{\#}$ the quotient of G by the Γ-closed normal subgroup generated by g_n, we have the diagram

$$\begin{array}{ccccc}
 & & \overset{\varpi}{\curvearrowright} & & \\
F_n & \xrightarrow{\widehat{\pi}} & G & \xrightarrow[/[g_n]]{\eta} & G^{\#} \\
\downarrow & \overset{\pi}{\searrow} & \downarrow & & \downarrow \\
F_n{}^{\mathcal{C}} & \xrightarrow{\pi^{\mathcal{C}}} & G_\varnothing(k)^{\mathcal{C}} & \xrightarrow{\eta^{\mathcal{C}}} & G_{\varnothing,\infty}(k)^{\mathcal{C}} \\
 & & \underset{\varpi^{\mathcal{C}}}{\curvearrowright} & &
\end{array} \tag{10-3}$$

where the vertical maps are taking pro-$\mathcal{C}$ completions. To make the notation consistent between the number field and the function field cases, when $Q = \mathbb{Q}$, we let $g_n = 1$, and hence η and $\eta^{\mathcal{C}}$ in (10-3) are both identity maps. First of all, we want to determine $m(\widehat{\pi}, \Gamma, G, A)$.

Proposition 10.4. *Let ℓ be the exponent of A. Assume $\ell \neq \mathrm{char}(Q)$ is relatively prime to $|\mu(Q)||\Gamma|$. If $Q = \mathbb{Q}$, then*

$$m(\widehat{\pi}, \Gamma, G, A) \le \frac{(n+1)\dim_{\mathbb{F}_\ell} A - \dim_{\mathbb{F}_\ell} A^\Gamma}{h_{G\rtimes\Gamma}(A)}.$$

If $Q = \mathbb{F}_q(t)$ and $A \neq \mu_\ell$, then

$$m(\widehat{\pi}, \Gamma, G, A) \le \frac{n\dim_{\mathbb{F}_\ell} A - \dim_{\mathbb{F}_\ell} A^\Gamma}{h_{G\rtimes\Gamma}(A)}.$$

Remark 10.5. Recall that in Theorem 1.1 we assume that k/Q is split completely at ∞. In the function field case, μ_ℓ is a $\mathrm{Gal}(k_\varnothing/Q)$-module but not a $\mathrm{Gal}(k_{\varnothing,\infty}/Q)$-module, so we exclude the case that $A = \mu_\ell$.

Proof. By the assumptions, we can apply Proposition 3.4 to compute the multiplicities. Because $\ell \nmid |\Gamma|$, we have for $i = 1, 2$ that $H^i(G \rtimes \Gamma, A) = H^i(G, A)^\Gamma$. Then by Lemma 10.3, we have

$$m(\widehat{\pi}, \Gamma, G, A) \le \frac{n\dim_{\mathbb{F}_\ell} A - \xi(A) + \delta_{k/Q,\varnothing}(A)}{h_{G\rtimes\Gamma}(A)}. \tag{10-4}$$

So we just need to compute $\delta_{k/Q,\varnothing}(A)$.

In the function field case, recall that A is a simple $\mathbb{F}_\ell[\mathrm{Gal}(k_\varnothing/Q)]$-module that is not μ_ℓ, so by Proposition 9.3 we see that $\delta_{k/Q,\varnothing}(A)$ is -1 if $A = \mathbb{F}_\ell$, and is 0 otherwise. So we proved the result in function field case.

In the number field case that $Q = \mathbb{Q}$, we need to compute each of the terms in the formula in Proposition 9.4. Let $T = S_\ell(k) \cup S_\infty(k)$. In this case, ℓ is odd as $\mu_2 \subset Q$. First, we apply Theorem 7.1

$$\log_\ell \chi_{k/Q,T}(A) = -\dim_{\mathbb{F}_\ell} H^0(\mathbb{Q}_\infty, A') = -\dim_{\mathbb{F}_\ell}(A')^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})},$$

where the first equality uses $\widehat{H}^0(\mathbb{Q}_\infty, A') = 0$ because $\#\mathcal{G}_\infty(\mathbb{Q}) = 2$ and [Neukirch et al. 2008, Proposition 1.6.2(a)]. Then because A is a simple $\mathbb{F}_\ell[\mathrm{Gal}(k_\varnothing/Q)]$-module, $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts trivially on A, and hence $(A')^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})} = \mathrm{Hom}_{\mathrm{Gal}(\mathbb{C}/\mathbb{R})}(A, \mu_\ell) = 0$. So we have $\log_\ell \chi_{k/Q,T}(A) = 0$. Then note that $\epsilon_{k/Q,\varnothing}(A)$ in the formula in Proposition 9.4 is $\dim_{\mathbb{F}_\ell} A$ in this case, and we obtain

$$\delta_{k/Q,\varnothing}(A) \le \dim_{\mathbb{F}_\ell} \mathrm{Hom}_{\mathrm{Gal}(k_T/Q)}(A, \mu_\ell) - \dim_{\mathbb{F}_\ell} A^{\mathrm{Gal}(k_\varnothing/Q)} + \dim_{\mathbb{F}_\ell} A,$$

where the right-hand side is 0 if $A = \mathbb{F}_\ell$ and is $\dim_{\mathbb{F}_\ell} A$ otherwise. So we proved the number field case. □

Lemma 10.6. *Use the assumptions in Proposition 10.4. Consider the function field case and the diagram (10-3). When n is sufficiently large, we have*

$$m(\varpi, \Gamma, G^\#, A) \le \frac{(n+1)\dim_{\mathbb{F}_\ell} A - \dim_{\mathbb{F}_\ell} A^\Gamma}{h_{G^\# \rtimes \Gamma}(A)}$$

Proof. Again, we use $x_1, \dots, x_n$ to denote the generators of F_n. We can make n large to assume $\widehat{\pi}(x_n) = g_n$ (recall that the multiplicity depends on n but not on the choice of ϖ). Then we have a commutative diagram

$$\begin{array}{ccc} F_n & \xrightarrow{\lambda\ /[x_n]} & F_{n-1} \\ \downarrow{\scriptstyle \widehat{\pi}} & \searrow^{\varpi} & \downarrow{\scriptstyle \phi} \\ G & \xrightarrow[\eta\ /[g_n]]{} & G^\# \end{array}$$

where the top map is defined by taking the quotient by the Γ-closed normal subgroup generated by x_n. Note that the composition of the top and the right arrows satisfies the conditions of Lemma 3.8, so we have

$$m(\varpi, \Gamma, G^\#, A) = m(\lambda, \Gamma, F_{n-1}, A) + m(\phi, \Gamma, G^\#, A).$$

By the statement and the computation of $H^i(F_n \rtimes \Gamma, A)$ in the proof of Lemma 3.2, we see that

$$m(\lambda, \Gamma, F_{n-1}, A) = \frac{\dim_{\mathbb{F}_\ell} A}{h_{G^\# \rtimes \Gamma}(A)}.$$

So by Proposition 10.4, it suffices to prove

$$m(\phi, \Gamma, G^\#, A) \le m(\widehat{\pi}, \Gamma, G, A), \tag{10-5}$$

which will immediately follow after we prove the embedding

$$\left\{U \mid \text{max. proper } F_{n-1} \rtimes \Gamma\text{-normal subgroup of } \ker\phi \text{ such that } \ker\phi/U \simeq_{G^\# \rtimes \Gamma} A\right\}$$
$$\xhookrightarrow{\kappa} \left\{V \mid \text{max. proper } F_n \rtimes \Gamma\text{-normal subgroup of } \ker\widehat{\pi} \text{ such that } \ker\widehat{\pi}/V \simeq_{G \rtimes \Gamma} A\right\}$$

mapping U to $\lambda^{-1}(U) \cap \ker\widehat{\pi}$.

Since $\ker\varpi = \ker\widehat{\pi}\ker\lambda$, for each U in the first set, we have

$$\ker\widehat{\pi}/(\lambda^{-1}(U)\cap\ker\widehat{\pi}) = \lambda^{-1}(U)\ker\widehat{\pi}/\lambda^{-1}(U) = \ker\varpi/\lambda^{-1}(U) \simeq_{G^{\#}\rtimes\Gamma} A,$$

so the map κ is well-defined. Also, if $V = \kappa(U)$, then

$$\ker\varpi/V\ker\lambda = (\ker\widehat{\pi})(V\ker\lambda)/V\ker\lambda = \ker\widehat{\pi}/(\ker\widehat{\pi}\cap(V\ker\lambda)). \tag{10-6}$$

Since $V\subset\ker\widehat{\pi}$ and $\ker\widehat{\pi}/V$ is a simple module, the last quotient is either 1 or isomorphic to A. On the other hand, both of V and $\ker\lambda$ are contained in $\lambda^{-1}(U)$, so is $V\ker\lambda$. Then (10-6) implies that $V\ker\lambda = \lambda^{-1}(U)$. So we see that if $\kappa(U_1) = \kappa(U_2) = V$, then $\lambda^{-1}(U_1) = \lambda^{-1}(U_2)$ and hence $U_1 = U_2$. So we conclude that κ is injective. □

Proposition 10.7. *Let $\mathcal{C}$ be a finite set of isomorphism classes of finite Γ-groups all of whose orders are prime to $|\mu(Q)||\Gamma|$ and $\mathrm{char}(Q)$ (if nonzero). Let A be a finite simple $G_{\varnothing,\infty}(k)^{\mathcal{C}}\rtimes\Gamma$-module of exponent $\ell\neq\mathrm{char}(k)$ relatively prime to $|\mu(Q)||\Gamma|$. When n is sufficiently large, there exists an admissible Γ-presentation $\mathcal{F}_n(\Gamma)\twoheadrightarrow G_{\varnothing,\infty}(k)^{\mathcal{C}}$, and*

$$m_{\mathrm{ad}}^{\mathcal{C}}(n,\Gamma,G_{\varnothing,\infty}(k)^{\mathcal{C}},A)\le m_{\mathrm{ad}}(n,\Gamma,G^{\#},A)\le\frac{(n+1)(\dim_{\mathbb{F}_\ell}A-\dim_{\mathbb{F}_\ell}A^{\Gamma})}{h_{G_{\varnothing,\infty}(k)^{\mathcal{C}}\rtimes\Gamma}(A)}.$$

Remark 10.8. The proposition shows that $m_{\mathrm{ad}}^{\mathcal{C}}(n,\Gamma,G_{\varnothing,\infty}(k)^{\mathcal{C}},\mathbb{F}_\ell)=0$. In other words, $G_{\varnothing,\infty}(k)^{\mathcal{C}}$ does not admit any nonsplit central group extension

$$1\to\mathbb{F}_\ell\to\widetilde{G}\rtimes\Gamma\to G_{\varnothing,\infty}(k)^{\mathcal{C}}\rtimes\Gamma\to 1,$$

such that $\widetilde{G}$ is of level $\mathcal{C}$. This is equivalent to the solvability (i.e., the existence of the dashed arrow) of the embedding problem

$$\begin{array}{ccccccccc} & & & & & & G_{\varnothing,\infty}(k)^{\mathcal{C}}\rtimes\Gamma & & \\ & & & & & \swarrow & \downarrow\alpha & & \\ 1 & \longrightarrow & \mathbb{F}_\ell & \longrightarrow & \widetilde{H}\rtimes\Gamma & \longrightarrow & H\rtimes\Gamma & \longrightarrow & 1 \end{array}$$

for any nonsplit central group extension in the lower row with $\widetilde{H}$ of level $\mathcal{C}$, and for any surjection α. In [Liu et al. 2024], this solvability is called the *Property E* of $G_{\varnothing,\infty}(k)$ and is proven using the classical techniques of embedding problems. So Proposition 10.7 provides a new proof of the Property E by counting multiplicities.

Proof. By [Liu et al. 2024, Proposition 2.2], the pro-prime-to-$(|\Gamma|\,\mathrm{char}\,Q)$ completion of $G_{\varnothing,\infty}(k)$ is an admissible Γ-group, so its Γ-quotient $G^{\#}$ is also admissible. Since $G_{\varnothing,\infty}(k)^{\mathcal{C}}$ is finite, when n is large, there exist elements $a_1,\dots,a_n$ of $G_{\varnothing,\infty}(k)^{\mathcal{C}}$ such that $\{Y(a_i)\}_{i=1}^n$ forms a generator sets of $G_{\varnothing,\infty}(k)^{\mathcal{C}}$. Note that $G_{\varnothing,\infty}(k)^{\mathcal{C}}$ is a quotient of $G^{\#}$ as described in (10-3). We choose a preimage $b_i\in G^{\#}$ of a_i for each i, and then $\{Y(b_i)\}_{i=1}^n$ generates $G^{\#}$ by Lemma 10.2(1). Recall that the multiplicity does not depend on the choice of presentation, so we assume ϖ in (10-3) maps $y_i\in F_n$ to $b_i\in G^{\#}$ for each $i=1,\dots,n$.

Then the restriction $\varpi|_{\mathcal{F}_n}$ is an admissible Γ-presentation of $G^{\#}$. We have by Corollary 4.5 that

$$m_{\mathrm{ad}}(n,\Gamma,G^{\#},A)=m(n,\Gamma,G^{\#},A)-\frac{n\dim_{\mathbb{F}_\ell}A^{\Gamma}}{h_{G^{\#}\rtimes\Gamma}(A)}.$$

Then the desired result follows by Propositions 5.4, 10.4 and Lemma 10.6. □

10.3. ***Existence of the presentation*** **(1-1).** Finally, we will prove that when n is sufficiently large, there exists a subset X of $\mathcal{F}_n^{\mathcal{C}}$ containing $n+1$ elements for which the following isomorphism, which is (1-1) in Theorem 1.1, holds:

$$G_{\varnothing,\infty}(k)^{\mathcal{C}}\simeq\mathcal{F}_n(\Gamma)^{\mathcal{C}}/[r^{-1}\gamma(r)]_{r\in X,\gamma\in\Gamma}.$$

In Proposition 10.7, we showed that when n is sufficiently large, there is an admissible Γ-presentation, denoted by

$$1\to N\to\mathcal{F}_n^{\mathcal{C}}\xrightarrow{\varpi_{\mathrm{ad}}^{\mathcal{C}}}G_{\varnothing,\infty}(k)^{\mathcal{C}}\to 1.$$

Let M be the intersection of all maximal proper $\mathcal{F}_n^{\mathcal{C}}\rtimes\Gamma$-normal subgroups of N, and define $R=N/M$ and $F=\mathcal{F}_n^{\mathcal{C}}/M$. Note that because $\mathcal{C}$ is finite, we have that $\mathcal{F}_n^{\mathcal{C}}$ is finite [Neumann 1967, Corollary 15.72]. Then R is a finite direct product $\prod_{i=1}^{t}A_i^{m_i}$ of finite irreducible $F\rtimes\Gamma$-groups A_i. Assume A_i and A_j are not isomorphic as $F\rtimes\Gamma$-groups if $i\neq j$. When a factor A_i is abelian, its multiplicity m_i is $m_{\mathrm{ad}}^{\mathcal{C}}(n,\Gamma,G_{\varnothing,\infty}(k)^{\mathcal{C}},A_i)$ computed in Proposition 10.7.

Let X be a subset of $\mathcal{F}_n^{\mathcal{C}}$. Then the closed $\mathcal{F}_n^{\mathcal{C}}\rtimes\Gamma$-normal subgroup generated by $\{r^{-1}\gamma(r)\}_{r\in X,\gamma\in\Gamma}$ is N if and only if the closed $F\rtimes\Gamma$-normal subgroup generated by $\{\bar r^{-1}\gamma(\bar r)\}_{\bar r\in\overline{X},\gamma\in\Gamma}$ is R, where $\overline{X}$ and $\bar r$ are the images of X and r in R respectively. Recall the properties of $\mathcal{F}_n$ listed at the beginning of Section 4. Because of the property (1), in the definition of Y in (3), we can take the generator set $\{\gamma_1,\dots,\gamma_d\}$ to be the whole group Γ, then

$$\{r^{-1}\gamma(r)\}_{r\in X,\gamma\in\Gamma}=Y(\{r\}_{r\in X})\quad\text{and}\quad\{\bar r^{-1}\gamma(\bar r)\}_{\bar r\in\overline{X},\gamma\in\Gamma}=Y(\{\bar r\}_{\bar r\in\overline{X}}).$$

By [Liu et al. 2024, Proposition 4.3], for a fixed integer u, the probability that the images under the map Y of $n+u$ random elements of R generate R as an $F\rtimes\Gamma$-normal subgroup is

$$\begin{aligned}\mathrm{Prob}([Y(\{r_1,\dots,r_{n+u}\})]_{F\rtimes\Gamma}=R)&\\ =\prod_{\substack{1\le i\le t\\ A_i\text{ abelian}}}\prod_{j=0}^{m_i-1}(1-h_{F\rtimes\Gamma}(A_i)^j|Y(A_i)|^{-n-u})&\prod_{\substack{1\le i\le t\\ A_i\text{ nonabelian}}}(1-|Y(A_i)|^{-n-u})^{m_i}.\end{aligned}$$

This product in the formula is a finite product. By [Liu et al. 2024, Lemma 3.5], we have $|Y(A_i)|=|A_i|/|A_i^{\Gamma}|$ for each i. Note that Lemma 4.6 shows that $|Y(A_i)|>1$ when A_i is nonabelian, so the product over nonabelian factors in the above formula is always positive. The term for an abelian factor A_i is positive if and only if

$$m_i\le\frac{(n+u)\log_\ell|Y(A_i)|}{h_{G_{\varnothing,\infty}(k)^{\mathcal{C}}\rtimes\Gamma}(A_i)}=\frac{(n+u)(\dim_{\mathbb{F}_\ell}A_i-\dim_{\mathbb{F}_\ell}A_i^{\Gamma})}{h_{G_{\varnothing,\infty}(k)^{\mathcal{C}}\rtimes\Gamma}(A_i)}.$$

Therefore, by Proposition 10.7, R can be $F\rtimes\Gamma$-normally generated by the Y-values of $n+1$ elements, and hence we finish the proof of Theorem 1.1.

11. Exceptional cases

We will discuss the cases that are not covered by the Liu–Wood–Zureick-Brown conjecture, using the techniques developed in this paper. In this section, the base field Q can be any global field. If Q is a number field, we denote by r_1 and r_2 the number of real and pairs of complex embeddings of Q.

Again, we let Γ be a nontrivial finite group and k/Q a Galois extension of global fields with $\mathrm{Gal}(k/Q) \simeq \Gamma$, such that $\mathrm{char}(Q)$ and $|\Gamma|$ are relatively prime. We assume that ℓ is a prime integer that is not $\mathrm{char}(Q)$ and is prime to $|\Gamma|$. Recall that $G_\varnothing(k)(\ell)$ denotes the pro-ℓ completion of $G_\varnothing(k)$. So $G_\varnothing(k)(\ell)$ is the Galois group of the maximal unramified pro-ℓ extension of k, which we will denote by $k_\varnothing(\ell)/k$. Note that $G_\varnothing(k)(\ell)$ is finitely generated, because $\dim_{\mathbb{F}_\ell} H^1(k_\varnothing, \mathbb{F}_\ell)$ is the minimal number of generators of $G_\varnothing(k)(\ell)$ and is finite. So when n is sufficiently large, there is a Γ-presentation $\pi : F_n'(\Gamma) \to G_\varnothing(k)(\ell)$. Moreover, we assume, throughout this section, that the ℓ-primary part of the class group of Q is trivial. Then $G_{\varnothing,\infty}(k)(\ell)$ is admissible by the proof of [Liu et al. 2024, Proposition 2.2], and hence we can assume that the presentation π induces an admissible presentation, i.e., $\pi^{\mathrm{ad}} := \pi|_{\mathcal{F}_n}$ is surjective.

In this section, we use the assumptions above and study the multiplicities from the presentation π^{ad} in the following two cases:

(1) When Q is a number field with $\mu_\ell \not\subset Q$, and k/Q is not required to be split completely at $S_\infty(Q)$ (see Section 11.1).

(2) When Q contains the ℓ-roots of unity μ_ℓ (see Section 11.2).

We will compare the multiplicities in these two cases with the multiplicities from Theorem 1.1, to see why the random group model used in the Liu–Wood–Zureick-Brown conjecture cannot be applied to these two exceptional cases.

We point out that we study only $G_\varnothing(k)(\ell)$ instead of $G_\varnothing(k)^{\mathcal{C}}$ for a general $\mathcal{C}$, simply because we want to keep the computation easy in this section and there is no previous work discussing these two exceptional cases beyond the distribution of ℓ-class tower groups. One can generalize the argument in this section to any finite set $\mathcal{C}$.

11.1. ***Other signatures.*** Assume Q is a number field with $\mu_\ell \not\subset Q$ (so ℓ is odd), and k is a Γ-extension of Q. For each $v \in S_\infty(Q)$, we set Γ_v to be the decomposition subgroup at v of the extension k/Q.

Lemma 11.1. *For a finite simple $\mathbb{F}_\ell[\mathrm{Gal}(k_\varnothing(\ell)/Q)]$-module A, we have*

$$m_{\mathrm{ad}}(n, \Gamma, G_\varnothing(k)(\ell), A) \le \begin{cases} r_1 + r_2 - 1 & \text{if } A = \mathbb{F}_\ell, \\ n + r_2 + 1 & \text{if } A = \mu_\ell, \\ \dfrac{(n+r_1+r_2)\dim_{\mathbb{F}_\ell} A - \sum_{v\in S_{\mathbb{R}}(Q)} \dim_{\mathbb{F}_\ell} A/A^{\Gamma_v} - (n+1)\dim_{\mathbb{F}_\ell} A^\Gamma}{h_{\mathrm{Gal}(k_\varnothing(\ell)/Q)}(A)} & \text{otherwise.} \end{cases}$$

Proof. Let T be $S_\infty(k) \cup S_\ell(k)$. Since ℓ is odd, $\widehat{H}^0(Q_v, A') = 0$ for any $v \in S_\infty(Q)$, and hence by applying Theorem 7.1 with $S = T$ we have

$$\begin{aligned}\log_\ell(\chi_{k/Q,T}(A)) &= -\sum_{v\in S_\infty(Q)} \dim_{\mathbb{F}_\ell} H^0(Q_v, A') \\ &= -\sum_{v\in S_{\mathbb{C}}(Q)} \dim_{\mathbb{F}_\ell} A - \sum_{v\in S_{\mathbb{R}}(Q)} \dim_{\mathbb{F}_\ell} A/A^{\Gamma_v}.\end{aligned}$$

The last equality is because:

(1) If $v \in S_{\mathbb{C}}(Q)$, then $\mathcal{G}_v(Q) = 1$ acts trivially on both μ_ℓ and A.

(2) If $v \in S_{\mathbb{R}}(Q)$, then $\mathcal{G}_v(Q) \simeq \mathbb{Z}/2\mathbb{Z}$ acts on μ_ℓ as taking inverse. Since the action of $\mathcal{G}_v(Q)$ on A factors through Γ_v, and Γ_v acts on A/A^{Γ_v} as taking inverse, we have $\dim_{\mathbb{F}_\ell}(A')^{\mathcal{G}_v(Q)} = \dim_{\mathbb{F}_\ell} \mathrm{Hom}_{\mathcal{G}_v(Q)}(A, \mu_\ell) = \dim_{\mathbb{F}_\ell} \mathrm{Hom}_{\mathcal{G}_v(Q)}(A/A^{\Gamma_v}, \mu_\ell) = \dim_{\mathbb{F}_\ell} A/A^{\Gamma_v}$.

By Proposition 9.4, we have

$$\delta_{k/Q,S}(A) \le \begin{cases} \epsilon_{k/Q,\varnothing}(A) - r_2 - 1 & \text{if } A = \mathbb{F}_\ell, \\ \epsilon_{k/Q,\varnothing}(A) - r_2 - r_1 + 1 & \text{if } A = \mu_\ell, \\ \epsilon_{k/Q,\varnothing}(A) - r_2 \dim_{\mathbb{F}_\ell} A - \sum_{v\in S_{\mathbb{R}}(Q)} \dim_{\mathbb{F}_\ell} A/A^{\Gamma_v} & \text{otherwise,} \end{cases}$$

where A can be μ_ℓ only if $\mu_\ell \subset k$. Note that by definition, $\epsilon_{k/Q,\varnothing}(A)$ is equal to $[Q : \mathbb{Q}] \dim_{\mathbb{F}_\ell} A$. So the desired result follows by Proposition 3.4, Corollary 4.5, and Proposition 5.4. □

Corollary 11.2. *Let $k/\mathbb{Q}$ be an imaginary quadratic field such that $k \neq \mathbb{Q}(\sqrt{-3})$, and γ denote the nontrivial element of $\Gamma = \mathrm{Gal}(k/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$. For an odd prime ℓ, we have the following isomorphism of Γ-groups*:

$$G_\varnothing(k)(\ell) \simeq \mathcal{F}_n(\Gamma)(\ell)/[r^{-1}\gamma(r)]_{r\in X} \tag{11-1}$$

for a sufficiently large positive integer n and some set X consisting of n elements of $\mathcal{F}_n(\Gamma)(\ell)$.

Remark 11.3. If we choose the n elements of set X randomly with respect to the Haar measure, then the quotient in (11-1) gives a random group that defines a probability measure on all n-generated pro-ℓ admissible Γ-groups. By taking $n \to \infty$, there is a limit probability measure, which can be computed using formulas in [Liu et al. 2024]. The discussion in [Liu et al. 2024, §7.2 and Theorem 7.5] shows that this limit probability measure agrees with the probability measure used in the Boston–Bush–Hajir heuristics [Boston et al. 2017].

Proof. When $Q = \mathbb{Q}$ and k is imaginary quadratic, we have $r_1 = 1$, $r_2 = 0$, and $\Gamma_\infty = \Gamma$. Let A be a finite simple $\mathbb{F}_\ell[\mathrm{Gal}(k_\varnothing(\ell)/\mathbb{Q})]$-module. Also, $\mu_\ell \not\subset k$ for any odd ℓ because $k \neq \mathbb{Q}(\sqrt{-3})$, so $A \neq \mu_\ell$. By Lemma 11.1 , when n is sufficiently large, we have:

$$m_{\mathrm{ad}}(n, \Gamma, G_\varnothing(k)(\ell), A) \le \begin{cases} 0 & \text{if } A = \mathbb{F}_\ell, \\ \dfrac{n(\dim_{\mathbb{F}_\ell} A - \dim_{\mathbb{F}_\ell} A^\Gamma)}{h_{\mathrm{Gal}(k_\varnothing(\ell)/\mathbb{Q})} A} & \text{otherwise.} \end{cases}$$

Note that $\Gamma \simeq \mathbb{Z}/2\mathbb{Z}$ implies that the normal subgroup of $\mathcal{F}_n(\Gamma)(\ell) \rtimes \Gamma$ generated by $Y(X)$ is exactly $[r^{-1}\gamma(r)]_{r\in X}$. Thus, the corollary follows by [Liu et al. 2024, Proposition 4.3]. □

11.2. ***When Q contains the ℓ-th roots of unity.*** In this subsection, we assume $\mu_\ell \subset Q$. In this case, μ_ℓ becomes the trivial $\mathrm{Gal}(k_\varnothing/Q)$-module $\mathbb{F}_\ell$, which makes the multiplicities in a presentation of $G_\varnothing(k)(\ell)$ significantly different from the previous cases.

Lemma 11.4. *Assume $\mu_\ell \subset Q$. For a finite simple $\mathbb{F}_\ell[\mathrm{Gal}(k_\varnothing(\ell)/Q)]$-module A, we have*

(1) *If Q is a function field and the genus of k is not 0, then $\delta_{k/Q,\varnothing}(A) = 0$.*

(2) *If Q is a number field, then $\delta_{k/Q,\varnothing}(A) \le (r_1 + r_2)\dim_{\mathbb{F}_\ell} A$.*

Proof. Because of the assumption $\mu_\ell \subset Q$, we have

$$\dim_{\mathbb{F}_\ell}(A')^{\mathrm{Gal}(k_\varnothing/Q)} = \dim_{\mathbb{F}_\ell}(A^\vee)^{\mathrm{Gal}(k_\varnothing/Q)} = \dim_{\mathbb{F}_\ell} A_{\mathrm{Gal}(k_\varnothing/Q)} = \dim_{\mathbb{F}_\ell} A^{\mathrm{Gal}(k_\varnothing/Q)}. \tag{11-2}$$

Then the first statement follows directly by Proposition 9.3(2). For the rest we assume that Q is a number field and let $T = S_\ell(k) \cup S_\infty(k)$. If ℓ is odd, then the assumption $\mu_\ell \subset Q$ implies that Q is totally imaginary. Then we can easily see by Theorem 7.1 that $\log_\ell \chi_{k/Q,T}(A) = -r_2 \dim_{\mathbb{F}_\ell} A$, and hence the statement for odd ℓ follows by Proposition 9.4 and (11-2). If $\ell = 2$, then we first want to compute, for each $v \in S_\infty(Q)$,

$$\dim_{\mathbb{F}_\ell} \widehat{H}^0(Q_v, A') - \dim_{\mathbb{F}_\ell} H^0(Q_v, A'). \tag{11-3}$$

For each $v \in S_{\mathbb{C}}(Q)$, we have $\mathcal{G}_v(Q) = 1$, and hence (11-3) becomes $-\dim_{\mathbb{F}_\ell} A$. For each $v \in S_{\mathbb{R}}(Q)$, the assumption $\ell \nmid |\Gamma|$ implies that $|\Gamma|$ is odd. So for each $\mathfrak{p} \in S_v(k)$, $\mathfrak{p}$ is real, and so is any prime of $k_\varnothing(\ell)$ lying above $\mathfrak{p}$. Thus, $\mathcal{G}_\mathfrak{p}(k)$ acts trivially on A, so it also acts trivially on A', which implies that $\widehat{H}^0(k_\mathfrak{p}, A') = H^0(k_\mathfrak{p}, A')$. Then (11-3) equals 0, and we obtain the statement for $\ell = 2$ by Proposition 9.4 and (11-2). □

Then by the same arguments in Section 10, we obtain the following bounds for the multiplicity of A.

Corollary 11.5. *Assume $\mu_\ell \subset Q$. When k is a function field, we assume that $Q = \mathbb{F}_q(t)$ for some prime power q such that $\ell \mid q-1$ and k/Q is split completely at ∞. Let A be a finite simple $\mathbb{F}_\ell[\mathrm{Gal}(k_\varnothing(\ell)/Q)]$-module. Then for a sufficiently large n, we have*

$$m_{\mathrm{ad}}(n, \Gamma, G_{\varnothing,\infty}(k)(\ell), A) \le \begin{cases} \dfrac{(n+1)\dim_{\mathbb{F}_\ell} A - \xi(A) - n\dim_{\mathbb{F}_\ell} A^\Gamma}{h_{G_{\varnothing,\infty}(k)(\ell)\rtimes\Gamma}(A)} & \text{if } Q \text{ is a function field,} \\ \dfrac{(n+r_1+r_2)\dim_{\mathbb{F}_\ell} A - \xi(A) - n\dim_{\mathbb{F}_\ell} A^\Gamma}{h_{G_{\varnothing,\infty}(k)(\ell)\rtimes\Gamma}(A)} & \text{if } Q \text{ is a number field.} \end{cases}$$

Remark 11.6. (1) Readers can compare the corollary with Proposition 10.7. When $A = \mathbb{F}_\ell$ and Q is $\mathbb{Q}(\zeta_\ell)$ or $\mathbb{F}_q(t)$ with $\ell \mid q-1$, one can check that the upper bound of the multiplicity is positive, which suggests the failure of the Property E of $G_{\varnothing,\infty}(k)$. Therefore, the random group model used in the Liu–Wood–Zureick-Brown conjecture is not expected to work in this exceptional case.

(2) If the upper bounds in Corollary 11.5 are sharp, then it also suggests that we should not expect the coincidence of the distributions of $G_{\varnothing,\infty}(k)(\ell)$ between the function field case and the number field case.

For example, when $Q = \mathbb{Q}$, $\ell = 2$ or $Q = \mathbb{Q}(\zeta_3)$, $\ell = 3$, the upper bound in the corollary equals the one for function fields. However, when $Q = \mathbb{Q}(\zeta_\ell)$ with $\ell > 3$, the upper bound is

$$\frac{(n + (\ell - 1)/2) \dim_{\mathbb{F}_\ell} A - \xi(A) - n \dim_{\mathbb{F}_\ell} A^\Gamma}{h_{G_{\varnothing,\infty}(k)(\ell) \rtimes \Gamma}(A)},$$

which is strictly larger than the upper bound for function fields.

Acknowledgements

I would like to thank Nigel Boston and Melanie Matchett Wood for helpful conversations and encouragement which inspired me to work on the questions studied in this paper. I also thank Nigel Boston, Yufan Luo, Mark Shusterman, Preston Wake, Ken Willyard and Melanie Matchett Wood for comments on and corrections to an early draft of the paper. I am grateful to the referee for suggestions and comments that improved the exposition of the paper. I am partially supported by NSF Grant DMS-2200541.

References

[Achter 2006] J. D. Achter, "The distribution of class groups of function fields", *J. Pure Appl. Algebra* **204**:2 (2006), 316–333. MR Zbl

[Achter 2008] J. D. Achter, "Results of Cohen–Lenstra type for quadratic function fields", pp. 1–7 in *Computational arithmetic geometry* (San Francisco, CA, 2006), edited by K. E. Lauter and K. A. Ribet, Contemp. Math. **463**, Amer. Math. Soc., Providence, RI, 2008. MR Zbl

[Adam and Malle 2015] M. Adam and G. Malle, "A class group heuristic based on the distribution of 1-eigenspaces in matrix groups", *J. Number Theory* **149** (2015), 225–235. MR Zbl

[Boston and Wood 2017] N. Boston and M. M. Wood, "Non-abelian Cohen–Lenstra heuristics over function fields", *Compos. Math.* **153**:7 (2017), 1372–1390. MR Zbl

[Boston et al. 2017] N. Boston, M. R. Bush, and F. Hajir, "Heuristics for p-class towers of imaginary quadratic fields", *Math. Ann.* **368**:1-2 (2017), 633–669. MR Zbl

[Boston et al. 2021] N. Boston, M. R. Bush, and F. Hajir, "Heuristics for p-class towers of real quadratic fields", *J. Inst. Math. Jussieu* **20**:4 (2021), 1429–1452. MR Zbl

[Clozel et al. 2008] L. Clozel, M. Harris, and R. Taylor, "Automorphy for some l-adic lifts of automorphic mod l Galois representations", *Publ. Math. Inst. Hautes Études Sci.* **108** (2008), 1–181. MR Zbl

[Cohen and Lenstra 1984] H. Cohen and H. W. Lenstra, Jr., "Heuristics on class groups of number fields", pp. 33–62 in *Number theory* (Noordwijkerhout, Netherlands, 1983), edited by H. Jager, Lecture Notes in Math. **1068**, Springer, 1984. MR Zbl

[Cohen and Martinet 1987] H. Cohen and J. Martinet, "Class groups of number fields: numerical heuristics", *Math. Comp.* **48**:177 (1987), 123–137. MR Zbl

[Ellenberg et al. 2016] J. S. Ellenberg, A. Venkatesh, and C. Westerland, "Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields", *Ann. of Math.* (2) **183**:3 (2016), 729–786. MR Zbl

[Friedman and Washington 1989] E. Friedman and L. C. Washington, "On the distribution of divisor class groups of curves over a finite field", pp. 227–239 in *Théorie des nombres* (Quebec, 1987), edited by J.-M. De Koninck and C. Levesque, de Gruyter, Berlin, 1989. MR Zbl

[Garton 2015] D. Garton, "Random matrices, the Cohen–Lenstra heuristics, and roots of unity", *Algebra Number Theory* **9**:1 (2015), 149–171. MR Zbl

[Golod and Shafarevich 1964] E. S. Golod and I. R. Shafarevich, "On the class field tower", *Izv. Akad. Nauk SSSR Ser. Mat.* **28** (1964), 261–272. In Russian. MR Zbl

[Goss 1996] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Math. (3) **35**, Springer, 1996. MR Zbl

[Katz and Sarnak 1999] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, Amer. Math. Soc. Colloq. Publ. **45**, Amer. Math. Soc., Providence, RI, 1999. MR Zbl

[Koch 2002] H. Koch, *Galois theory of p-extensions*, Springer, 2002. MR Zbl

[Liu 2022] Y. Liu, "Non-abelian Cohen–Lenstra heuristics in the presence of roots of unity", preprint, 2022. arXiv 2202.09471

[Liu 2024] Y. Liu, "On the p-rank of class groups of p-extensions", *Int. Math. Res. Not.* **2024**:6 (2024), 5274–5325. MR Zbl

[Liu and Wood 2020] Y. Liu and M. M. Wood, "The free group on n generators modulo $n+u$ random relations as n goes to infinity", *J. Reine Angew. Math.* **762** (2020), 123–166. MR Zbl

[Liu et al. 2024] Y. Liu, M. M. Wood, and D. Zureick-Brown, "A predicted distribution for Galois groups of maximal unramified extensions", *Invent. Math.* **237**:1 (2024), 49–116. MR Zbl

[Lubotzky 2001] A. Lubotzky, "Pro-finite presentations", *J. Algebra* **242**:2 (2001), 672–690. MR Zbl

[Malle 2008] G. Malle, "Cohen–Lenstra heuristic and roots of unity", *J. Number Theory* **128**:10 (2008), 2823–2835. MR Zbl

[Malle 2010] G. Malle, "On the distribution of class groups of number fields", *Exp. Math.* **19**:4 (2010), 465–474. MR Zbl

[Neukirch et al. 2008] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, 2nd ed., Grundl. Math. Wissen. **323**, Springer, 2008. MR Zbl

[Neumann 1967] H. Neumann, *Varieties of groups*, Springer, 1967. MR Zbl

[Shusterman 2022] M. Shusterman, "Balanced presentations for fundamental groups of curves over finite fields", *Math. Res. Lett.* **29**:4 (2022), 1251–1259. MR Zbl

[Venkatesh and Ellenberg 2010] A. Venkatesh and J. S. Ellenberg, "Statistics of number fields and function fields", pp. 383–402 in *Proceedings of the International Congress of Mathematicians*, *II* (Hyderabad, India, 2010), edited by R. Bhatia et al., Hindustan Book Agency, New Delhi, 2010. MR

[Wang and Wood 2021] W. Wang and M. M. Wood, "Moments and interpretations of the Cohen–Lenstra–Martinet heuristics", *Comment. Math. Helv.* **96**:2 (2021), 339–387. MR Zbl

[Wood 2019] M. M. Wood, "Nonabelian Cohen–Lenstra moments", *Duke Math. J.* **168**:3 (2019), 377–427. MR Zbl

Communicated by Akshay Venkatesh
Received 2023-02-04 Revised 2023-12-17 Accepted 2024-07-16

yyyliu@illinois.edu *Department of Mathematics, University of Illinois Urbana-Champaign, Urbana, IL, United States*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2025 is US $565/year for the electronic version, and $820/year (+$70, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 19 No. 5 2025