NON-ABELIAN COHEN–LENSTRA HEURISTICS IN THE PRESENCE OF ROOTS OF UNITY

YUAN LIU

Abstract. For a Galois extension $K/F_q(t)$ of Galois group $\Gamma$ with $\gcd(q,|\Gamma|) = 1$, we define an invariant $\omega_K$, and show that it determines the Weil pairing of the curve corresponding to $K$ and it descends to the prime-to-$|\Gamma|$-torsion part of the lifting invariants of Hurwitz schemes introduced by Ellenberg–Venkatesh–Westerland and Wood. By keeping track of the image of $\omega_K$, we compute, as $K$ varies and $q \to \infty$, the average number of surjections from the Galois group of maximal unramified extension of $K$ to $H$, for any $\Gamma$-group $H$ whose order is prime to $q|\Gamma|$. Motivated by this result, we modify the conjecture of Wood, Zureick-Brown and the author about non-abelian Cohen–Lenstra, for both function fields and number fields, to cover the cases when the base field contains extra roots of unity. We also discuss how to use the invariant $\omega_K$ to construct a random group model, and prove in a special case that the model produces the same moments as our function field result.

Contents

1. Introduction 1
2. Definition of the invariants 8
3. Relationship between $\omega_K$ and the Weil pairing associated to $K$ 21
4. The function field moments as $q \to \infty$ 28
5. A random pro-$\ell$ $\Gamma$-group for $\Gamma = \mathbb{Z}/2\mathbb{Z}$ 35
6. Conjectures and Evidences 42
Appendix A. A random group model for random 3-manifolds 50
References 51

1. Introduction

Let $\Gamma$ be a finite group. The Cohen–Lenstra [CL84] and Cohen–Martinet [CM87] heuristics give predictions for the distribution of the class groups of $K$ as $K$ varies over all $\Gamma$-extensions of $\mathbb{Q}$ with prescribed signature. Although only few cases of these heuristics are proven, huge breakthroughs have been made in the function field analogue, which was first formulated by Friedman and Washington [FW89]. Ellenberg, Venkatesh, and Westerland [EVW16] translated the heuristics into questions about counting the $\mathbb{F}_q$-points of the Hurwitz schemes, the moduli schemes of branched covers of $\mathbb{P}^1$, and proved a version (as $q \to \infty$) of the function field analogue of the Cohen–Lenstra heuristics.

The class group is the Galois group of the maximal abelian unramified extension. So it is natural to study the distributions of the non-abelian analogues of the class group. In [BBH17] and [BBH21], Boston, Bush, and Hajir extended the Cohen–Lenstra heuristics to a pro-$\ell$ setting (for an odd prime $\ell$) by considering the distribution of the Galois groups of the maximal unramified pro-$\ell$ extensions of quadratic fields. Boston and Wood [BW17] proved the function field analogue of the Boston–Bush–Hajir heuristics. Wood, Zureick-Brown and the author [LWZB19] considered a more generalized setting. Let $Q$ be a global field that is either $\mathbb{Q}$ or $\mathbb{F}_q(t)$. As $K$ varies over all
\textcolor{red}{\Gamma}$-extensions of $Q$ that is split completely at $\infty$, \cite{LWZB19} gives conjectures of the distribution of the Galois group of the maximal unramified extension of $K$ whose degree is prime to both $|\Gamma|$ and the number of roots of unity in $Q$, and not divisible by $\text{char}(Q)$; and also proves the function field analogue as $q \to \infty$.

All of the conjectures above fail when the base field contains extra roots of unity. For example, the Cohen–Lenstra–Martinet heuristics predict that the probability that a quadratic extension of $\mathbb{Q}(\sqrt{-3})$ (which contains the 3rd roots of unity) has trivial 3-part of class group is $\prod_{i=1}^\infty (1 - 3^{-i}) \approx .840$, however, Malle’s numerical result \cite{Mal08} suggests that this probability should be $\frac{4}{3} \prod_{i=1}^\infty (1 + 3^{-i})^{-1} \approx .852$. The reason for this phenomenon is better understood in the function field case: Friedman and Washington in \cite{FW89} already discussed the importance of the Weil pairing of the curve corresponding to the function field extension $K/\mathbb{F}_q(t)$. When the $t$-th roots of unity $\mu_t$ is contained in $\mathbb{F}_q(t)$ (that is, when $t$ divides $q - 1$), the Weil pairing reduces to some non-trivial structure on the $\ell$-part of the $\ell$-class group of $K$, which makes the distribution of class groups different from the case that $\mu_t \not\subset \mathbb{F}_q(t)$. By keeping track of the image of the Weil pairing, Lipnowski and Tsimerman \cite{LT19} refined the Cohen–Lenstra heuristics for the distribution of the $\ell$-part of class groups of quadratic extensions over $\mathbb{F}_q(t)$ in the case when $t$ divides $q - 1$, and used the results of Ellenberg–Venkatesh–Westerland to prove the refined conjecture as $q \to \infty$; and Lipnowski, Sawin, and Tsimerman \cite{LST20} gave a similar conjecture in the number field case, by making local adjustments at the primes lying over $\ell$ and $\infty$.

In this paper, we generalize the non-abelian analogues of Cohen–Lenstra heuristics to include the roots-of-unity case. Let $\Gamma$ be a finite group, and $Q$ be a number field or $\mathbb{F}_q(t)$. As $K$ varies over $\Gamma$-extensions of $Q$ that is split completely at each archimedean prime when $Q$ is a number field or at $\infty$ when $Q = \mathbb{F}_q(t)$, we study the distribution of the Galois group of the maximal unramified and split-completely-at-$\infty$ extension of $K$ whose degree is prime to $|\Gamma|$ and not divisible by $\text{char}(Q)$.

\subsection*{1.1. Main results} The bulk of this paper deals with the function field case, that is $Q = \mathbb{F}_q(t)$. A $\Gamma$-extension $K/\mathbb{F}_q(t)$ that is split completely at $\infty$ corresponds to a $\Gamma$-cover $X/\mathbb{F}_q^1$. By passing this extension to $\mathbb{F}_q$, we first define an invariant $\omega_K$ associated to $K$ that, roughly speaking, plays the role of the Weil pairing associated to $X_{\mathbb{F}_q}$ in the non-abelian setting. For a field $L$, we let $G_\mathcal{O}(L) := \mathcal{L}_G/L$ denote the Galois group of the maximal unramified extension $L\mathcal{O}$ of $L$. Consider the exact sequence

$$1 \to G_\mathcal{O}(K_{X_{\mathbb{F}_q}}) \to G_\mathcal{O}(K) \to \text{Gal}(K/\mathbb{F}_q) \to \hat{\mathbb{Z}} \cdot \text{Frob} \to 1,$$

and a splitting $\hat{\mathbb{Z}} \cdot \text{Frob} \to G_\mathcal{O}(K)$ defined by identifying Frobenius element in the decomposition group of the extension $K_\mathcal{O}/K$ at a preselected place of $K_\mathcal{O}$ over $\infty$. Then this splitting defines a Frobenius action on $G_\mathcal{O}(K_{X_{\mathbb{F}_q}})$ by conjugation. We let $G'_\mathcal{O}(K)$ denote the pro-prime-to-$q|\Gamma|$ completion of $G_\mathcal{O}(K_{X_{\mathbb{F}_q}})$ and denote the corresponding extension by $K'_\mathcal{O}/\mathbb{F}_q(t)$. (Equivalently, $G'_\mathcal{O}(K)$ is the pro-prime-to-$q|\Gamma|$ completion of the étale fundamental group $\pi_1^\text{ét}(X_{\mathbb{F}_q})$.) Then $G'_\mathcal{O}(K)$ naturally obtains an action of Frobenius from $G_\mathcal{O}(K_{X_{\mathbb{F}_q}})$; and similarly, we can define a Frobenius action on the Galois group $\text{Gal}(K'_\mathcal{O}/\mathbb{F}_q(t))$. Moreover, $G'_\mathcal{O}(K)$ also has an action of $\Gamma$ by conjugation when we fix a homomorphic splitting of $\text{Gal}(K'_\mathcal{O}/\mathbb{F}_q(t)) \to \text{Gal}(K/\mathbb{F}_q(t)/\mathbb{F}_q(t)) \approx \Gamma$. We define the invariant $\omega_K$ to be a specific Frobenius-equivariant isomorphism (see Definition 2.8)

$$\omega_K : \hat{\mathbb{Z}}(1)_{(q|\Gamma)} \to H_2(\text{Gal}(K'_\mathcal{O}/\mathbb{F}_q(t)), \hat{\mathbb{Z}}(1)_{(q|\Gamma)})$$

where the subscript $(q|\Gamma)'$ represents the pro-prime-to-$q|\Gamma'$ completion. The invariant $\omega_K$ is first defined group-theoretically by studying the Schur covering group of $\text{Gal}(K'_\mathcal{O}/\mathbb{F}_q(t))$. Then we also give a cohomological definition: $\omega_K$ defines a central extension of $G'_\mathcal{O}(K)$ by $\hat{\mathbb{Z}}(1)_{(q|\Gamma)'}$, and hence corresponds to a class in $H^2(G'_\mathcal{O}(K), \hat{\mathbb{Z}}(1)_{(q|\Gamma)'});$ under the functorial isomorphism between Galois
cohomology and étale cohomology, the corresponding class in $H^2_{\text{ét}}(X_{F_q}, \hat{\mathbb{Z}}(1)(\langle \Gamma \rangle)^\vee)$ has trace $-|\Gamma|$ (see Lemma 2.11 and Corollary 2.12).

Then we pull everything back to $\overline{F}_q$ by taking the maximal $\Gamma$-equivariant quotient fixed by the Frob action. Such quotient of $G^\#_\mathcal{O}(K)$ is naturally the Galois group of the maximal unramified extension of $K$ that is splitting completely over $\infty$ and has degree prime-to-$|\Gamma|$, and we denote this quotient by $G^\#_\mathcal{O}(K)$ and the corresponding extension by $K^\#_\mathcal{O}/K$. For a subextension $L$ of $K^\#_\mathcal{O}/K$ that is Galois over $\mathbb{F}_q(t)$, we define an invariant $\omega_{L/K}$ to be the composition

$$\omega_{L/K} : \hat{\mathbb{Z}}(1)(\langle \Gamma \rangle)^\vee \xrightarrow{\omega_K} H_2(\text{Gal}(K^\#_\mathcal{O}/\mathbb{F}_q(t)), \mathbb{Z})_{\langle \langle \Gamma \rangle \rangle} \xrightarrow{\text{coinf}} H_2(\text{Gal}(L/\mathbb{F}_q(t)), \mathbb{Z})_{\langle \langle \Gamma \rangle \rangle}^\vee,$$

where coinf is the coinflation map defined by the quotient map between Galois groups. All the maps are Frob-equivariant and Frob acts trivially on the last term, so $\omega_{L/K}$ factors through $\mu_{q-1}$, and $\text{im}(\omega_{L/K})$ is contained in the $(q-1)$-torsion subgroup of $H_2(\text{Gal}(L/\mathbb{F}_q(t)), \mathbb{Z})_{\langle \langle \Gamma \rangle \rangle}^\vee$.

The invariant $\omega_K$ is “abelianized” to the Weil pairing associated to $X_{\overline{F}_q}$. Let $\ell$ be a prime number such that $\ell \nmid q|\Gamma|$. The pro-$\ell$ completion $G_\ell(\overline{K}/q)(\ell)$ of $G_\ell(\overline{K}/q)$ is a pro-$\ell$ Demushkin group (a special type of one-relator pro-$\ell$ group). Similarly to what we discussed previously, the invariant $\omega_K$ defines to a central extension of $G_\ell(\overline{K}/q)(\ell)$ by $\mathbb{Z}_\ell(1)$, from which we obtain information of the relator in a pro-$\ell$ presentation of $G_\ell(\overline{K}/q)(\ell)$. This information, by properties of Demushkin groups (namely, the transgression map associated to the presentation), completely determines the cup product

$$H^1(G_\ell(\overline{K}/q), \mathbb{Z}_\ell) \times H^1(G_\ell(\overline{K}/q), \mathbb{Z}_\ell) \xrightarrow{\cup} H^2(G_\ell(\overline{K}/q), \mathbb{Z}_\ell).$$

Because $G_\ell(\overline{K}/q)$ acts trivially on $\mathbb{Z}_\ell(1)$ and $H^1(G_\ell(\overline{K}/q), \mathbb{Z}_\ell(1))$ can be identified as the $\ell$-adic Tate module of $X_{\overline{F}_q}$, the cup product above followed by the trace map gives the Weil pairing associated to $X_{\overline{F}_q}$. Similarly, the invariant $\omega_{L/K}$ determines the image of the Weil pairing (see Proposition 3.6, and also see Definition 3.5 for the definition of the image of Weil pairing).

Then, we generalize the results of Lipnowski–Sawin–Tsimerman to the non-abelian setting by keeping track of our invariant $\omega_{L/K}$. In fact, $\omega_K$ is defined in the way such that $\omega_{L/K}$ agrees with the prime-to-$|\Gamma|$-torsion part of a component invariant of Hurwitz schemes, which is first introduced by Ellenberg–Venkatesh–Westerland and then carefully explained by Wood in [Woo21] (we refer this invariant by the *EVW-W lifting invariant*). Then by modifying the moment computation using Hurwitz schemes in [LWZB19], we obtain the moment result in the function field case as $q \to \infty$.

Let $r\text{Disc}K$ denote the norm of the radical of the ideal $\text{Disc}(K/Q)$. Let $E_\Gamma(D, Q)$ be the set of the pairs $(K, \iota)$, where $K$ is a split-completely-at-infinity extension of $Q$ with $r\text{Disc} K = D$, and $\iota$ is an isomorphism $\text{Gal}(K/Q) \to \Gamma$. An *admissible $\Gamma$-group* is a group with a $\Gamma$ action such that it is of order prime to $|\Gamma|$ and is generated, under the action of $\Gamma$, by the elements in the form of $g^{-1} \gamma(g)$ for $g \in G$, $\gamma \in \Gamma$. All $\Gamma$-equivariant quotients of $G^\#_\mathcal{O}(K)$ are admissible $\Gamma$-groups.

**Theorem 1.1.** Let $\Gamma$ be a finite group, $H$ a finite admissible $\Gamma$-group, and $\delta$ a group homomorphism $\hat{\mathbb{Z}}(1)(\langle \Gamma \rangle)^\vee \to H_2(H \rtimes \Gamma, \mathbb{Z})_{\langle \langle \Gamma \rangle \rangle}^\vee$. Then

$$\lim_{N \to \infty} \lim_{q \to \infty} \sum_{\substack{n \leq N \text{ and } \text{ord}(\text{im} \delta) = 1 \text{ mod } q-1}} \sum_{K \in E_\Gamma(q^n, \mathbb{F}_q(t))} \# \left\{ \pi \in \text{Surf} \left( G^\#_\mathcal{O}(K), H \right) \bigg| \pi_* \circ \omega_{K^\#_\mathcal{O}/K} = \delta \right\} \sum_{n \leq N} \# E_\Gamma(q^n, \mathbb{F}_q(t)) = \frac{1}{[H : H^\Gamma]}.$$

where in the limit $q$ is always a prime power, $\text{ord}(\text{im} \delta)$ is the order of the image of $\delta$, and $\pi_*$ is the coinflation map $H_2(\text{Gal}(K^\#_\mathcal{O}/\mathbb{F}_q(t)), \mathbb{Z})_{\langle \langle \Gamma \rangle \rangle}^\vee \to H_2(H \rtimes \Gamma, \mathbb{Z})_{\langle \langle \Gamma \rangle \rangle}^\vee$ induced by $\pi$. 
Inspired by this theorem, we make the following conjecture about the distribution of the prime-
to-\text{char}(Q)\Gamma|\Gamma| completion of the maximal unramified Galois group of K, for a fixed base field Q, in
both the function field case and the number field case.

**Conjecture 1.2** (Moment part of Conjecture 6.4, and Conjecture 6.7). Let \( \Gamma \) be a finite group,
\( H \) a finite admissible \( \Gamma \)-group. Let \( q \) be a prime power such that \( \gcd(q, |\Gamma||H|) = 1 \), and \( \delta \) a group
homomorphism \( \hat{\mathbb{Z}}(1)_{(q\Gamma)'} \rightarrow H_2(H \rtimes \Gamma, \mathbb{Z})_{(q\Gamma)'} \). If \( \text{ord}(|\delta|) \mid q - 1 \), then

\[
\lim_{N \to \infty} \frac{\sum_{n \leq N} K \in E_{\Gamma}(q^n, \mathbb{F}_q(t)) \sum_{\pi \in \text{Sur}_{\Gamma} \left( \Gamma_{\hat{\mathbb{Z}}(1)}(K), H \right) \mid \pi \circ \omega_{K^\delta/\mathbb{K}} = \delta}}{\sum_{n \leq N} \#E_{\Gamma}(q^n, \mathbb{F}_q(t))} = \frac{1}{[H : H^1]},
\]

otherwise, \( \#\{\pi \in \text{Sur}_{\Gamma} \left( \Gamma_{\hat{\mathbb{Z}}(1)}(K), H \right) \mid \pi \circ \omega_{K^\delta/\mathbb{K}} = \delta\} = 0 \) for any \( K \in E_{\Gamma}(q^n, \mathbb{F}_q(t)) \).

Let \( Q \) be a number field, and \( m \) the maximal integer such that the \( m \)-th roots of unity is contained
in \( Q \). For any extension \( K/Q \), we define \( \Gamma_{\hat{\mathbb{Z}}(1)}(K) := \Gamma_{\hat{\mathbb{Z}}(1)}(K_{\text{Gal}(K/Q)}) \). Assume that \( \Gamma_{\hat{\mathbb{Z}}(1)}(Q) \) is
pro-prime-to \( |H| \). Then

\[
\lim_{N \to \infty} \frac{\sum_{D \leq N} \sum_{K \in E_{\Gamma}(D, Q)} \#\text{Sur}_{\Gamma} \left( \Gamma_{\hat{\mathbb{Z}}(1)}(K), H \right)}{\sum_{D \leq N} \#E_{\Gamma}(D, Q)} = \frac{\#H_2(H \rtimes \Gamma, \mathbb{Z})_{(\hat{\mathbb{Z}}(1)_{(q\Gamma)'})}[m]}{[H : H^1] \cdot |H|^u},
\]

where \( u \) is the rank of the group of units in the ring \( \mathcal{O}_Q \) of algebraic integers of \( Q \).

We add the requirement “pro-prime-to-\( |G_{\hat{\mathbb{Z}}(1)}(Q)| \)” in the number field conjecture because, when
\( G_{\hat{\mathbb{Z}}(1)}(Q) \neq 1 \), the group \( G_{\hat{\mathbb{Z}}(1)}(K_{\text{Gal}(Q/K)}) \) is not an admissible \( \Gamma \)-group and its distribution would be very
different from the function field case.

We also conjecture that there exists a unique probability measure that gives the conjectural
moment in the function field case (see Conjecture 6.1). Then the conjectural moment in the number field case is obtained by taking the quotient of a group according to this probability measure modulo \( u \) elements according to the Haar measure. This number field conjecture is inspired by [Mal10],
[LST20], and two other evidences from algebraic number theory:

1. Using the previous work [Liu20] of the author, we show that, in a presentation of the Galois group
   \( G_{\hat{\mathbb{Z}}(1)}(K) \), it needs \( u \) more relators in the number field case than in the function field case. (See §6.2)
2. When \( Q = \mathbb{Q}(\mu_{\ell}) \) and \( K \) is nice (namely, when \( K \) is \( \ell \)-CM), Schmidt [Sch96] proved that there is a maximal positively ramified pro-\( \ell \) extension \( K_{\text{pos}}(\ell) \) of \( K \) such that the Galois group of \( K_{\text{pos}}(\ell) \) over the cyclotomic \( \mathbb{Z}_{\ell} \)-extension \( K_{\infty} \) of \( K \) is a very nice analogue of the
   pro-\( \ell \) completion of the étale fundamental group of \( \mathbb{X}^1_{\mathbb{F}_\ell} \). Using this positively ramified
   extension, we show that \( G_{\hat{\mathbb{Z}}(1)}(K)(\ell) \) is the quotient of \( G_{\text{pos}}(K) \) modulo \( u \) elements, where
   \( G_{\text{pos}}(K) \) is the maximal quotient of \( \text{Gal}(K_{\text{pos}}(\ell)/K_{\infty}) \) fixed by \( \text{Gal}(K_{\infty}/K) \) (which is the analogue of \( G_{\hat{\mathbb{Z}}(1)}(K)(\ell) \) from the function field case). (See §6.3)

Regarding the function field case, another advantage of studying the invariant \( \omega_K \) is that it shows
us how to construct a random group model to predict the distribution of interest to us. By the Grothendieck’s theory of specialization, \( G_{\hat{\mathbb{Z}}(1)}(K) \) has a pro-prime-to-\( q\Gamma|\Gamma| \) presentation in the form of
\[
\langle x_1, \ldots, x_g \mid [x_1, x_2] \cdots [x_{2g-1}, x_{2g}] \rangle,
\]
where \( g \) is the genus of \( \mathbb{X}^1_{\mathbb{F}_q} \). Let \( F \) be the free pro-prime-to-\( q\Gamma|\Gamma| \) group on generators \( x_1, \ldots, x_{2g} \), and let \( R \) be the closed normal subgroup of \( F \) generated by
\[
[x_1, x_2] \cdots [x_{2g-1}, x_{2g}].
\]
Then the short exact sequence
\[
1 \rightarrow R/\langle F, R \rangle \rightarrow F/\langle F, R \rangle \rightarrow G_{\hat{\mathbb{Z}}(1)}(K) \rightarrow 1 \tag{1.1}
\]
is a central extension with \( R/[F, R] \simeq \hat{\mathbb{Z}}(q\mathbb{F}) \); and moreover, the kernel is contained in the commutator of \( F/[F, R] \), so the extension is stem. Note that \( H_2(G, \mathbb{Z}) \) is the Schur multiplier of \( G \), and it is isomorphic to the kernel of a Schur covering (that is, a maximal stem extension) of \( G \). Thus, the isomorphism \( \omega_K \) implies that there are an action of \( \text{Frob} \) and an action of \( \Gamma \) on the sequence (1.1) such that they preserve the kernel \( R/[F, R] \), they induce the natural \( \text{Frob} \) and \( \Gamma \) actions on \( G'_\mathbb{Q}(K) \), and moreover, on \( R/[F, R] \), \( \Gamma \) acts trivially and \( \text{Frob} \) acts as multiplication by \( q \). Then we expect that by considering the \( \text{Frob} \) action as a random automorphism of \( F/[F, R] \) satisfying all the requirements, we can obtain a random group model that gives the conjectural moment in the function field case.

In general, understanding the group structure of such random group models is difficult. In this paper, we only study this random group model when we focus on the pro-\( \ell \) completions for an odd prime \( \ell \) and \( \Gamma = \mathbb{Z}/2\mathbb{Z} \). By the classification of Demuškin group by Labute [Lab67], a pro-\( \ell \) Demuškin group whose abelianization is torsion-free necessarily has a presentation as described in the preceding paragraph, and we denote such Demuškin group by \( \mathcal{G}_q \). Then, up to isomorphism, \( \mathcal{G}_n \) admits a unique Schur covering

\[
1 \rightarrow \mathbb{Z}_\ell \rightarrow \tilde{\mathcal{G}}_n \xrightarrow{\pi} \mathcal{G}_n \rightarrow 1,
\]

and we show that there exists a \( \Gamma = \mathbb{Z}/2\mathbb{Z} \) action (unique up to isomorphism) on \( \tilde{\mathcal{G}}_n \) such that the action preserves and acts trivially on \( \ker \pi_n \) and its induced action on the abelianization of \( \mathcal{G}_n \) is taking inversion (the last condition is naturally satisfied by the \( \Gamma \) action on \( G'_\mathbb{Q}(K)(\ell) \), since the étale fundamental group of \( \mathbb{P}^1_{\mathbb{F}_q} \) is trivial). Then we define a random group \( Y_{q,n} \) to be the maximal \( \Gamma \)-equivariant quotient of \( \mathcal{G}_n \) fixed by a random automorphism of \( \tilde{\mathcal{G}}_n \) that preserves and acts as multiplication by \( q \) on \( \ker \pi_n \). (See Definition 5.3 for a more careful definition of the random group.) Then we prove that the moment obtained by \( Y_{q,n} \) is exactly the moment in Conjecture 1.2.

**Theorem 1.3** (see Theorem 5.6). Let \( H \) be a finite \( \ell \)-group with an action of \( \Gamma = \mathbb{Z}/2\mathbb{Z} \) such that \( H \) is admissible. Let \( n \) be a sufficiently large integer such that there exists a \( \Gamma \)-equivariant surjection from \( \mathcal{G}_n \) to \( H \). Let \( \delta \) be a group homomorphism \( \mathbb{Z}_\ell \rightarrow H_2(H \times \Gamma, \mathbb{Z})(\ell) \) such that \( \text{ord}(\text{im} \delta) \mid q - 1 \).

Then

\[
E(\#\{\pi \in \text{Sur}_\Gamma(Y_{q,n}, H) \mid \pi_\dagger = \delta\}) = \frac{1}{[H : H]}.
\]

where \( \pi_\dagger \) is the coflation map \( \mathbb{Z}_\ell \simeq H_2(\mathcal{G}_n \times \Gamma, \mathbb{Z})(\ell) \rightarrow H_2(H \times \Gamma, \mathbb{Z})(\ell) \) induced by the \( \Gamma \)-equivariant quotient map \( \mathcal{G}_n \rightarrow Y_{q,n} \xrightarrow{\pi} H \).

We conjecture that, as \( n \rightarrow \infty \), the probability measures defined by \( Y_{q,n} \) weakly converge to a probability measure that gives the moments in Conjecture 1.2 (see Conjecture 6.3). Theorem 1.3 is proved by studying the orbits of \( \text{Sur}_\Gamma(\mathcal{G}_n, H) \) under the action of the automorphisms of \( \tilde{\mathcal{G}}_n \) that preserves and acts as multiplication by \( q \) on \( \ker \pi_n \). By using the method of successive approximation in [Lab67], we prove that two surjections in \( \text{Sur}_\Gamma(\mathcal{G}_n, H) \) are in the same orbit if and only if they induce the same coflation map. This random group model can also be used in other scenarios with similar group structures. For example, in Appendix A, we apply the model to study the fundamental groups of random 3-manifolds constructed by random Heegaard splittings, in the notion defined by Dunfield and Thurston [DT06]. We show that when \( \phi \) is a random automorphism of \( \tilde{\mathcal{G}}_n \) (forgetting the \( \Gamma \) action) that preserves and acts trivially on \( \ker \pi_n \), the moment obtained by the random group

\[
\lim_{n \rightarrow \infty} \tilde{\mathcal{G}}_n / [x_1, x_3, \ldots, x_{2n-1}, \phi(x_1), \phi(x_3), \ldots, \phi(x_{2n-1})]
\]

agrees with the average size of \( \text{Sur}(\pi_1(M), H) \), for any \( \ell \)-group \( H \), as \( M \) varies as a random 3-manifold (see Proposition A.1).
1.2. Prior works and further questions. The study of random group models that are relating to the Cohen–Lenstra type of questions started at the very beginning: in the original paper [CL84] of Cohen and Lenstra, they used the random matrix

$$\lim_{n \to \infty} \text{coker}(M),$$

to give the probability measure in the totally real case of their conjecture. Translating it into a random abelian group, this model is equivalent to

$$\lim_{n \to \infty} \mathbb{Z}_\ell^{\oplus n} / n + 1 \text{ random elements}.$$

In all the generalizations of Cohen–Lenstra in the non-roots-of-unity case, the corresponding random group models are constructed using balanced presentations (that is, presentations such that the difference between the numbers of generators and relators is fixed). Boston–Bush–Hajir studied the balanced pro-$\ell$ presentations in [BBH17, BBH21]. Wood, Zureick-Brown and the author in [LWZB19] gave the conjectural probability measures by using a form of balanced presentations of admissible $\Gamma$-groups, which is a modification of the probability measures of random balanced presentations studied in [LW20]. In the non-roots-of-unity case, the random balanced presentation models work very well, and the author proved in [Liu20] that the unramified Galois groups of interest to us can always be obtained by a balanced $\Gamma$-presentation as conjectured in [LWZB19].

However, when considering the roots-of-unity case, the balanced presentation models fail. Similar phenomenon happens to random 3-manifolds: Dunfield and Thurston in [DT06] tried to use balanced presentations to study random 3-manifolds, but they concluded that the fundamental groups of random 3-manifolds have many more finite quotients than the random balanced presentation model. It was first suggested by Friedman and Washington [FW89] that, instead of studying random presentation, we could consider the Frobenius map as a random automorphism acting on Jacobian varieties, and hence study the random matrix

$$\lim_{n \to \infty} \text{coker}(I_n - \mathcal{F})$$

where $\mathcal{F}$ is a random invertible matrix that is compatible with the Weil pairing on Jacobian. The random matrices in this setting and their relationship with function field case have been vastly studied, for example, see [KS99, Ach06, Ach08, Gar15, AM15, LT19, LST20].

The random group model constructed in this paper is a non-abelian generalization of (1.2) and sets up a framework for the study of the non-abelian Cohen–Lenstra heuristics in the roots of unity case. There are many important questions in this direct that are left to be solved. We don’t know how to compute the probability measure defined by $Y_{q,n}$, and whether the limit of the measure as $n \to \infty$ has total mass 1. Although, Theorem 1.3 strongly suggests that our random group model is the right object to study, what we really want is that the moment with respect to the limit measure equals to $1/[H : H^F]$ (that is, to take $\lim_{n \to \infty}$ inside $E$). The recent work of Sawin and Wood [SW22a, SW22b] studies, in a very general setting, how one can get the probability measure directly from the moments, without the help of any random group structures; and we expect that their idea can be applied to our moment results and to prove some of the conjectures in Section 6.

Also, the moment result for $Y_{q,n}$ in Theorem 1.3 cannot be easily generalized to the situation either when $\Gamma \not\simeq \mathbb{Z}/2\mathbb{Z}$, or when studying the distribution of $G_0^\#(K)$, not just of $G_0^\#(K)(\ell)$. The main reasons of this difficulty are: 1) when $\Gamma \not\simeq \mathbb{Z}/2\mathbb{Z}$, we don’t know how to give a canonical definition of a pro-$\ell$ Demuškin $\Gamma$-group as in Lemma 5.2; and 2) the proof of Theorem 1.3 vastly uses the filtration of pro-$\ell$ groups given by the lower central series, which does not exists for a general group.

There is a potential to apply our random group model to obtain some numerical results. For example, for fixed $n$ and $q$, we can take the pro-$C$ completion of the random group $Y_{q,n}$ for a finite
set of \( \ell \)-groups \( C \) (for the definition of \( pro-C \) completion, see §6.1). Since \( \mathcal{G}_n^C \) is always finite, it is possible to list all the automorphisms of \( \mathcal{G}_n^C \) satisfying the conditions in the definition of \( Y_{q,n} \), and then we could see which quotients of \( G_n^C \) can occur as \( Y_{q,n}^C \), and compute the probability that they occur. As \( n \to \infty \), if the probability measures converge fast, then we may get an approximation of the probability that \( G_n^\#(K)(\ell)^C \simeq H \) for small \( \ell \)-groups \( H \).

For Cohen–Lenstra in the presence of roots of unity, Lipnowski–Sawin–Tsimerman in [LT19, LST20] made moment conjectures for the distributions of class groups of quadratic fields. In the non-abelian setting, Wood in [Woo19] gave a conjecture for the average number of unramified \( G \)-extensions of a quadratic extension of \( \mathbb{Q} \) or \( \mathbb{F}_q(t) \) for any finite group \( G \). The conjectures made in this paper agree with all the previous conjectures about moments. Wood’s work also considers some cases that cannot be addressed by the method in this paper – it also deals with the case that \( G \) is of even order and the case that the quadratic fields are imaginary. Malle in [Mal10] and Boston–Bush in [BB21] gave conjectures and numerical evidences in some cases for the probability measures of the distributions of class groups and class tower groups respectively.

It is also interesting to understand the difference between the function field case and the number field case, which is related to the very important question: for number fields, what is the best analogue of the étale fundamental group from the function field case? Conjecture 1.2 and the two evidences §6.2 and §6.3 strongly suggest that, for any \( \Gamma \)-extension \( K/Q \) such that no archimedean prime is ramified, there is some group associated to \( K \) such that its group structure is similar to the prime-to-characteristic part of the étale fundamental groups of curves and \( G_\bigotimes(K)_{[[\Gamma]]} \) is the \( \Gamma \)-equivariant quotient of this group modulo rank \( \mathcal{O}_Q^\times \) elements. When \( K \) and \( Q \) are nice, this group can be defined by the positively ramified extension by [Sch96] and the discussion in §6.3. We would like to understand how to generalize the notion of positively ramifications for arbitrary \( K/Q \). When we have a better understanding of this mysterious group, we want to construct an invariant associated to \( K \) that is analogous to \( \omega_K \) in the function field case, and then we want to know whether this invariant agrees with the invariants defined in previous work (the lifting invariant for number fields in [Woo19] and the Artin–Verdier pairing invariant in [LST20]).

### 1.3. Outline of the paper.

In Section 2, we define the invariants \( \omega_K \) and \( \omega_{L/K} \): we give the group theoretical definition of \( \omega_K \) in §2.1, the cohomological definition of \( \omega_K \) in §2.2, and the definition and a group theoretical description of \( \omega_{L/K} \) in §2.3. In Section 3, we explain how the invariant \( \omega_K \) is related to the Weil pairing in §3.1 and how \( \omega_{L/K} \) determines the image of the Weil pairing in §3.2. In Section 4, we first recall the definition of the EVW-W lifting invariants in §4.1, we show that \( \omega_{L/K} \) is the prime-to-\(|\Gamma|\)-torsion part of the EVW-W lifting invariant in §4.2, and we give the proof Theorem 1.1 in §4.3. In Section 5, we construct our random group model in §5.1, and give the proof of Theorem 1.3 in §5.2 and §5.3. In Section 6, we give the statements of conjectures regarding the probability measures and the Cohen–Lenstra moments in §6.1, and provide the algebraic number theoretical evidences in §6.2 and §6.3 to support Conjecture 1.2.

### 1.4. Notation.

For a group \( G \) and an element \( g \in G \), we let \( \text{ord}(G) \) and \( \text{ord}(g) \) denote the orders of \( G \) and \( g \) respectively. For \( a, b \in G \), we write \([a, b] = a^{-1}b^{-1}ab\) and \( a^b = b^{-1}ab \). Whenever we talk about homomorphism of profinite groups, we always mean continuous homomorphisms. A \( \Gamma \)-group \( H \) is a profinite group \( H \) with a continuous action by \( \Gamma \), and we write \( H \rtimes \Gamma \) for the semidirect product defined by the \( \Gamma \) action on \( H \). We write \( \text{Hom}_G \), \( \text{Sur}_G \), and \( \text{Aut}_G \) to represent the sets of \( G \)-equivariant homomorphisms, surjections, and automorphisms respectively. A subgroup of a \( \Gamma \)-group that is closed under \( \Gamma \) action is called a \( \Gamma \)-subgroup, and a \( \Gamma \)-quotient is the quotient by a normal \( \Gamma \)-subgroup. We write \( G^\Gamma \) for the maximal \( \Gamma \)-subgroup of \( G \) on which \( \Gamma \) acts trivially. For a profinite group \( G \), we write \( G(\ell) \) and \( G(n) \) for the pro-\( \ell \) completion and the pro-prime-to-\( n \) completion respectively.
completion of \(G\), and for the latter, we sometimes also call it “pro-(n)’ completion”. A \([\Gamma]\)-\(\Gamma\)-group is a profinite \(\Gamma\)-group whose finite quotients all have order prime to \(|\Gamma|\).

A stem extension of \(G\) is a central extension of \(\pi : \widetilde{G} \rightarrow G\) such that \(\ker \pi \subset [\widetilde{G}, \widetilde{G}]\). A Schur covering of the group \(G\) is a stem extension of \(G\) of maximal possible order; or equivalently, a central extension \(\pi : \widetilde{G} \rightarrow G\) such that under the universal coefficients theorem map \(H^2(G, \ker \pi) \rightarrow \text{Hom}(H_2(G, \mathbb{Z}), \ker \pi)\) the image of the class of \(\pi\) is an isomorphism. A Schur covering always exists, but is not necessarily unique. A \(\ell\)-Schur covering (resp. a \((n)\)-Schur covering) of \(G\) is a stem extension such that the image of the class of \(\pi\) maps to a quotient map \(H_2(G, \mathbb{Z}) \rightarrow \ker \pi\) and \(\ker \pi \cong H_2(G, \mathbb{Z})_{(\ell)}\) (resp. \(\ker \pi \cong H_2(G, \mathbb{Z})_{(n\ell)}\)). Two extensions \(\pi_i : G_i \rightarrow G\), \(i = 1, 2\) are called isomorphic if there exists an isomorphism \(\phi : G_1 \rightarrow G_2\) such that \(\pi_2 \circ \phi = \pi_1\). A splitting of a quotient map \(\pi : G \rightarrow G\) is a (not necessarily homomorphic) map \(s : G \rightarrow G\) such that \(\pi \circ s\) is the identity map. For a global field \(K\) and a set \(S\) of primes of \(K\), we write \(G_S(K)\) for the Galois group of the maximal unramified-outside-\(S\) extension of \(K\), and write \(K_S/K\) for the corresponding field extension.

Acknowledgement. I would like to thank Nigel Boston, Wei Ho and Melanie Matchett Wood for insightful conversations and encouragements, and Shizhang Li for helpful discussions regarding the proof of Lemma 2.11. I thank Nathan Dunfield, Shelly Harvey and Chris Leininger for discussions regarding 3-manifolds. I also thank Nigel Boston, Nathan Dunfield, Shizhang Li, Will Sawin, Melanie Matchett Wood and Foling Zou for comments on an early draft. I am partially supported by NSF Grant DMS-2200541.

2. Definition of the invariants

2.1. Group theoretical definition of the invariant \(\omega_K\). Let \(K\) be a global field of \(\text{char}(K) = p > 0\) and let \(k \subset K\) be the finite constant field with algebraic closure \(\bar{k}\). Assume that \(K/k(t)\) is split completely at the place \(\infty\). Then considering an exact sequence

\[
1 \rightarrow G_0(K\bar{k}) \rightarrow G_0(K) \rightarrow \text{Gal}(\bar{k}(t)/k(t)) = \hat{\mathbb{Z}} \cdot \text{Frob}_k \rightarrow 1, \tag{2.1}
\]

where \(\text{Frob}_k\) is the Frobenius element of \(k\), there is a homomorphic splitting \(\hat{\mathbb{Z}} \cdot \text{Frob}_k \rightarrow G_0(K)\) defined by identifying \(\text{Frob}_k\) with the Frobenius element in a decomposition group of \(K_0/K\) at a preselected place of \(K\) over \(\infty\). Then this splitting defines a \(\text{Frob}_k\) action on \(G_0(K\bar{k})\) by conjugation in \(G_0(K)\).

Let \(\Gamma\) be a finite group, and we further assume that \(K\) is a Galois extension of \(k(x)\) with Galois group isomorphic to \(\Gamma\). Then \(\text{Gal}(K_0/K\bar{k}(t))\) acts on its normal subgroup \(G_0(K\bar{k})\) by conjugation, and therefore \(\text{Gal}(K\bar{k}/\bar{k}(t)) \approx \Gamma\) naturally gives an outer action on \(G_0(K\bar{k})\). We let \(G_0(K\bar{k})_{[p|\Gamma]}\) denote the pro-prime-to-\(p\) completion of \(G_0(K\bar{k})\). Then the outer action of \(\Gamma\) on \(G_0(K\bar{k})\) lifts to a \(\Gamma\) action on \(G_0(K\bar{k})_{[p|\Gamma]}\). This lift is not unique, but by the Schur–Zassenhaus theorem, all lifts are conjugate, and thus we pick one such lift. Note that \(G_0(K\bar{k})_{[p|\Gamma]}\) is the quotient of \(G_0(K\bar{k})\) modulo a characteristic normal subgroup, so it has a \(\text{Frob}_k\) action induced from (2.1).

Throughout this section, we use the following notation.

Notation 2.1. \(\bullet\) Let \(k\) be a finite field of \(\text{char}(k) = p > 0\), \(\Gamma\) a non-trivial finite group of order not divisible by \(p\), and \(K/k(t)\) a \(\Gamma\)-extension that is split completely at \(\infty\).

\(\bullet\) Let \(G_0(K)\) denote the pro-prime-to-\(p\) completion of \(G_0(K\bar{k})\), and \(K_0\) denote the corresponding field extension of \(K\). We’ve seen that \(G_0(K)\) has the actions of \(\text{Frob}_k\) and \(\Gamma\).

\(\bullet\) Let \(G_0^\#(K)\) denote the maximal \(\Gamma\)-equivariant quotient of \(G_0(K)\) such that the induced \(\text{Frob}_k\) action on it is trivial. Then \(G_0^\#(K)\) is naturally a quotient of \(G_0(K)\) by (2.1),
and we let \( K'_O/K \) denote the corresponding extension. Equivalently, \( K'_O \) is the maximal unramified extension of \( K \), that is split completely at all places of \( K \) over \( \infty \) and of order prime to \( |\Gamma| \) and \( p \).

- Similarly, for a prime \( \ell \) that is prime to \( p|\Gamma| \), \( G'_O(K)(\ell) \) is the pro-\( \ell \) completion of \( G_O(K\overline{K}) \), and we let \( K'_O(\ell) \) denote the corresponding field extension of \( K\overline{K} \). The pro-\( \ell \) completion \( G'_O(K)(\ell) \) of \( G'_O(K) \) is the maximal \( \Gamma \)-equivariant quotient of \( G'_O(K)(\ell) \) such that the induced \( \text{Frob} \) action on it is trivial, and we let \( K'_O(\ell)/K \) denote the corresponding extension.

Then the quotient maps in Notation 2.1 define a \( \Gamma \)-equivariant surjection \( G_O(K\overline{K}) \to \text{Gal}(K'_O/K) \), and hence we obtain the following group surjection

\[
\rho_K : \text{Gal}(K'_O/\overline{K}(t)) \to \text{Gal}(K'_O/K(t)) \simeq \text{Gal}(K'_O/K) \times \Gamma.
\] (2.2)

**Lemma 2.2.** There is a \( \text{Frob}_k \)-equivariant isomorphism

\[
H^2(\text{Gal}(K'_O(\ell)/\overline{K}(t)), \mathbb{Z}_\ell(1)) \simeq \mathbb{Z}_\ell \tag{2.3}
\]

for any \( \ell \nmid p|\Gamma| \); and there is a \( \text{Frob}_k \)-equivariant isomorphism

\[
H^2(\text{Gal}(K'_O/\overline{K}(t)), \mathbb{Z}(1)(p|\Gamma)|') \simeq \hat{\mathbb{Z}}(1)(p|\Gamma)|' \tag{2.4}
\]

As a consequence, there are \( \text{Frob}_k \)-equivariant isomorphisms

\[
H_2(\text{Gal}(K'_O(\ell)/\overline{K}(t)), \mathbb{Z}(\ell)) \simeq \mathbb{Z}(1) \quad \text{and} \quad H_2(\text{Gal}(K'_O/\overline{K}(t)), \mathbb{Z})(p|\Gamma)|' \simeq \hat{\mathbb{Z}}(1)(p|\Gamma)|'.
\] (2.5)

**Proof.** Denote the smooth projective curve over \( k \) associated to \( K \) by \( X_K \) and let \( X_\ell \) denote the base change of \( X \) to \( \overline{K} \). The Galois group \( G_O(K\overline{K}) \) is exactly the étale fundamental groups \( \pi^\text{ét}_1(X_\ell) \).

Because we assume that \( \Gamma \) is non-trivial, so \( X \) has positive genus, then by [NSW08, Remark, page 607], the group cohomology of \( G_O(K\overline{K}) \) agrees with the étale cohomology of \( X_\ell \). Then by the Poincaré duality, for a prime \( \ell \nmid p|\Gamma| \) and a positive integer \( n \), we have a functorial isomorphism

\[
H^2(G_O(K\overline{K}), \mu_{\ell^n}) \simeq \mathbb{Z}/\ell^n\mathbb{Z},
\] (2.6)

where both sides have trivial actions of \( \text{Frob}_k \) and \( \Gamma \).

We consider the inflation map \( \iota_1 : H^2(G'_O(K), \mu_{\ell^n}) \to H^2(G_O(K\overline{K}), \mu_{\ell^n}) \). Because \( G'_O(K) \) is the pro-prime-to-\( p|\Gamma| \) completion of \( G_O(K\overline{K}) \), we have \( H^1(\ker(G_O(K\overline{K}) \to G'_O(K)), \mu_{\ell^n}) = 0 \), and hence, it follows by the Hochschild–Serre exact sequence that \( \iota_1 \) is an injection. Similarly, the inflation map \( \iota_2 : H^2(G'_O(K)(\ell), \mu_{\ell^n}) \to H^2(G'_O(K), \mu_{\ell^n}) \) is an injection. Note that \( G'_O(K)(\ell) \) is a pro-\( \ell \) Demuškin group with free abelianization \([\text{NSW08, Thm.10.1.2(ii)}]\). Then, because \( G'_O(K)(\ell) \) acts trivially on \( \mu_{\ell^n} \), it follows by the definition of Demuškin group that there is an isomorphism

\[
H^2(G'_O(K)(\ell), \mu_{\ell^n}) \simeq \mathbb{Z}/\ell^n\mathbb{Z}.
\]

Therefore (2.6) implies that the injections \( \iota_1 \) and \( \iota_2 \) are isomorphisms. By taking inverse limit over all \( n \) and the fact that \( \hat{\mathbb{Z}}(1)(p|\Gamma)|' \) is the \( \prod \mathbb{Z}(1) \) for all primes \( \ell \nmid p|\Gamma| \), we have

\[
H^2(G'_O(K)(\ell), \mathbb{Z}(\ell)) \simeq \mathbb{Z}(\ell) \quad \text{and} \quad H^2(G'_O(K), \hat{\mathbb{Z}}(1)(p|\Gamma)|') \simeq \hat{\mathbb{Z}}(1)(p|\Gamma)|',
\]

and they both have trivial actions of \( \text{Frob}_k \) and \( \Gamma \). Then by the Hochschild–Serre spectral sequence, we have

\[
H^2(\text{Gal}(K'_O(\ell)/\overline{K}(t)), \mathbb{Z}(1)(p|\Gamma)|') = H^2(G'_O(K), \hat{\mathbb{Z}}(1)(p|\Gamma)|')^\Gamma \simeq \hat{\mathbb{Z}}(1)(p|\Gamma)|',
\]

and similarly, \( H^2(\text{Gal}(K'_O(\ell)/\overline{K}(t)), \mathbb{Z}(\ell)) \simeq \mathbb{Z}(\ell) \), which proves (2.3) and (2.4).

Let \( G \) denote \( \text{Gal}(K'_O/\overline{K}(t)) \). Since the class group of \( \overline{K}(t) \) is trivial, \( G^{ab} \) is generated by all the inertia subgroups of the maximal abelian subextension of \( K'_O/\overline{K}(t) \). Since \( K'_O/\overline{K} \) is unramified, each inertia subgroup of \( K'_O/\overline{K}(t) \) is isomorphic to its image in \( \text{Gal}(K\overline{K}/\overline{K}(t)) \simeq \Gamma \). So the exponent
of $G^{ab}$ divides $|\Gamma|$, and hence $\text{Ext}^1_{\mathbb{Z}}(G^{ab}, \hat{\mathbb{Z}}(1)_{(p|\Gamma)')} = 0$. Because $G$ acts trivially on $\hat{\mathbb{Z}}(1)_{(p|\Gamma)'}$, it follows by the universal coefficient theorem and (2.4) that, for any $n$ that is prime to $p|\Gamma$,

$$\text{Hom}(H_2(G, \mathbb{Z}), \mathbb{Z}/n\mathbb{Z}) \simeq H^2(G, \mathbb{Z}/n\mathbb{Z}) = \mu_n.$$ 

So $H_2(G, \mathbb{Z})/nH_2(G, \mathbb{Z}) \simeq \mu_n$, and by taking the inverse limit over all such $n$, we have

$$H_2(G, \mathbb{Z})_{(p|\Gamma)'} \simeq \hat{\mathbb{Z}}(1)_{(p|\Gamma)'}.$$ 

By applying the same argument, we can prove $H_2(\text{Gal}(K'_G/\mathbb{Q}), \mathbb{Z})(t) \simeq \mathbb{Z}_t(1)$. 

**Corollary 2.3.** There are isomorphisms

$$H^2(\text{Gal}(K'_G/\mathbb{Q}(t)), \hat{\mathbb{Z}}(1)_{(p|\Gamma)'}) \simeq \hat{\mathbb{Z}}(1)_{(p|\Gamma)'}$$

and $H^2(\text{Gal}(K'_G/\mathbb{Q}(t)), \mathbb{Z}_t(1)) \simeq \mathbb{Z}_t(1)$.

**Proof.** Consider the short exact sequence

$$1 \rightarrow \text{Gal}(K'_G/\mathbb{Q}(t)) \rightarrow \text{Gal}(K'_G/\mathbb{Q}(t)) \rightarrow \text{Gal}(\mathbb{Q}(t)/\mathbb{Q}(t)) \rightarrow 1$$

Since $\text{Gal}(\mathbb{Q}(t)/\mathbb{Q}(t))$ is a free group generated by Frobenius, it has cohomological dimension 1. Then by the Hochschild–Serre spectral sequence (e.g. by [NSW08, Chap.II, §4, Ex.4]), there is an exact sequence

$$0 \rightarrow H^1(\text{Gal}(\mathbb{Q}(t)/\mathbb{Q}(t)), H^1(\text{Gal}(K'_G/\mathbb{Q}(t)), \hat{\mathbb{Z}}(1)_{(p|\Gamma)'})) \rightarrow H^2(\text{Gal}(K'_G/\mathbb{Q}(t)), \hat{\mathbb{Z}}(1)_{(p|\Gamma)'}).$$

Recall that $\text{Gal}(K'_G/\mathbb{Q}(t)) \simeq \text{Gal}(K'_G/\mathbb{T}) \times \Gamma$, where $\text{Gal}(K'_G/\mathbb{T})$ is pro-$p$ completion of $\text{Gal}(K)$. We showed in the proof of Lemma 2.2 that the abelianization of $\text{Gal}(K'_G/\mathbb{T}(t))$ has exponent dividing $|\Gamma|$, so

$$H^1(\text{Gal}(K'_G/\mathbb{T}(t)), \hat{\mathbb{Z}}(1)_{(p|\Gamma)'}) = \text{Hom}((\text{Gal}(K'_G/\mathbb{T}(t)), \hat{\mathbb{Z}}(1)_{(p|\Gamma)'})) = 0.$$ 

So, the first isomorphism in the corollary follows by (2.7) and Lemma 2.2, and the second isomorphism in the corollary follows by similar arguments.

We recall the definition of admissible $\Gamma$-groups in [LWZB19]: for a finite group $\Gamma$, a profinite $\Gamma$-group is admissible if it is of order prime to $|\Gamma|$ and is topologically generated, under the $\Gamma$ action, by the elements in the form of $g^{-1}\gamma(g)$ for $g \in G, \gamma \in \Gamma$. In particular, for an admissible $\Gamma$-group $H$, one can check that $(H \rtimes \Gamma)^{ab} \simeq \Gamma^{ab}$.

**Lemma 2.4.** (1) The action of $\text{Gal}(K/\mathbb{T}(t)) \simeq \Gamma$ on $G'_G(K)$ makes $G'_G(K)$ an admissible $\Gamma$-group.

(2) The $(p|\Gamma)'$-Schur covering of $\text{Gal}(K'_G/\mathbb{T}(t))$ has kernel isomorphic to $\hat{\mathbb{Z}}_{(p|\Gamma)'}$:

$$1 \rightarrow \hat{\mathbb{Z}}_{(p|\Gamma)'} \rightarrow \hat{\mathbb{G}} \xrightarrow{\pi} \text{Gal}(K'_G/\mathbb{T}(t)) \rightarrow 1. \tag{2.8}$$

Moreover, such $(p|\Gamma)'$-Schur covering is unique up to isomorphism; that is, if there are two such coverings $\pi_i : G_i \rightarrow \text{Gal}(K'_G/\mathbb{T}(t))$ for $i = 1, 2$, then there is an isomorphism $\phi : G_1 \rightarrow G_2$ such that $\pi_1 = \pi_2 \circ \phi$.

(3) There exists a unique Frobenius action on the group $\hat{\mathbb{G}}$ in (2.8), with which (2.8) becomes a short exact sequence of Frobenius $p$-groups

$$1 \rightarrow \hat{\mathbb{Z}}(1)_{(p|\Gamma)'} \rightarrow \hat{\mathbb{G}} \xrightarrow{\pi} \text{Gal}(K'_G/\mathbb{T}(t)) \rightarrow 1. \tag{2.9}$$

**Proof.** We let $H$ denote $G'_G(K)$ and $G$ denote $\text{Gal}(K'_G/\mathbb{T}(t))$, so $G \simeq H \rtimes \Gamma$. The subgroup of $H$ generated by elements $\{h^{-1}\gamma(h) | h \in H, \gamma \in \Gamma\}$ is the commutator subgroup $[H, \Gamma]$ of $G$, which is a normal subgroup contained in $H$. Then $H/[H, \Gamma]$ is a quotient of $H$ with the trivial action of $\Gamma$, hence $H/[H, \Gamma]$ is not admissible.
and hence it is a quotient of $G$. However, such quotient corresponds to an unramified extension of $\mathbb{K}(t)$, which must be trivial. So $H = [H, \Gamma]$, which proves (1).

We denote $A := \hat{Z}_{(p|\Gamma)'}$. Note that $H^2(G, A) \simeq \text{Ext}(G, A)$; and to see this correspondence explicitly, we can construct a group extension for every cohomology class $c$. For each $c \in H^2(G, A)$, there is a normalized 2-cocycle $\alpha$ contained in $c$, i.e., a cocycle such that $\alpha(g, 1) = \alpha(1, g) = 0$ for any $g \in G$. Then the equivalent class of group extensions corresponding to $c$ can be represented by a group $\widetilde{G}$ with underlying set $A \times G$ and the multiplicative rule

$$(a, x)(b, y) = (a + x(b) + \alpha(x, y), xy),$$

and the extension

$$1 \rightarrow A \rightarrow \widetilde{G} \xrightarrow{\pi} G \rightarrow 1,$$

(2.10)

where the surjection $\pi$ is the projection to the second component. Since $G$ acts trivially on $A$, (2.10) is a central extension, so it is a stem extension if and only if the central extension reduced from (2.10) obtained by modulo $mA$ from $\widetilde{G}$ is nonsplit for any $m \in \hat{Z}_{(p|\Gamma)'}$, which happens exactly when the image of $c$ in $H^2(G, A/mA)$ is nonzero. From the proof of Lemma 2.2, we see that, forgetting the $\text{Frob}_k$-action,

$$H^2(G, A/mA) \simeq \mathbb{Z}/m\mathbb{Z}$$

as groups for any $m \in \hat{Z}_{(p|\Gamma)'}$. Thus, we see that (2.10) is a stem extension if and only if the image of $c$ under the isomorphism (2.4) is contained in $\hat{Z}_{(p|\Gamma)'}$. We denote the set of these classes corresponding to stem extensions by $\mathcal{C}$.

Next, we show that the group extension (2.10) defined by all the cohomological classes in $\mathcal{C}$ are isomorphic to each other. We pick a $c$ in $\mathcal{C}$, let $\alpha$ be the normalized 2-cocycle in $c$ and let $G$ be the group extension defined by $\alpha$. Then for any $d \in \mathcal{C}$, we can write $d$ as $mc$ for some $m \in \hat{Z}_{(p|\Gamma)'}$, and $ma$ is the normalized 2-cocycle contained in $d$. We let $\widetilde{G}_d$ represent the group extension defined by $ma$. Then there is an isomorphism

$$\widetilde{G} \xrightarrow{\sim} \widetilde{G}_d$$

defined by $(a, 1) \mapsto (ma, 1)$ for all $a \in A$

$$(0, x) \mapsto (0, x)$$

for all $x \in G$,

which clearly gives an isomorphism between the extensions $\widetilde{G} \rightarrow G$ and $\widetilde{G}_d \rightarrow G$. Then by (2.5), these stem extensions are $(p|\Gamma)'$-Schur coverings, so we finish the proof of the statement (2).

Denote $A(1) := \hat{Z}(1)_{(p|\Gamma)'}$. We can apply the argument above about group extensions to $\text{Gal} (K'_0/k(t))$ and see that the each equivalence classes of group extensions

$$1 \rightarrow A(1) \rightarrow \hat{G} \xrightarrow{\hat{\pi}} \text{Gal}(K'_0/k(t)) \rightarrow 1$$

(2.11)

is represented by a class in $H^2(\text{Gal}(K'_0/k(t)), A(1))$. By taking restriction, we get a group extension

$$1 \rightarrow A(1) \rightarrow \hat{\pi}^{-1}(G) \rightarrow G \rightarrow 1,$$

(2.12)

and it is a central extension since $G$ acts trivially on $A(1)$. So (2.12) is a stem extension if and only if the extension obtained by quotienting $\hat{G}$ in (2.11) by $mA(1)$ is nonsplit for any $m$, which happens exactly when the image of the corresponding cohomology class $c$ in $H^2(\text{Gal}(K'_0/k(t)), \mu_m)$ is nonzero for any $m \in \hat{Z}_{(p|\Gamma)'}$. From the proof of Lemma 2.2 and Corollary 2.3, we see that

$$H^2(\text{Gal}(K'_0/k(t)), \mu_m) \simeq H^2(G, \mu_m)^{\text{Gal}(\mathbb{K}(t)/k(t))} \simeq \mathbb{Z}/m\mathbb{Z}.$$
So (2.12) is a stem extension if and only if the image of $c$ under the first isomorphism in Corollary 2.3 is contained in $\hat{\mathbb{Z}}_{(p|\Gamma)}^\times$. Then by using the same argument in the proof of the statement (2), we see that all of the extensions (2.11) corresponding to such cohomological classes are isomorphic.

We fix an extension (2.11) such that (2.12) is a stem extension. Recall that we identify $\text{Frob}_k$ as an element of $\text{Gal}(K'_0/k(t))$ whose image in $\text{Gal}(\overline{k}(t)/k(t))$ is a generator. Then we pick an element $f$ in $\hat{\pi}^{-1}(\text{Frob}_k)$. Since $\text{Gal}(K'_0/k(t)) = G \times \langle \text{Frob}_k \rangle$ and $f$ generate a free subgroup of $\text{Gal}(K'_0/k(t))$, we have that

$$\hat{G} = \hat{\pi}^{-1}(G) \rtimes \langle f \rangle,$$

which gives an action of $f$ (defined by conjugation) on every term of (2.12). This $f$-action does not depend on the choice of $f$, because two different choices of $f$ differ by an element of $\hat{\mathbb{Z}}(1)_{(p|\Gamma)}^\times$, which is contained in the center of $\pi^{-1}(G)$. So this unique $f$-action on (2.12) gives the exact sequence in the statement (3).

The following is a group theoretical property of stem extensions that will be useful in this paper.

**Lemma 2.5.** Let $1 \to A \to \tilde{G} \to G \to 1$ be a stem extension. If $H$ is a subgroup of $\tilde{G}$ that maps surjectively to $G$, then $H = \tilde{G}$.

**Proof.** Since $\tilde{G} = AH$, all the conjugates of the subgroup $H$ are in the form of $a^{-1}Ha$ for $a \in A$. However, $A$ is in the center of $\tilde{G}$, so $a^{-1}Ha = H$, which implies that $H$ is a normal subgroup of $\tilde{G}$. If $H$ is a proper subgroup of $\tilde{G}$, then $\tilde{G}/H$ is a non-trivial abelian group, so $A$ is not contained in the commutator subgroup of $\tilde{G}$, which contradicts to the assumption that the group extension is stem. \qed

The following is a group theoretical property of stem extensions that will be useful in this paper.

**Lemma 2.5.** Let $1 \to A \to \tilde{G} \to G \to 1$ be a stem extension. If $H$ is a subgroup of $\tilde{G}$ that maps surjectively to $G$, then $H = \tilde{G}$.

**Proof.** Since $\tilde{G} = AH$, all the conjugates of the subgroup $H$ are in the form of $a^{-1}Ha$ for $a \in A$. However, $A$ is in the center of $\tilde{G}$, so $a^{-1}Ha = H$, which implies that $H$ is a normal subgroup of $\tilde{G}$. If $H$ is a proper subgroup of $\tilde{G}$, then $\tilde{G}/H$ is a non-trivial abelian group, so $A$ is not contained in the commutator subgroup of $\tilde{G}$, which contradicts to the assumption that the group extension is stem. \qed

The function field extension $K\overline{k}/\overline{k}(t)$ corresponds to a ramified Galois $\Gamma$-cover $C \to \mathbb{P}^1_{\overline{k}}$ and we let $P_1, \ldots, P_m \in \mathbb{P}^1_{\overline{k}}$ denote the branch loci of this covering. So there is a natural surjection

$$\pi_1^\text{\text{et}}(\mathbb{P}^1_{\overline{k}} - \{P_1, \ldots, P_m\}) \to \text{Gal}(K_0'/\overline{k}(t)) \to \text{Gal}(K\overline{k}/\overline{k}(t)).$$

By the Grothendieck’s theory of specialization and the description of the fundamental group of a Riemann surface, the pro-prime-to-$p$ completion of the étale fundamental group above, which we will denote by $\Omega_K$, is a free pro-prime-to-$p$ group on $m - 1$ generators and has a presentation

$$\Omega_K := \pi_1^\text{\text{et}}(\mathbb{P}^1_{\overline{k}} - \{P_1, \ldots, P_m\})_{(p^\infty)} = \langle g_1, \ldots, g_m \mid g_1g_2\cdots g_m = 1 \rangle \quad (2.13)$$

where the image of $g_i$ in $\Omega_K$ is a generator of an inertia group of $P_i$, and is mapped to a generator of an inertia subgroup at $P_i$ of $\text{Gal}(K_0'/\overline{k}(t))$ (and resp. of $\text{Gal}(K\overline{k}/\overline{k}(t))$). We call the tuple $\underline{g} := (g_1, \ldots, g_m)$ satisfying the description above for an arbitrary ordering of $P_1, \ldots, P_m$ by a system of inertia generators for $K$. The systems of inertia generators are not unique. The Frobenius $\text{Frob}_k$ acts on each Galois group, and hence we obtain a $\text{Frob}_k$-equivariant surjection when we choose compatible lifts of $\text{Frob}_k$

$$\varpi_K : \Omega_K \to \text{Gal}(K_0'/\overline{k}(t)). \quad (2.14)$$

By (2.13), $\Omega_K$ is a quotient of the free pro-prime-to-$p$ group generated by $g_1, \ldots, g_m$. So we obtain a surjection of groups

$$\rho_K : \langle g_1, \ldots, g_m \rangle \to \text{Gal}(K_0'/\overline{k}(t)), \quad (2.15)$$

which factors through $\varpi_K$. The map $\rho_K$ is just a group surjection, because the free group $\langle g_1, \ldots, g_m \rangle$ does not have any natural $\text{Frob}_k$-action.
Let \( z = t - a_i \) for some \( a_i \in \overline{K} \) corresponds to the branch locus \( P_t \). Then an inertia subgroup \( \text{Gal} \left( k((z^{1/\infty})) / k((z)) \right) \) at \( P_t \) of \( \pi_1^\Theta \left( \{ P_1, \ldots, P_m \} \right) \) is naturally identified with \( \hat{\mathbb{Z}}(1) \) via
\[
\text{Gal} \left( k((z^{1/\infty})) / k((z)) \right) \rightarrow \hat{\mathbb{Z}}(1)
\]
\[
\sigma \mapsto \lim_m \left( \frac{\sigma(\sqrt[m]{z})}{\sqrt[m]{z}} \right).
\]
Under these identifications, by [Woo21, §5.1 & 5.2], in the presentation \( (2.13) \), each inertia generator \( g_i \) for \( i = 1, \ldots, m \) maps to a common generator of \( \hat{\mathbb{Z}}(1) \). For a system of inertia generators \( g = (g_1, \ldots, g_m) \), we let \( I(g) \) denote the common generator of \( \hat{\mathbb{Z}}(1) \).

For a central group extension \( \pi : G \rightarrow H \) with an isomorphism \( \ker \pi \cong A \) for some abelian group \( A \), the differential map \( d_\pi \) of \( \pi \) is the homomorphism
\[
d_\pi : H_2(G, \mathbb{Z}) \rightarrow A
\]
that is the image of the class containing \( \pi \) under the quotient map \( H^2(G, A) \rightarrow \text{Hom}(H_2(G, \mathbb{Z}), A) \) in the universal coefficient theorem.

**Proposition 2.6.** Let \( \hat{G}, \pi \) be as described in the group extension \( (2.8) \) in Lemma 2.4, and let \( \rho_K \) be the surjection \( (2.15) \).

1. Then there is a unique surjection
\[
\tilde{\rho}_K : (g_1, \ldots, g_m) \rightarrow \hat{G},
\]
such that \( \rho_K = \pi \circ \tilde{\rho}_K \) and \( \text{ord}(\tilde{\rho}_K(g_i)) = \text{ord}(\rho_K(g_i)) \) for each \( i = 1, \ldots, m \).
2. The kernel of \( \pi \) is generated by \( \tilde{\rho}_K(g_1 \cdots g_m) \). So we can define a Frob\(_K\)-equivariant isomorphism
\[
\iota_\pi : \hat{\mathbb{Z}}(1)(\rho_1(\Gamma)) \rightarrow \ker \pi
\]
\[
I(g) \mapsto \tilde{\rho}_K(g_1 \cdots g_m).
\]
Moreover, this isomorphism is independent of the choice of the system of inertia generators.

3. The differential map \( d_\pi : H_2(\text{Gal}(K'_O / K(t)), \mathbb{Z})) \rightarrow \ker \pi \) of \( \pi \) factors through a Frob\(_K\)-equivariant isomorphism \( H_2(\text{Gal}(K'_O / K(t)), \mathbb{Z})(\rho_1(\Gamma)) \rightarrow \ker \pi \), which by abuse of notation will be also denoted by \( d_\pi \). Then the Frob\(_K\)-equivariant isomorphism \( \omega_K := d_\pi \circ \iota_\pi : \hat{\mathbb{Z}}(1)(\rho_1(\Gamma)) \rightarrow H_2(\text{Gal}(K'_O / K(t)), \mathbb{Z})(\rho_1(\Gamma)) \) does not depend on the choice of the stem extension \( \pi \).

**Remark 2.7.** The isomorphism \( \iota_\pi \) identifies \( \hat{G} \) as a group extension of \( \text{Gal}(K'_O / K(t)) \) with kernel \( \hat{\mathbb{Z}}(1)(\rho_1(\Gamma)) \), and hence corresponds to an element \( \epsilon \) in \( H^2(\text{Gal}(K'_O / K(t)), \hat{\mathbb{Z}}(1)(\rho_1(\Gamma))) \). Then the differential map \( H_2(\text{Gal}(K'_O / K(t)), \mathbb{Z})(\rho_1(\Gamma)) \rightarrow \hat{\mathbb{Z}}(1)(\rho_1(\Gamma)) \) obtained from \( \epsilon \) is the inverse of \( \omega_K \).

**Proof.** We let \( \overline{g_i} \) be the image of \( g_i \) in \( \Omega_K \). We denote \( t_i := \varpi_K(\overline{g_i}) \) for each \( i \) (\( \varpi_K \) is the map \( (2.14) \)), which is a generator of an inertia subgroup at \( P_t \) of \( \text{Gal}(K'_O / K(t)) \). Then \( \text{ord}(t_i) \) equals the order of its image in \( \text{Gal}(KK(t)) \simeq \Gamma \) because \( K'_O \) is unramified over \( KK(t) \). By definition \( \rho_K \) is a lift of \( \varpi_K \), \( \rho_K(g_i) = t_i \) and hence \( \text{ord}(\rho_K(g_i)) = \text{ord}(t_i) \). Consider the central group extension \( (2.8) \). The kernel has order prime to \( |\Gamma| \), so for each \( i \), there exists a unique lift \( \overline{t}_i \in \pi^{-1}(t_i) \) of \( t_i \) in \( \hat{G} \) such that \( \text{ord}(\overline{t}_i) = \text{ord}(t_i) \). The elements \( \overline{t}_i \)'s generate a subgroup of \( \hat{G} \) that maps surjectively to \( \text{Gal}(K'_O / K(t)) \), and therefore by Lemma 2.5, they generate \( \text{Gal}(K'_O / K(t)) \) because \( (2.8) \) is a stem extension. So the homomorphism \( (g_1, \ldots, g_m) \rightarrow \hat{G} \) mapping \( g_i \) to \( \overline{t}_i \) is a surjection, and is the unique surjection satisfies the conditions for \( \tilde{\rho}_K \) given in (1).
By the properties of \( \tilde{\rho}_K \), the image of \( g_i \) in \( \tilde{G} \) has order equal to \( \text{ord}(t_i) \). So the surjection \( s \) defines a \( \tilde{G} \)-extension \( L/\mathbb{K}(t) \) that contains \( K'_\mathcal{O} \) as a subfield, and its inertia subgroup at \( P_i \) maps isomorphically to the inertia subgroup at \( \tilde{P}_i \) of \( K'_\mathcal{O}/\mathbb{K}(t) \). Thus, \( L \) is unramified over \( K'_\mathcal{O} \) and hence is unramified over \( \mathbb{K} \), and moreover, \( \text{Gal}(L/\mathbb{K}) \) is pro-prime-to-\( (p|\Gamma') \). By definition of \( K'_\mathcal{O} \), we see that \( L \) must be \( K'_\mathcal{O} \), so \( r \) generates \( \ker \pi \).

Assume that \( h := (h_1, \ldots, h_m) \) is another system of inertia generators. Then there exists \( \alpha \in \mathbb{Z}(1)_{(p)}^\alpha \) such that \( I(h) = I(g)^\alpha \), and there is a permutation \( \sigma \in S_m \) such that \( h_i \) is conjugate to \( g_\sigma(i)^\alpha \) for all \( i \). Then \( h \) defines a surjection \( \rho_K' : \langle h_1, \ldots, h_m \rangle \to \text{Gal}(K'_\mathcal{O}/\mathbb{K}(t)) \), where \( h_i \) maps to the corresponding inertia generator, and \( \rho_K' \) lifts to a surjection \( \tilde{\rho}_K' : \langle h_1, \ldots, h_m \rangle \to \tilde{G} \) such that \( \text{ord}(\tilde{\rho}_K'(h_i)) = \text{ord}(\rho_K'(h_i)) \) for each \( i \). To prove the last claim in the statement (2), we need to show \( \tilde{\rho}_K'(h_1 \cdots h_m) = \tilde{\rho}_K(g_1 \cdots g_m)^\alpha \).

Recall that \( \Omega_K \) is a free pro-prime-to-\( p \) group on \( m-1 \) generators. By Lemma 2.5, the surjection \( \varpi_K \) in (2.14) lifts to a surjection \( \varpi_K : \Omega_K \to \tilde{G} \) such that \( \varpi_K = \pi \circ \varpi_K \). For each \( i \), we let \( \overline{h}_i \) denote the image of \( h_i \) in \( \Omega_K \) and then define

\[
z_i := \overline{\varpi}_K(\overline{h}_i)^{-1}\tilde{\rho}_K'(h_i).
\]

Because both of \( \overline{\varpi}_K(\overline{h}_i) \) and \( \tilde{\rho}_K'(h_i) \) have image \( \rho_K'(h_i) \) in \( \text{Gal}(K'_\mathcal{O}/\mathbb{K}(t)) \), \( z_i \) is contained in \( \ker \pi \), so is in the center of \( \tilde{G} \). Thus, \( z_i \) is contained in \( \ker \pi \), so \( z_i \) is contained in the center of \( \tilde{G} \). Thus,

\[
\tilde{\rho}_K'(h_1 \cdots h_m) = \prod_{i=1}^m \overline{\varpi}_K(\overline{h}_i)z_i = \overline{\varpi}_K(\overline{h}_1 \cdots \overline{h}_m)z_1 \cdots z_m = z_1 \cdots z_m.
\]

Similarly, we define \( w_i := \overline{\varpi}_K(\overline{g}_i)^{-1}\tilde{\rho}_K(g_i) \) for each \( i \). Then \( w_i \) is in the center of \( \tilde{G} \) and \( \tilde{\rho}_K(g_1 \cdots g_m) = w_1 \cdots w_m \cdot \tilde{\rho}_K(g_1 \cdots g_m) \). Now, we fix an index \( i \) and suppose \( j = \sigma(i) \). There exists \( x \in \Omega_K \) such that \( h_i = x^{-1}g_j x \). We pick the lift \( y = \varpi_K(x) \) of \( \varpi_K(x) \). Then \( y^{-1}\tilde{\rho}_K(g_j)^\alpha y \) has order equal to \( \text{ord}(\tilde{\rho}_K(g_j)) = \text{ord}(\rho_K(g_j)) = \text{ord}(\rho_K'(h_i)) \) and is a lift of \( \rho_K'(h_i) \), so \( y^{-1}\tilde{\rho}_K(g_j)^\alpha y = \tilde{\rho}_K(h_i) \). Then

\[
z_i = \overline{\varpi}_K(\overline{h}_i)^{-1}\tilde{\rho}_K'(h_i) = y^{-1}\overline{\varpi}_K(\overline{g}_j)^{-1}\tilde{\rho}_K(g_j)^\alpha y = y^{-1}w_j(\tilde{\rho}_K(g_j)^{-2}w_j^2 \tilde{\rho}_K(g_j)^{-1})(\tilde{\rho}_K(g_j)^{-2}w_j^2 \tilde{\rho}_K(g_j)^{-1})(\tilde{\rho}_K(g_j)^{-2}w_j^2 \tilde{\rho}_K(g_j)^{-1}) \cdots (\tilde{\rho}_K(g_j)^{-2}w_j^2 \tilde{\rho}_K(g_j)^{-1}) y = w_j^\alpha.
\]

So we finish the proof of (2).

Since \( \pi \) defines a stem extension, its corresponding differential map is surjective, so \( d_\pi \) defined in (3) is a Frobenius-equivariant isomorphism because of (2.5) in Lemma 2.2. Suppose there are two stem extensions \( 1 \to A_i \to \tilde{G}_i \to \text{Gal}(K'_\mathcal{O}/\mathbb{K}(t)) \to 1 \) for \( i = 1, 2 \). By Lemma 2.4 (2) and (3), there exists an Frobenius-equivariant isomorphism \( \phi : \tilde{G}_1 \to \tilde{G}_2 \) such that \( \pi_1 = \pi_2 \circ \phi \), so \( \phi|_{A_i} : A_1 \to A_2 \) is an isomorphism. Then the differential map \( d_{\pi_i} \) satisfies \( d_{\pi_2} = \phi|_{A_1} \circ d_{\pi_1} \). For each \( i \), let \( \iota_{\pi_i} \)
denote the map in (2.16) for \( \pi_i \). Then by definition of \( t_{\pi_i} \), we obtain that \( t_{\pi_2} = \phi|_{A_1} \circ t_{\pi_1} \). Thus \( d_{\pi_1}^{-1} \circ t_{\pi_1} = d_{\pi_2}^{-1} \circ t_{\pi_2} \) and then we proved (3).

Since the map \( \omega_K \) in Proposition 2.6 does not depend on the choice of \( \pi \) and the system of inertia generators, it is an invariant associated to \( K \).

**Definition 2.8** (Invariant \( \omega_K \) associated to \( K \)). We define the invariant \( \omega_K \) associated to \( K \) to be the \( \text{Pro}_{k} \)-equivariant isomorphism \( \omega_K : \hat{\mathbb{Z}}(1)_{(q|1)} \to H_2(\text{Gal}(K'/\hat{k}(t)), \mathbb{Z})_{(p|1)}' \) in Proposition 2.6(3).

### 2.2 Cohomological definition of \( \omega_K \).

As discussed in Remark 2.7, the inverse of \( \omega_K \) is the differential map of a class \( \epsilon \in H^2(\text{Gal}(K'/\hat{k}(t)), \hat{\mathbb{Z}}(1)(\mathbb{Q}/1)) \). In this subsection, we identify \( \epsilon \) as a class in the étale cohomology \( H_2^\text{ét}(X_T, \hat{\mathbb{Z}}(1)_{(p|1)}) \) for the curve \( X_T \) whose function field is \( K\hat{k} \), and we compute the trace of this class in Corollary 2.12.

**Lemma 2.9.** Use the notation in Proposition 2.6. Let \( \overline{g}_i \in \Omega_K \) denote the image of \( g_i \) under the quotient map defined by the presentation (2.13). Then there is a surjection \( \varrho_K \) that factors through \( \hat{\rho}_K \) and is defined by

\[
\varrho_K : \Omega_K \quad \longrightarrow \quad \widetilde{G}
\]

\[
\overline{g}_i \quad \longmapsto \quad \hat{\rho}_K(g_i) \quad \text{for} \quad i = 1, \ldots, m - 1.
\]

In particular, we have the following identity

\[
\hat{\rho}_K(g_1 \cdots g_m) = \varrho_K(\overline{g}_m)^{-1} \varrho_K(g_m).
\]

**Proof.** We consider the injective homomorphism

\[
\varepsilon : \Omega_K \quad \longrightarrow \quad \langle g_1, \ldots, g_m \rangle
\]

\[
\overline{g}_i \quad \longmapsto \quad g_i \quad \text{for} \quad i = 1, \ldots, m - 1.
\]

Then the composition map \( \varrho_K := \hat{\rho}_K \circ \varepsilon \) is a homomorphism from \( \Omega_K \) to \( \widetilde{G} \) such that \( \varrho_K(\overline{g}_i) = \hat{\rho}_K(g_i) \) for \( i = 1, \ldots, m - 1 \). Then, since \( \hat{\rho}_K(g_i), \ i = 1, \ldots, m - 1 \) generate \( \text{Gal}(K'/\hat{k}(t)) \), it follows by Lemma 2.5 that \( \varrho_K \) is a surjection. Because \( \overline{g}_1 \cdots \overline{g}_m = 1 \), we see that \( \varrho_K(\overline{g}_m) = \varrho_K(\overline{g}_1 \cdots \overline{g}_{m-1})^{-1} = \hat{\rho}_K(g_1 \cdots g_m)^{-1} \hat{\rho}_K(g_m). \)

**Lemma 2.10.** Let \( \widetilde{G} \) and \( \pi \) be as in the group extension (2.8) in Lemma 2.4. We define \( \overline{H} := \pi^{-1}(G'_{O}(K)) \) and \( \varpi := \pi|_{\tilde{H}}, \) and obtain the following stem extension of \( G'_{O}(K) \)

\[
1 \longrightarrow \ker \varpi \longrightarrow \overline{H} \overset{\varpi}{\longrightarrow} G'_{O}(K) \longrightarrow 1.
\]

Then, for any integer \( n \) satisfying \( \gcd(n, p|1) = 1 \), the transgression map defined by the extension \( \varpi \)

\[
t_g\varpi_\cdot n : H^1(\ker \varpi, \mathbb{Z}/n\mathbb{Z}) \longrightarrow H^2(G'_{O}(K), \mathbb{Z}/n\mathbb{Z})
\]

is an isomorphism.

**Proof.** We first show that (2.18) is a stem extension. It is central because (2.8) is central. So it suffices to prove that \( \ker \varpi \) is contained in \( [\overline{H}, \overline{H}] \), or equivalently, that the homomorphism of abelianizations \( \overline{H}^{ab} \to G'_{O}(K)^{ab} \) induced by \( \varpi \) is an isomorphism. Let \( N \) denote the kernel of \( \overline{H}^{ab} \to G'_{O}(K)^{ab} \). Then the short exact sequence \( 1 \to N \to \overline{H}^{ab} \to G'_{O}(K)^{ab} \to 1 \) has an action of \( \Gamma \) inherited from \( \pi \), and in particular, the \( \Gamma \) action on \( N \) is trivial. Because \( G'_{O}(K) \) is an admissible \( \Gamma \)-group (Lemma 2.4(1)), its abelianization is a \( \hat{\mathbb{Z}}_{(1)}'\Gamma' \)-module whose \( \Gamma \)-invariant is trivial. Then, since \( \hat{\mathbb{Z}}_{(1)}'[\Gamma'] \) is a semisimple ring, we have

\[
\overline{H}^{ab} \cong N \oplus G'_{O}(K)^{ab}.
\]
On the other hand, by taking quotient of $\tilde{G}$ in (2.8) modulo $[\tilde{H}, \tilde{H}]$, we obtain a short exact sequence

$$1 \rightarrow N \rightarrow \tilde{H}^{ab} \times \Gamma \rightarrow G'_0(K)^{ab} \times \Gamma \rightarrow 1,$$

which is a stem extension because $\pi$ is stem. The isomorphism (2.19) implies that the abelianization of $\tilde{H}^{ab} \times \Gamma$ is isomorphic to $N \times \Gamma^{ab}$. Therefore, $N$ must be trivial, so (2.18) is stem.

Consider the transgression map $t_{g_{π,n}} : H^1(\ker π, \mathbb{Z}/n\mathbb{Z}) \rightarrow H^2(\text{Gal}(K'_0/\overline{k}(t)), \mathbb{Z}/n\mathbb{Z})$ defined by $π$. Since $\text{Gal}(K'_0/\overline{k}(t))^{ab} \cong \Gamma^{ab}$ and we’ve shown that $π$ is the pro-prime-to-$p|\Gamma|$ Schur covering of $\text{Gal}(K'_0/\overline{k}(t))$, the prime-to-$p|\Gamma|$ part of the Schur multiplier of $\tilde{G}$ is trivial [Kar93, Chap.10, Prop.1.12]. So $H^2(\tilde{G}, \mathbb{Z}/n\mathbb{Z}) = 0$, and then $t_{g_{π,n}}$ is surjective. On the other hand, since $π$ is a stem extension, $\tilde{G}^{ab} \cong \text{Gal}(K'_0/\overline{k}(t))^{ab}$, so the inflation map $H^1(\text{Gal}(K'_0/\overline{k}(t)), \mathbb{Z}/n\mathbb{Z}) \rightarrow H^1(\tilde{G}, \mathbb{Z}/n\mathbb{Z})$ is an isomorphism, which shows that $t_{g_{π,n}}$ is an isomorphism.

Finally, consider the exact sequence

$$0 \rightarrow H^1(G'_0(K), \mathbb{Z}/n\mathbb{Z}) \rightarrow H^1(\tilde{H}, \mathbb{Z}/n\mathbb{Z}) \rightarrow H^1(\ker π, \mathbb{Z}/n\mathbb{Z}) \xrightarrow{t_{g_{π,n}}} H^2(G'_0(K), \mathbb{Z}/n\mathbb{Z}) \rightarrow \cdots.$$

Because $\tilde{H}^{ab} \cong G'_0(K)^{ab}$, $t_{g_{π,n}}$ is injective. Also, $t_{g_{π,n}}$ is the composition map

$$H^1(\ker π, \mathbb{Z}/n\mathbb{Z}) \xrightarrow{\cong} H^1(\ker π, \mathbb{Z}/n\mathbb{Z}) \xrightarrow{t_{g_{π,n}}} H^2(G'_0(K), \mathbb{Z}/n\mathbb{Z}) \xrightarrow{\text{res}} H^2(\text{Gal}(K'_0/\overline{k}(t)), \mathbb{Z}/n\mathbb{Z}).$$

Recall that we’ve shown in the proof of Lemma 2.2 that the map $\text{res}$ is an isomorphism. So we see that $t_{g_{π,n}}$ being injective and $t_{g_{π,n}}$ being surjective implies that $t_{g_{π,n}}$ is also an isomorphism. □

Use the notation in Lemmas 2.9 and 2.10. Let $X$ be the smooth projective curve over $k$ whose function field is $K$, and let $X_{\overline{k}}$ denote the base change of $X$ to $\overline{k}$. Assume that $n$ is a positive integer relatively prime to $p|\Gamma|$. We consider the following composition map

$$H^1(\ker π, \mu_n) \xrightarrow{t_{g_{π,n}}} H^2(G'_0(K), \mu_n) \xrightarrow{\cong} H^2_{\text{ét}}(X_{\overline{k}}, \mu_n) \xrightarrow{\text{tr}_{X,n}} \mathbb{Z}/n\mathbb{Z}. \quad (2.20)$$

Here $t_{g_{π,n}}$ is obtained by tensoring $\mu_n$ to the transgression map in Lemma 2.10. The middle arrow follows by the canonical isomorphism between Galois cohomology and étale cohomology and the fact (we proved in Lemma 2.2) that the inflation map $H^2(G'_0(K), \mu_n) \rightarrow H^2(G'_0(\overline{k}), \mu_n)$ is an isomorphism. The last arrow is the trace obtained by the Poincaré duality.

Let $i$ denote the homomorphism

$$\begin{align*}
\ker π & \xrightarrow{i} \hat{\mathbb{Z}}(1)_{(p|\Gamma)^r} \\
\rho_K(g_1 \cdots g_m) & \mapsto I(g),
\end{align*} \quad (2.21)$$

and then let $i_n : \ker π \rightarrow \mu_n$ denote the composition of $i$ and the natural surjection $\hat{\mathbb{Z}}(1)_{(p|\Gamma)^r} \rightarrow \mu_n$.

**Lemma 2.11.** The image of $i_n$ under (2.20) is $-|\Gamma| \mod n$.

**Proof.** We first recall the definition of $\text{tr}_{X,n}$. Let $C^1(X_{\overline{k}})$ be the free group on the set of prime 1-cycles on $X_{\overline{k}}$. Then the cycle map $\text{cl}_X : C^1(X_{\overline{k}}) \rightarrow H^2_{\text{ét}}(X_{\overline{k}}, \mu_n)$ is the composition of the canonical maps $C^1(X_{\overline{k}}) \rightarrow \text{Pic}(X_{\overline{k}})$ and $\text{Pic}(X_{\overline{k}}) \rightarrow H^2_{\text{ét}}(X_{\overline{k}}, \mu_n)$, and $\text{cl}_X$ maps a prime 1-cycle to the element whose $\text{tr}_{X,n}$-trace is 1. Rewriting everything in Galois cohomology, these two maps are two connecting homomorphisms. We let $S$ denote the set of all places of $K_{\overline{k}}$, and for any extension $L$ of $K_{\overline{k}}$, we let $S(L)$ denote the set of all places of $L$. Then the first map $C^1(X_{\overline{k}}) \rightarrow \text{Pic}(X_{\overline{k}})$ is the connecting homomorphism

$$\delta_1 : \bigoplus_{p \in S} \mathbb{Z} = H^0\left( G_0(K_{\overline{k}}), \bigoplus_{\mathfrak{p} \in S(K_{\overline{k}})} \mathbb{Z} \right) \rightarrow H^1\left( G_0(K_{\overline{k}}), \mathcal{O}_{K_{\overline{k}}}^\times \right).$$
associated to the short exact sequence of $G_{O}(K\overline{k})$-modules

$$1 \longrightarrow \mathcal{O}_{K_{\mathfrak{o}}}^\times \longrightarrow K_{\mathfrak{o}}^\times \oplus_{\mathfrak{p}\in S(K_{\mathfrak{o}})} \mathbb{Z} \longrightarrow 0. \tag{2.22}$$

The second map $\text{Pic}(X_{\overline{\mathfrak{g}}}) \to H^{2}_{\text{ét}}(X_{\overline{\mathfrak{g}}}, \mu_{n})$ is

$$\delta_{2} : H^{1}(G_{O}(K\overline{k}), \mathcal{O}_{K_{\mathfrak{o}}}^\times) \longrightarrow H^{2}(G_{O}(K\overline{k}), \mu_{n}),$$

associated to the Kummer sequence $1 \to \mu_{n} \to \mathcal{O}_{K_{\mathfrak{o}}}^\times \xrightarrow{n} \mathcal{O}_{K_{\mathfrak{o}}}^\times \to 1.$

There is a short exact sequence

$$1 \longrightarrow N \longrightarrow G'_{S}(K) \longrightarrow G'_{\mathfrak{o}}(K) \longrightarrow 1,$$

where $G'_{S}(K)$ denotes $G_{S}(K\overline{k})(\mathfrak{p}|\Gamma)'$. Applying the Hochschild--Serre exact sequence, we obtain

$$0 \longrightarrow H^{1}(G'_{\mathfrak{o}}(K), \mu_{n}) \longrightarrow H^{1}(G'_{S}(K), \mu_{n}) \longrightarrow H^{1}(N, \mu_{n})G'_{\mathfrak{o}}(K) \xrightarrow{t_{g}} H^{2}(G'_{\mathfrak{o}}(K), \mu_{n}) \longrightarrow 0, \tag{2.23}$$

where the last arrow uses the fact that $G'_{\mathfrak{o}}(K)$ is a free pro-prime-to-$|\Gamma|$ group. By the Riemann existence theorem (a prime-to-$p|\Gamma|$ analogue of [NSW08, Thm.(10.1.10)]), $N$ is the free product of the prime-to-$p|\Gamma|$ completions of inertia subgroups at places in $S(K'_{\mathfrak{o}})$, so

$$H^{1}(N, \mu_{n})G'_{\mathfrak{o}}(K) = \left( \bigoplus_{\mathfrak{p}\in S(K'_{\mathfrak{o}})} H^{1}(\mathcal{T}_{\mathfrak{p}}, \mu_{n}) \right)^{G'_{\mathfrak{o}}(K)} = \bigoplus_{\mathfrak{p}\in S} H^{1}(\mathcal{T}_{\mathfrak{p}}, \mu_{n}),$$

where $\mathcal{T}_{\mathfrak{p}}$ (resp. $\mathcal{T}_{\mathfrak{Q}}$) is the pro-prime-to-$p|\Gamma|$ completion of the local inertia group at $\mathfrak{p}$ (resp. $\mathfrak{Q}$).

The last equality above is because $\mathcal{T}_{\mathfrak{Q}} = \mathcal{T}_{\mathfrak{p}}$ for each $\mathfrak{Q}|\mathfrak{p}$ and $G'_{\mathfrak{o}}(K)$ acts transitively and freely on all the primes above $\mathfrak{p}$, which both follow by the fact that $K'_{\mathfrak{o}}/K\overline{k}$ is split completely at all primes. For a place $\mathfrak{p} \in S$, we let $(K\overline{k})_{\mathfrak{p}}$ denote the completion of $K\overline{k}$ at $\mathfrak{p}$. Let $a_{\mathfrak{p}}$ be a uniformizer of the prime $\mathfrak{p}$ of $(K\overline{k})_{\mathfrak{p}}$. Then $\mathcal{T}_{\mathfrak{p}}$ is the prime-to-$p|\Gamma|$ completion of the $\text{Gal}((K\overline{k})_{\mathfrak{p}}[a_{\mathfrak{p}}^{1/\infty}]/(K\overline{k})_{\mathfrak{p}})$, so there is a canonical isomorphism $\mathcal{Z}(1)(\mathfrak{p}|\Gamma)' \to \mathcal{T}_{\mathfrak{p}}$ arising from the action of $\mathcal{Z}(1)$ as ring automorphisms of $(K\overline{k})_{\mathfrak{p}}[a_{\mathfrak{p}}^{1/\infty}]$ over $(K\overline{k})_{\mathfrak{p}}$. So we can define a surjection

$$f_{\mathfrak{p}} : \mathbb{Z} \longrightarrow H^{1}(\mathcal{T}_{\mathfrak{p}}, \mu_{n})$$

$$1 \mapsto \left( \sigma \mapsto \frac{\sigma(\sqrt[n]{a_{\mathfrak{p}}})}{\sqrt[n]{a_{\mathfrak{p}}}} \right).$$

We will prove by explicitly computing the cocycles that the following diagram commutes

$$\begin{array}{ccc}
\bigoplus_{\mathfrak{p}\in S} \mathbb{Z} & \xrightarrow{\delta_{1}} & H^{1}(G_{O}(K\overline{k}), \mathcal{O}_{K_{\mathfrak{o}}}^\times) \\
\oplus f_{\mathfrak{p}} & \downarrow \cong & \\
\bigoplus_{\mathfrak{p}\in S} H^{1}(\mathcal{T}_{\mathfrak{p}}, \mu_{n}) & \xrightarrow{t_{g}} & H^{2}(G_{O}(K\overline{k}), \mu_{n}), \tag{2.24}
\end{array}$$

where the lower map $t_{g}$ is the composition of $t_{g}$ in (2.23) and the canonical isomorphism $H^{2}(G'_{\mathfrak{o}}(K), \mu_{n}) \cong H^{2}(G_{O}(K\overline{k}), \mu_{n}).$

Let $1_{\mathfrak{p}}$ denote the element 1 in the component $\mathbb{Z}$ for $\mathfrak{p}$. Then $f_{\mathfrak{p}}(1_{\mathfrak{p}}) \in H^{1}(\mathcal{T}_{\mathfrak{p}}, \mu_{n}) \subset H^{1}(N, \mu_{n})^{G'_{\mathfrak{o}}(K)} = \text{Hom}_{G'_{\mathfrak{o}}(K)}(N, \mu_{n})$ is a surjection from $N \to \mu_{n}$ whose kernel is closed under the conjugation in $G'_{\mathfrak{o}}(K)$. Let $L$ denote the field fixed by $\ker f_{\mathfrak{p}}(1_{\mathfrak{p}})$. By the Kummer theory, there exists $b \in K'_{\mathfrak{o}}$ such that $L = K'_{\mathfrak{o}}(\sqrt[n]{b})$ and $\text{ord}_{\mathfrak{p}}(b) = 1$ for any $\mathfrak{Q} \in S(K'_{\mathfrak{o}})$ above $\mathfrak{p}$. Then the isomorphism
Gal(L/K'_O) \simeq \mu_n induced by f_p(1_p) is defined by \( g \mapsto \frac{g(\sqrt[p]{b})}{\sqrt[p]{b}} \) for \( g \in \text{Gal}(L/K'_O) \). So we have a central group extension

\[
1 \longrightarrow \mu_n \longrightarrow \text{Gal}(L/K \kappa) \longrightarrow G'_O(K) \longrightarrow 1.
\]

and we pick a splitting \( t : G'_O(K) \rightarrow \text{Gal}(L/K \kappa) \). Then \( tg \circ f_p(1_p) \) is the class corresponding to this central extension, and explicitly, the class containing the 2-cocycle

\[
z : G'_O(K) \times G'_O(K) \longrightarrow \mu_n
\]

\[
(\sigma, \tau) \mapsto \frac{t(\sigma \tau)^{-1} t(\sigma)t(\sqrt[p]{b})^n}{\sqrt[p]{b}}.
\]

On the other hand, let’s compute \( \delta_2 \circ \delta_1(1_p) \). The image of \( b \) under the quotient map in (2.22) is invariant under the \( G_O(K \kappa) \) action. Then, because we assume \( \text{ord}_p(b) = 1 \), the image of \( b \) is \( 1_p \) in \( \oplus_{p \in S} \mathbb{Z} \). Then by chasing the diagram for the connecting homomorphism \( \delta_1, \delta_1(1_p) \) is the class containing the 1-cocycle

\[
x : G_O(K \kappa) \longrightarrow O_{K'_O}^\times
\]

\[
\sigma \mapsto \frac{\sigma(b)}{b}.
\]

We choose a splitting \( s : O_{K'_O}^\times \rightarrow O_{K'_O}^\times \) of the Kummer sequence such that \( s \left( \frac{\sigma(b)}{b} \right) = \frac{t(\sigma)(\sqrt[p]{b})}{\sqrt[p]{b}} \) for any \( \sigma \in G_O(K \kappa) \). There exists such a splitting because \( \left( \frac{t(\sigma)(\sqrt[p]{b})}{\sqrt[p]{b}} \right)^n = \frac{\sigma(b)}{b} \). Then by chasing the diagram for \( \delta_2 \), we see that \( \delta_2 \circ \delta_1(1_p) \) is the class of the 2-cocycle

\[
y : G_O(K \kappa) \times G_O(K \kappa) \longrightarrow \mu_n
\]

\[
(\sigma, \tau) \mapsto \sigma(s(x(\tau)))s(x(\sigma))s(x(\tau \sigma))^{-1} = \frac{t(\sigma)t(\tau)(\sqrt[p]{b})}{t(\tau)(\sqrt[p]{b})}.
\]

The two 2-cocycles \( z \) and \( y \) are the same because \( y(\sigma, \tau) = t(\sigma \tau)(z(\sigma, \tau)) = z(\sigma, \tau) \) as \( z(\sigma, \tau) \subset \mu_n \) is fixed by \( t(\sigma, \tau) \). Therefore, we proved that (2.24) commutes, which implies that \( tg \circ f_p(1_p) \) corresponds to the element of \( H^2_{\text{et}}(X_{/\kappa}, \mu_n) \) of tr, trace 1.

Recall that \( \Omega_K \) denotes the prime-to-\( p \) completion of the étale fundamental group \( \pi^\text{et}_1(F^1_{/\kappa} - \{P_1, \ldots, P_m\}) \) where \( P_1, \ldots, P_m \) correspond to the primes ramified in \( K \kappa/K(t) \). So the prime-to-\( p \) completion of \( \ker(\Omega_K \rightarrow \text{Gal}(K \kappa/K(t))) \) is a quotient of \( G'_S(K) \). Let \( g_K \) denote the surjection defined in Lemma 2.9, and let \( \alpha : G'_S(K) \rightarrow \bar{H} \) that factors through the map obtained by restricting \( g_K \) to \( \ker(\Omega_K \rightarrow \text{Gal}(K \kappa/K(t))) \) and then taking the prime-to-\( p \) completion, we obtain the following commutative diagram

\[
1 \longrightarrow N \longrightarrow G'_S(K) \longrightarrow G'_O(K) \longrightarrow 1
\]

\[
1 \longrightarrow \ker \varpi \longrightarrow \bar{H} \longrightarrow G'_O(K) \longrightarrow 1,
\]

\[18\]
which induces a commutative diagram of the Hochschild–Serre exact sequences

\[
\begin{array}{ccc}
\vdots & \rightarrow & H^1(N, \mu_n)^G'_\mathcal{O}(K) \\
\uparrow \alpha & & \uparrow \iota_g \\
\rightarrow & & \rightarrow \\
\vdots & \rightarrow & H^2(G'_\mathcal{O}(K), \mu_n) \\
\end{array}
\]

\[\text{induced by } \alpha\]  \hspace{1cm} (2.25)

Here the isomorphism in the second row follows from Lemma 2.10.

We use the notation in Lemma 2.9 to let \( \overline{g}_i \) denote the image of \( g_i \) in \( \Omega_K \) for each \( i = 1, \ldots, m \). By Lemma 2.9, \( g_K \) identifies \( \ker \varpi \) as the Galois group of an extension of \( K'_\mathcal{O} \), denoted by \( E/K'_\mathcal{O} \), that is ramified only at the primes over the prime \( v \) of \( \overline{K}(t) \) corresponding to \( P_m \). Let \( p_1, \ldots, p_c \) denote all the primes of \( K \overline{K} \) lying above \( v \), and let \( e \) denote the ramification index of the extension \( p_i/v \). Let \( h \) denote \( g_K(\overline{g}_m) \) in \( H \). Then \( h \) generates the inertia subgroup of \( E/K'_\mathcal{O} \) at one prime above \( v \), and because \( h \in \ker \varpi = \ker \pi \) is in the center of \( \tilde{G} \) (where \( \pi \) and \( \tilde{G} \) are defined in Lemma 2.4), we have that \( h \) generates the inertia subgroup at each prime above \( v \).

Let \( I(\overline{g}_i) \) denote the image of \( I(\overline{g}) \) under the surjection \( \tilde{\mathbb{Z}}(1)_{(p)} \rightarrow \mu_n \). For an element \( \zeta \in \mu_n \), a pro-cyclic group \( D \), and one generator \( d \) of \( D \), we write \([d \mapsto \zeta] \) for the element of \( \text{Hom}(D, \mu_n) \) that sends \( d \) to \( \zeta \). Then \( i_n \) is the element \([\tilde{\rho}_K(g_1 \cdots g_m) \mapsto I(\overline{g}_n)] \) in \( H^1(\ker \varpi, \mu_n) \). Because \( \tilde{\rho}_K(g_1 \cdots g_m) \) is in the center of \( \tilde{G} \), it follows by Lemma 2.9 and \( \text{ord}(\tilde{\rho}_K(g_m)) = e \) that

\[
\tilde{\rho}_K(\overline{g}_m) = (\tilde{\rho}_K(g_m) \tilde{\rho}_K(g_1 \cdots g_m)^{-1})^e = \tilde{\rho}_K(g_1 \cdots g_m)^{-e},
\]

and hence the image of \( i_n \) in the \( p_i \)-component of \( H^1(N, \mu_n)^G'_\mathcal{O}(K) = \oplus_p H^1(T_p, \mu_n) \) is \([\overline{g}_m \mapsto I(\overline{g}_n)^{-e}] \).

Recall that \( I(\overline{g}_n) \) is defined to be \([\overline{g}_m \mapsto (\sqrt[a_v]{a_v} \overline{\varpi})^{-1}] \) for any uniformizer \( a_v \) of the ring of integers of \( \overline{K}(t)_v \). So

\[
[\overline{g}_m \mapsto I(\overline{g}_n)^{-e}] = [\overline{g}_m \mapsto (\sqrt[a_v]{a_v} \overline{\varpi})^{-1}] = [\overline{g}_m \mapsto (\sqrt[a_v]{a_v} \overline{\varpi})^{-e}].
\]

Here we choose \( a_v \) and \( a_p \) to be compatible uniformizers such that \( a_v = a_p^e \), and then the last equality is because \( (K \overline{K})_p/\overline{K}(t)_v \) is a degree-\( e \) completely ramified extension. So we see that the image of \( i_n \) under the composition map \( H^1(\ker \varpi, \mu_n) \rightarrow H^1(T_p, \mu_n) \rightarrow H^2(G'_\mathcal{O}(K), \mu_n) \) has trace \(-e\). By summing over all \( p \) and considering the diagram (2.25), we see that the image of \( i_n \) in \( H^2(G'_\mathcal{O}(K), \mu_n) \) has trace \(-ec = -[K \overline{K} : \overline{K}(t)] = -|\Gamma|\).

\[\square\]

**Corollary 2.12.** The map \( \varphi \) in (2.21) identifies (2.18) as a central extension of \( G'_\mathcal{O}(K) \) with kernel \( \tilde{\mathbb{Z}}(1)_{(p)} \). Then the class of \( H^2(G'_\mathcal{O}(K), \tilde{\mathbb{Z}}(1)_{(p)} \rightarrow \text{Gal}(K'_\mathcal{O}/\overline{K}(t)) \). In particular, this class corresponds to the class of \( H^2_{\mathcal{O}}(X_{\mathcal{O}}, \tilde{\mathbb{Z}}(1)_{(p)} \). Proof. Let \( \varphi \) denote a splitting of \( \varpi \) such that \( \varphi(1) = 1 \). Consider the following 2-cocycle in \( Z^2(G'_\mathcal{O}(K), \ker \pi) \)

\[
\lambda : G'_\mathcal{O}(K) \times G'_\mathcal{O}(K) \rightarrow \ker \varpi
\]

defined by \( \lambda(x, y) = \varphi(xy)^{-1} \varphi(x) \varphi(y) \), which is the normalized 2-cocycle corresponding to the extension \( \varpi \). Then the transgression map \( t\varphi \) maps \( i \) to the class of \( i \circ \lambda \) [Kar93, Pages 16-17]. Since the class of \( i \circ \lambda \) is the normalized 2-cocycle corresponding to the central extension of \( G'_\mathcal{O}(K) \) with kernel \( \tilde{\mathbb{Z}}(1)_{(p)} \) described in the corollary, we proved the statement (1). The statement (2) is trivial, and the last statement follows by the statement (1) and Lemma 2.11. \[\square\]
2.3. Definition of the invariant $\omega_{L/K}$.

**Definition 2.13** (Invariant $\omega_{L/K}$ associated to $L/K$). For a subextension $L$ of $K'/K$ such that $L$ is Galois over $k(t)$, we define the $\omega$-invariant $\omega_{L/K}$ associated to $L/K$ to be the Frob-$k$-equivariant homomorphism $\omega_{L/K}$ that is the composition map as follows

$$\omega_{L/K} : \hat{\mathbb{Z}}(1)_{(p \mid \Gamma)'} \xrightarrow{\omega_K} H_2(\text{Gal}(K'_O/K(t)), \mathbb{Z})_{(p \mid \Gamma)'} \xrightarrow{\text{coinf}} H_2(\text{Gal}(L\overline{k}/\overline{k}(t)), \mathbb{Z})_{(p \mid \Gamma)'}$$

where the map coinf is the coinflation map defined by the surjection $\alpha : \text{Gal}(K'_O/K(t)) \to \text{Gal}(L\overline{k}/\overline{k}(t))$. In particular, when $L = K^+_O$, we denote $\omega_K^+ := \omega_{K^+_O/K}$.

**Lemma 2.14.** Let $n$ be an integer that is divisible by $|\Gamma|$, and $G, H$ are two extensions of $\Gamma$ such that $\ker (G \to \Gamma)$ and $\ker (H \to \Gamma)$ are pro-prime-to-$n$ admissible $\Gamma$-groups. Assume that there is a surjection $\alpha : G \to H$ and a $(n')$-Schur covering of $H$

$$1 \longrightarrow \ker \pi' \longrightarrow S \xrightarrow{\pi'} H \longrightarrow 1. \quad (2.26)$$

Then there exists a $(n')$-Schur covering of $G$ such that the following diagram commutes

$$
\begin{array}{cccccc}
1 & \longrightarrow & \ker \pi & \longrightarrow & T & \xrightarrow{\pi} & G & \longrightarrow & 1 \\
& \downarrow & & \downarrow & & \downarrow & & \alpha \\
1 & \longrightarrow & \ker \pi' & \longrightarrow & S & \xrightarrow{\pi'} & H & \longrightarrow & 1,
\end{array}
$$

and the first vertical arrow is the composition map

$$\ker \pi \xrightarrow{d_{\pi}^{-1}} H_2(G, \mathbb{Z})_{(n)'} \xrightarrow{\text{coinf}} H_2(H, \mathbb{Z})_{(n)'},$$

where $d_{\pi}$ and $d_{\pi'}$ is the differential maps defined by $\pi$ and $\pi'$ respectively.

**Proof.** There is a commutative diagram induced by $\alpha : G \to H$

$$
\begin{array}{cccc}
H^2(H, \ker \pi') & \longrightarrow & \text{Hom}(H_2(H, \mathbb{Z}), \ker \pi') & \\
\downarrow & & \downarrow & \\
H^2(G, \ker \pi') & \longrightarrow & \text{Hom}(H_2(G, \mathbb{Z}), \ker \pi'),
\end{array}
$$

where the vertical maps are induced by $\alpha$, and the horizontal maps are from the universal coefficient theorem. Moreover, since $\ker (G \to \Gamma)$ and $\ker (H \to \Gamma)$ are admissible $\Gamma$-groups, we have that $G^{ab}$ and $H^{ab}$ are both isomorphic to $\Gamma^{ab}$, so $\text{Ext}_{\mathbb{Z}}^1(G, \ker \pi') = \text{Ext}_{\mathbb{Z}}^1(H, \ker \pi') = 0$ and the two horizontal maps are isomorphisms.

The image of the class of $\pi'$ in the upper-right entry of the above diagram is the differential map $d_{\pi'}$ (we view $d_{\pi'}$ as the quotient map $H_2(H, \mathbb{Z}) \to \ker \pi'$ that factors through $H_2(H, \mathbb{Z})_{(n)'} \xrightarrow{\sim} \ker \pi'$). We let $d$ denote the image of $d_{\pi'}$ in the lower-right entry, so $d$ is the composition $H_2(G, \mathbb{Z})_{(n)'} \to H_2(H, \mathbb{Z})_{(n)'} \xrightarrow{d_{\pi}} \ker \pi'$. Let $\pi : E \to G$ be a group extension of $G$ whose corresponding class in $H^2(G, \ker \pi')$ is the preimage of $d$. Then $E$ has a subgroup $E'$ such that $E' \to G$ is a stem extension of kernel isomorphic to $\text{im} \ d$. Because every stem extension is a homomorphic image of a Schur covering group [Kar93, Chap.11, Cor.2.4], $E' \to G$ can be extended to a $(n')$-Schur covering $\pi : T \to G$. Then one can check by our construction that $\pi$ fits into the diagram in the lemma. \qed

The following is an analogue of Proposition 2.6, which gives a group theoretical description of the invariant $\omega_{L/K}$.
Corollary 2.15. Use the assumptions and notation in Definition 2.13. Let $g = (g_1, \ldots, g_m)$ be a system of inertia generators for $K$, $\varphi : \langle g_1, \ldots, g_m \rangle \to \text{Gal}(L\overline{k}/\overline{k}(t))$ the surjection defined by $g$ and $L$, and

$$1 \to B \to S \xrightarrow{\pi'} \text{Gal}(L\overline{k}/\overline{k}(t)) \to 1$$

be a $(p|\Gamma)'$-Schur covering of $\text{Gal}(L\overline{k}/\overline{k}(t))$. Then there is a unique surjection $\widetilde{\varphi} : \langle g_1, \ldots, g_m \rangle \to S$ such that $\varphi = \pi' \circ \widetilde{\varphi}$ and $\text{ord}(\tilde{\varphi}(g_i)) = \text{ord}(\varphi(g_i))$ for each $i = 1, \ldots, m$.

The invariant $\omega_{L/K}$ is the composition of the map $\mathbb{Z}(1)_{(p|\Gamma)'} \to B$ defined by $I(g) \mapsto \tilde{\varphi}(g_1 \cdots g_m)$ and the inverse of the differential map $H_2(\text{Gal}(L\overline{k}/\overline{k}(t)), \mathbb{Z})_{(p|\Gamma)'} \xrightarrow{\sim} B$ defined by $\pi'$.

Proof. The existence and uniqueness of $\tilde{\varphi}$ can be proven by repeating the proof of Proposition 2.6(1).

Note that $G^\prime_\mathcal{O}(K)$ is an admissible $\Gamma$-group, so is $\text{Gal}(L\overline{k}/K\overline{k})$. By applying Lemma 2.14 to $\alpha : \text{Gal}(K^\prime_{\mathcal{O}/\overline{k}(t)}) \to \text{Gal}(L\overline{k}/\overline{k}(t))$, we obtain $\pi : \widetilde{G} \to \text{Gal}(K^\prime_{\mathcal{O}/\overline{k}(t)})$ in the diagram in Lemma 2.14. Then by Proposition 2.6, for a choice of $g$, we have the following commutative diagram

$$\begin{array}{ccc}
\widetilde{G} & \xrightarrow{\pi} & \text{Gal}(K^\prime_{\mathcal{O}/\overline{k}(t)}) \\
\downarrow \rho_K & & \downarrow \alpha \\
S & \xrightarrow{\pi'} & \text{Gal}(L\overline{k}/\overline{k}(t)).
\end{array}$$

Then the corollary follows by the definitions of $\omega_K$ and $\omega_{L/K}$, Proposition 2.6(3), and Lemma 2.14.

Remark 2.16. (1) The invariant $\omega_{L/K}$ is not necessarily an isomorphism, because the coinflation map is not.

(2) Assume that $L$ is contained in $K^\#_{\mathcal{O}}$. Then $\text{Frob}_k$ acts trivially on $\text{Gal}(L\overline{k}/\overline{k}(t))$, and $\text{Gal}(L\overline{k}/\overline{k}(t))$ is naturally isomorphic to $\text{Gal}(L/k(t))$. In this case, the invariant $\omega_{L/K}$ factors through the prime-to-$p|\Gamma|$ part of the roots of unity of $k$, which we denote by $\mu(k)_{(p|\Gamma)'}$.

So by abuse of notation, we write

$$\omega_{L/K} : \mu(k)_{(p|\Gamma)'} \to H_2(\text{Gal}(L/k(t)), \mathbb{Z})_{(p|\Gamma)'}.$$

The image of $\omega_{L/K}$ is contained in the $|\mu(k)_{(p|\Gamma)}|$-torsion subgroup of $H_2(\text{Gal}(L/k(t)), \mathbb{Z})_{(p|\Gamma)'}$.

(3) Every argument in this section works when replacing “pro-prime-to-$p|\Gamma|$ completion” with “pro-$\ell$ completion”, for any prime $\ell$ that does not divide $p|\Gamma|$. So we can define the pro-$\ell$ analogues of the invariants $\omega_K$ and $\omega_{L/K}$. Explicitly, under the assumptions in Definitions 2.8 and 2.13, we can define $\text{Frob}_k$-equivariant

$$\omega_{K,\ell} : \mathbb{Z}_{\ell}(1) \xrightarrow{\sim} H_2(\text{Gal}(K^\prime_{\mathcal{O}/\overline{k}(t)}), \mathbb{Z})(\ell)$$

and

$$\omega_{L/K,\ell} : \mathbb{Z}_{\ell}(1) \to H_2(\text{Gal}(L\overline{k}/\overline{k}(t)), \mathbb{Z})(\ell),$$

and give group theoretical descriptions of these invariants.

3. Relationship between $\omega_K$ and the Weil pairing associated to $K$

Throughout this section, we assume that $k$, $K$, $p$ and $\Gamma$ be as in Notation 2.1, and $\ell$ is a prime such that $\ell \nmid p|\Gamma|$. In this section, we will discuss how the invariant $\omega_K$ is abelianized to the Weil pairing associated to $K$. In §3.1, we will first explain how a pro-$\ell$ presentation of $G^\prime_\mathcal{O}(K\overline{k})(\ell)$
determines its cup product. Then in §3.2, we will show how \( \omega_K \) determines the Weil pairing and how \( \omega_{L/K} \) determines the image of Weil pairing associated to \( L/K \).

3.1. Presentation of \( G_\Omega(K\overline{K})(\ell) \) determines cup product. Because \( \Gamma \) is assumed to be non-trivial (see Notation 2.1), by [NSW08, Thm.10.1.2(i)(b) and (iii)], \( G_\Omega(K\overline{K})(\ell) \) is a pro-\( \ell \) Demuškin group generated by \( 2g \) generators whose abelianization is isomorphic to \( \mathbb{Z}_{2g} \), and by a nice choice of the generating set, it admits a pro-\( \ell \) presentation in the form of

\[
G_\Omega(K\overline{K})(\ell) \simeq \langle x_1, \ldots, x_{2g} \mid [x_1, x_2][x_3, x_4] \cdots [x_{2g-1}, x_{2g}] = 1 \rangle.
\]

Let \( F \) be a free pro-\( \ell \) group on \( 2g \) generators \( x_1, \ldots, x_{2g} \) and the following a pro-\( \ell \) presentation of \( G_\Omega(K\overline{K})(\ell) \) (which is called a minimal presentation of \( G_\Omega(K\overline{K})(\ell) \) because the minimal number of generators for \( F \) and \( G_\Omega(K\overline{K})(\ell) \) are equal)

\[
1 \to R \to F \xrightarrow{\phi} G_\Omega(K\overline{K})(\ell) \to 1.
\]  

Since \( F \) is free and \( F^{ab} \simeq G_\Omega(K\overline{K})(\ell)^{ab} \simeq \mathbb{Z}_{2g}^{\ell} \), the transgression map in the Hochschild–Serre exact sequence of (3.1) is isomorphic, and we denote it by

\[
tg : H^1(R, \mathbb{Z}_\ell) \xrightarrow{G_\Omega(K\overline{K})(\ell)} H^2(G_\Omega(K\overline{K})(\ell), \mathbb{Z}_\ell).
\]

Then for every element \( \lambda \) of \( R \), there is a trace map \( \text{tr}_\lambda \) associated to \( \lambda \) as follows

\[
\text{tr}_\lambda : H^2(G_\Omega(K\overline{K})(\ell), \mathbb{Z}_\ell) \to \mathbb{Z}_\ell
\]

\[
\varphi \mapsto (tg^{-1}\varphi(\lambda)).
\]

By definition of Demuškin groups and [NSW08, Prop.(3.9.12)(ii)(iii)], if \( \lambda \) generates \( R \) as a normal subgroup of \( F \), then \( \text{tr}_\lambda \) is an isomorphism.

For a group \( G \), let \( \{G^{(i)}\}_{i=1}^\infty \) denote the lower central series of \( G \), i.e., \( G^{(1)} := G \) and \( G^{(i+1)} := [G^{(i)}, G] \). We assume that \( x_1, \ldots, x_{2g} \) are generators of \( F \) and \( \lambda \) is an element generating \( R \) as a normal subgroup. Then by [NSW08, Prop.(3.9.13)(i)], \( \lambda \) can be written in the following form

\[
\lambda = \prod_{1 \leq i < j \leq 2g} [x_i, x_j]^{a_{ij}} \cdot \lambda', \quad \lambda' \in F^{(3)}, \ a_{ij} \in \mathbb{Z}_\ell. \tag{3.3}
\]

We let \( \chi_1, \ldots, \chi_{2g} \) be the corresponding \( \mathbb{Z}_\ell \)-basis of \( H^1(F, \mathbb{Z}_\ell) = H^1(G_\Omega(K\overline{K})(\ell), \mathbb{Z}_\ell) \) such that \( \chi_i(x_j) = 1 \) if \( i = j \) and 0 otherwise. Then, by [NSW08, Prop.(3.9.13)(ii)], the cup product of \( H^1(G_\Omega(K\overline{K})(\ell), \mathbb{Z}_\ell) \) with itself is completely determined by the \( a_{ij} \) in (3.3): the bilinear form

\[
H^1(G_\Omega(K\overline{K})(\ell), \mathbb{Z}_\ell) \times H^1(G_\Omega(K\overline{K})(\ell), \mathbb{Z}_\ell) \xrightarrow{\cup} H^2(G_\Omega(K\overline{K})(\ell), \mathbb{Z}_\ell) \xrightarrow{\text{tr}_\lambda} \mathbb{Z}_\ell \tag{3.4}
\]

is given by the matrix \( M_\lambda = [m_{ij}] \) with respect to the basis \( \chi_1, \ldots, \chi_{2g} \), where

\[
m_{ij} = \text{tr}_\lambda(\chi_i \cup \chi_j) = \begin{cases} -a_{ij} & \text{if } i < j \\ a_{ji} & \text{if } i > j \\ 0 & \text{if } i = j. \end{cases} \tag{3.5}
\]

Since \( G_\Omega(K\overline{K})(\ell) \) is the pro-\( \ell \) completion of \( G_\Omega(K\overline{K}) \), it’s clear that \( H^1(G_\Omega(K\overline{K})(\ell), \mathbb{Z}_\ell) = H^1(G_\Omega(K\overline{K}), \mathbb{Z}_\ell) \), and we’ve shown in the proof of Lemma 2.2 that the inflation map

\[
H^2(G_\Omega(K\overline{K})(\ell), \mathbb{Z}_\ell) \to H^2(G_\Omega(K\overline{K}), \mathbb{Z}_\ell)
\]

is an isomorphism. So (3.4) implies that the bilinear form

\[
H^1(G_\Omega(K\overline{K}), \mathbb{Z}_\ell) \times H^1(G_\Omega(K\overline{K}), \mathbb{Z}_\ell) \xrightarrow{\cup} H^2(G_\Omega(K\overline{K}), \mathbb{Z}_\ell) \xrightarrow{\text{tr}_\lambda} \mathbb{Z}_\ell \tag{3.6}
\]

is given by the matrix \( M_\lambda \) in (3.5).
We consider a $\ell$-Schur covering of $\text{Gal}(K^*_\mathcal{O}(\ell)/\mathcal{K}(t))$ (a pro-$\ell$ analogue of (2.8))

$$1 \longrightarrow \ker \pi_\ell \longrightarrow \widetilde{G}_\ell \xrightarrow{\pi_\ell} \text{Gal}(K^*_\mathcal{O}(\ell)/\mathcal{K}(t)) \longrightarrow 1,$$

where $\ker \pi_\ell \simeq \mathbb{Z}_\ell$. Restricting $\pi_\ell$ to an extension of $G_\mathcal{O}(K\mathcal{K})(\ell)$, we denote $\widetilde{H}_\ell := \pi_\ell^{-1}(G_\mathcal{O}(K\mathcal{K})(\ell))$ and $\varpi_\ell := \pi_\ell|_{\widetilde{H}_\ell}$, and obtain the following stem extension of $G_\mathcal{O}(K\mathcal{K})(\ell)$

$$1 \longrightarrow \ker \varpi_\ell \longrightarrow \widetilde{H}_\ell \xrightarrow{\varpi_\ell} G_\mathcal{O}(K\mathcal{K})(\ell) \longrightarrow 1. \tag{3.8}$$

**Lemma 3.1.** Let $1 \to R \to F \xrightarrow{\phi} G_\mathcal{O}(K\mathcal{K})(\ell) \to 1$ be a minimal pro-$\ell$ presentation of $G_\mathcal{O}(K\mathcal{K})(\ell)$. Then there is a surjection $\tilde{\phi} : F \to \widetilde{H}_\ell$ such that $\phi = \varpi_\ell \circ \tilde{\phi}$.

1. If $\lambda \in R$ generates $R$ as a normal subgroup of $F$, then $\tilde{\phi}(\lambda)$ is a generator of $\ker \varpi_\ell$. For two elements $\lambda_1, \lambda_2 \in R$ such that each of them generates $R$ as a normal subgroup, the followings are equivalent
   (a) $\tilde{\phi}(\lambda_1) = \tilde{\phi}(\lambda_2)$
   (b) $\lambda_1 \equiv \lambda_2 \mod F(3)$.
2. The transgression map in the Hochschild–Serre exact sequence of (3.8)

$$tg_{\varpi_\ell} : H^1(\ker \varpi_\ell, \mathbb{Z}_\ell) \longrightarrow H^2(G_\mathcal{O}(K\mathcal{K})(\ell), \mathbb{Z}_\ell)$$

is an isomorphism. Moreover, for any class $\varphi \in H^2(G_\mathcal{O}(K\mathcal{K})(\ell), \mathbb{Z}_\ell)$ and any $\lambda \in R$ that generates $R$ as a normal subgroup, we have $\text{tr}_\lambda(\varphi) = (tg_{\varpi_\ell}^{-1}\varphi)(\tilde{\phi}(\lambda))$.

**Remark 3.2.** The surjection $\tilde{\phi}$ is not unique, but the last equality in the statement (2) holds for any choice of $\tilde{\phi}$. Indeed, any two surjections $\tilde{\phi}_1$ and $\tilde{\phi}_2$ as described in (1) differ by a character $\chi : F \to \ker \varpi_\ell$ whose kernel contains $\lambda$ (since $\lambda \in [F, F]$), and hence $\tilde{\phi}_1(\lambda) = \tilde{\phi}_2(\lambda)$.

**Proof.** First, similarly to Lemma 2.10, the group extension $\varpi_\ell$ is a stem extension of $G_\mathcal{O}(K\mathcal{K})(\ell)$. Since $F^{ab} \simeq G_\mathcal{O}(K\mathcal{K})(\ell)^{ab}$, the following short exact sequence

$$1 \longrightarrow R/[F, R] \longrightarrow F/[F, R] \longrightarrow G_\mathcal{O}(K\mathcal{K})(\ell) \longrightarrow 1 \tag{3.9}$$

is a Schur covering group of $H$ ([Kar93, Chap. 11, Thm. 2.3(iii) and (iv)(b)]). Moreover, since $H^2(G_\mathcal{O}(K\mathcal{K})(\ell), \mathbb{Z}) \simeq H^2(G_\mathcal{O}(K\mathcal{K})(\ell), \mathbb{Z})$, the kernel of the Schur covering $R/[F, R]$ is isomorphic to $\mathbb{Z}_\ell$. Because $\text{Ext}^2_{G_\mathcal{O}(K\mathcal{K})(\ell)}(\mathbb{Z}^{ab}, \mathbb{Z}) = \text{Ext}^2_{G_\mathcal{O}(K\mathcal{K})(\ell)}(\mathbb{Z}_\ell^{ab}, \mathbb{Z}) = 0$, $G_\mathcal{O}(K\mathcal{K})(\ell)$ has a unique isomorphism class of Schur covering. So $\varpi_\ell$ and (3.9) are isomorphic as extensions of $G_\mathcal{O}(K\mathcal{K})(\ell)$, i.e., there is an isomorphism $\iota$ such that

$$\begin{array}{c}
\begin{array}{ccc}
\widetilde{H}_\ell & \xrightarrow{\varpi_\ell} & G_\mathcal{O}(K\mathcal{K})(\ell) \\
\downarrow \sim & & \\
F/[F, R] & \longrightarrow & G_\mathcal{O}(K\mathcal{K})(\ell)
\end{array}
\end{array} \tag{3.10}$$

commutes. Then we define $\tilde{\phi}$ to be the composition of $F \to F/[F, R]$ and $\iota$, and it follows immediately that $\phi = \varpi_\ell \circ \tilde{\phi}$. If $\lambda \in F$ generates $R$ as a normal subgroup, then $\tilde{\phi}(\lambda)$ generates $\widetilde{H}_\ell$ as a normal subgroup of $\widetilde{H}_\ell$, so it is a generator of $\ker \varpi_\ell$, which finishes the proof of the first sentence in (1) of the lemma.

Because $R$ is contained in $F^{(2)} = [F, F]$, we have $F^{(3)} \supset [F, R] = \ker \tilde{\phi}$, so (1a) implies (1b). Taking the quotient of a group $G$ modulo $G^{(i)}$ is a functor mapping surjections to surjections. For a quotient map $\pi : E_1 \to E_2$, we denote the induced quotient map by $\pi^{(i)} : E_1/E_1^{(i)} \to E_2/E_2^{(i)}$. So
we have a commutative diagram of surjections induced by $\phi$, $\tilde{\phi}$ and $\varpi_{\ell}$

\[
\begin{array}{ccc}
\tilde{H}/\tilde{H} & \xrightarrow{\varpi_{\ell}(3)} & G_{\mathcal{O}(K\overline{k})(\ell)}/G_{\mathcal{O}(K\overline{k})(\ell)(3)} \\
\end{array}
\]

The exact sequence

\[1 \rightarrow F^{(2)}/F^{(3)} \rightarrow F/F^{(3)} \rightarrow F/F^{(2)} \rightarrow 1\]

is stem, where $F/F^{(2)} \simeq \mathbb{Z}_\ell^{2g}$ and $F^{(2)}/F^{(3)} \simeq \mathbb{Z}_\ell^{2g^2-2g}$ (because $F^{(2)}/F^{(3)}$ is generated by images of $[x_i, x_j]$ for $i \neq j$). Because the cup product (3.4) for the Demuškin group $G_{\mathcal{O}(K\overline{k})(\ell)}$ is non-degenerate, it follows by (3.3) that the image of $R$ in $F/F^{(3)}$ is isomorphic to $\mathbb{Z}_\ell$ which is contained in $F^{(2)}/F^{(3)}$. Recall that $\tilde{\phi}$ factors through the isomorphism $\iota : F/[F, R] \rightarrow \tilde{H}/H$, the $(F/[F, R])/(F/[F, R])^{(3)}$ is isomorphic to $\tilde{H}/\tilde{H}^{(3)}$, where the former is isomorphic to $F/F^{(3)}$ because $[F, R] \subset F^{(3)}$. So we conclude that $\tilde{\phi}^{(3)}$ is isomorphic, and hence the image of $R$ in $\tilde{H}/\tilde{H}^{(3)}$ is isomorphic to $\mathbb{Z}_\ell$. Then because the image of $R$ in $\tilde{H}$ is isomorphic to $\mathbb{Z}_\ell$, we see that $\tilde{\phi}(R) \cap \tilde{H}^{(3)} = 1$, so (1b) implies (1a), and we finish the proof of (1).

Because (3.8) is a stem extension, in the Hochschild–Serre exact sequence

\[0 \rightarrow H^1(G_{\mathcal{O}(K\overline{k})(\ell)}, \mathbb{Z}_\ell) \rightarrow H^1(\tilde{H}, \mathbb{Z}_\ell) \rightarrow H^1(ker \varpi_{\ell}, \mathbb{Z}_\ell) \xrightarrow{tg_{\varpi_{\ell}}} H^2(G_{\mathcal{O}(K\overline{k})(\ell)}, \mathbb{Z}_\ell),\]

the second arrow is an isomorphism, so $tg_{\varpi_{\ell}}$ is an injection. On the other hand, because we’ve shown that there is a surjection $\tilde{\phi}$ such that $\phi = \varpi_{\ell} \circ \tilde{\phi}$, we have the diagram

\[
\begin{array}{ccc}
H^1(R, \mathbb{Z}_\ell)^{G_{\mathcal{O}(K\overline{k})(\ell)}} & \xrightarrow{tg} & H^1(ker \varpi_{\ell}, \mathbb{Z}_\ell) \\
& \sim & \\
& & H^2(G_{\mathcal{O}(K\overline{k})(\ell)}, \mathbb{Z}_\ell)
\end{array}
\]

where the vertical map is induced by $\tilde{\phi}|_{R}$. Moreover, the vertical map is an isomorphism, since $H^1(R, \mathbb{Z}_\ell)^{G_{\mathcal{O}(K\overline{k})(\ell)}} = \text{Hom}_F(R, \mathbb{Z}_\ell) = \text{Hom}(R/[F, R], \mathbb{Z}_\ell)$ and $\iota$ is an isomorphism. Then from the diagram, we see that $tg_{\varpi_{\ell}}$ is an isomorphism and the equality $(tg^{-1}_\varpi(\phi)\varpi)(\lambda) = (tg^{-1}_{\varpi_{\ell}}\varpi)(\tilde{\phi}(\lambda))$ holds, which proves the statement (2) in the lemma.

Lemma 3.1 shows that, after taking the quotient map $\tilde{\phi}$, the extension (3.8) carries exactly the information of the symplectic form (3.4). So we formulate this symplectic form using only the structure of (3.8) in the following corollary. Because after taking the quotient map $\tilde{\phi}$ on $F$, the corollary naturally follows by how the minimal presentation (3.1) determines the symplectic form (3.6), so by abuse of notation, we don’t distinguish the symbols used for $F$ and for $\tilde{H}$.

**Corollary 3.3.** Consider the stem extension (3.8), and let $\lambda$ be a generator of $ker \varpi_{\ell}$. Define a trace map $tr_\lambda$ as

\[tr_\lambda : H^2(G_{\mathcal{O}(K\overline{k})(\ell)}, \mathbb{Z}_\ell) \rightarrow \mathbb{Z}_\ell,\]

\[\varphi \mapsto (tg^{-1}_{\varpi_{\ell}}\varpi)(\lambda),\]
where \( t_{\omega} \) is the transgression map in Lemma 3.1(2). Assume that \( \{x_1, \ldots, x_{2g}\} \) is a minimal set of generators of \( H_\ell \). Then \( \lambda \) can be uniquely written in the form of

\[
\lambda = \prod_{1 \leq i < j \leq 2g} [x_i, x_j]^{a_{ij}} \cdot \lambda', \quad \lambda' \in \tilde{H}^{(3)}_\ell, \quad a_{ij} \in \mathbb{Z}_\ell.
\]

Note that \( \{\varpi(x_1), \ldots, \varpi(x_{2g})\} \) is a minimal set of generators of \( G_0(K \mathbb{F})(\ell) \). Let \( \chi_1, \ldots, \chi_{2g} \) be the corresponding \( \mathbb{Z}_\ell \)-basis of \( H^1(G_0(K \mathbb{F}), \mathbb{Z}_\ell) \) such that \( \chi_i(\varpi(x_j)) = 1 \) if \( i = j \) and 0 otherwise. Then the symplectic form

\[
H^1(G_0(K \mathbb{F}), \mathbb{Z}_\ell) \times H^1(G_0(K \mathbb{F}), \mathbb{Z}_\ell) \xrightarrow{\cup} H^2(G_0(K \mathbb{F}), \mathbb{Z}_\ell) \xrightarrow{\text{tr}_\lambda} \mathbb{Z}_\ell \tag{3.11}
\]

with respect to the basis \( \chi_1, \ldots, \chi_{2g} \) is given by the matrix \( M_\lambda = [m_{ij}] \), where

\[
m_{ij} = \text{tr}_\lambda(\chi_i \cup \chi_j) = \begin{cases} -a_{ij} & \text{if } i < j \\ a_{ji} & \text{if } i > j \\ 0 & \text{if } i = j. \end{cases}
\]

For a positive integer \( n \), the symplectic form above with all coefficients replaced with \( \mathbb{Z}/\ell^n \mathbb{Z} \) is given by the matrix \( M_\lambda \mod \ell^n \).

**Proof.** The corollary follows by the argument at the beginning of the section from (3.1) to (3.5) and Lemma 3.1. \( \square \)

### 3.2. The invariant \( \omega_{L/K} \)

**determines the image of Weil pairing.** Let \( X \) be the smooth projective curve over \( k \) whose function field is \( K \), and let \( X_\mathbb{F} \) denote the base change of \( X \) to \( \mathbb{F} \). Let \( \text{Jac}_X \) denote the Jacobian variety of \( X_\mathbb{F} \). Then \( \text{Jac}_X \) has an isomorphic principal polarisation, so the Weil pairing associated to \( X_\mathbb{F} \) is a bilinear pairing

\[
\text{Jac}_X[\ell^n] \times \text{Jac}_X[\ell^n] \longrightarrow \mu_{\ell^n},
\]

which is non-degenerate and alternating. By [Mil80, Chap.V, §2, Rmk.2.4(f)] and [Del77, Dualité §3], the Weil pairing can be identified with the cup product of étale cohomology followed by the trace map

\[
H^1_{\text{ét}}(X_\mathbb{F}, \mu_{\ell^n}) \times H^1_{\text{ét}}(X_\mathbb{F}, \mu_{\ell^n}) \xrightarrow{\cup} H^2_{\text{ét}}(X_\mathbb{F}, \mu_{\ell^{2n}}) \xrightarrow{\text{tr}_{X,\ell^n}} \mu_{\ell^n}. \tag{3.12}
\]

Since \( \mu_{\ell^n} \) is a trivial \( G_0(K \mathbb{F}) \)-module, we fix an isomorphism \( \mu_{\ell^n} \cong \mathbb{Z}/\ell^n \mathbb{Z} \) that is compatible among all \( n \); in other words, we pick a generator \( \zeta \) of \( \mathbb{Z}_\ell(1) \) and then identify \( \mathbb{Z}_\ell \) with \( \mathbb{Z}_\ell(1) \) by sending 1 to \( \zeta \). Then it follows by the functorial isomorphism between Galois cohomology and étale cohomology that, for a generator \( \lambda \) of \( \ker \omega_\ell \) in (3.8), the symplectic form defined by (3.12) is equivalent to the one defined by the mod-\( \ell^n \) analogue of (3.11) followed by an automorphism of \( \mathbb{Z}/\ell^n \mathbb{Z} \).

**Lemma 3.4.** Identify \( \mathbb{Z}_\ell \) with \( \mathbb{Z}_\ell(1) \) by \( 1 \mapsto \zeta \).

1. Let \( \lambda \) be a generator of \( \ker \omega_\ell \) in (3.8), and let \( M_\lambda \) and \( \text{tr}_\lambda \) be as defined in Corollary 3.3. Then the Weil pairing on the \( \ell \)-adic Tate module of \( X_\mathbb{F} \)

\[
H^1(G'_0(K \mathbb{F}), \mathbb{Z}_\ell(1)) \times H^1(G'_0(K \mathbb{F}), \mathbb{Z}_\ell(1)) \longrightarrow \mathbb{Z}_\ell(1)
\]

is equivalent to the composition of the symplectic form determined by the matrix \( M_\lambda \) and an isomorphism \( \text{tr}_X \circ \text{tr}_\lambda^{-1} \in \text{Aut}(\mathbb{Z}_\ell) \), where \( \text{tr}_X := \lim_{n \to \infty} \text{tr}_{X,\ell^n} \).

2. Let \( g := (g_1, \ldots, g_m) \) be a system of inertia generators for \( K \) such that \( I(g) \) is the generator \( \zeta^{-1} \) of \( \mathbb{Z}_\ell(1) \). Then let \( \lambda \) be the image of \( g_1 \cdots g_m \) in \( \ker \omega_\ell \) as in the pro-\( \ell \) analogue of Proposition 2.6(2). Then, \( \text{tr}_\lambda = \text{tr}_X \) as trace maps from \( H^2(G_0(K \mathbb{F}), \mathbb{Z}_\ell(1)) \to \mathbb{Z}_\ell \).
Proof. The statement (1) follows immediately by taking the inverse limit of (3.12) over all \( n \). The statement (2) says that the right block of the following diagram commutes

\[
\begin{array}{c}
H^1(\ker\varpi, \mathbb{Z}_p(1)) \\ \cap \uparrow \sim
\end{array}
\begin{array}{c}
\longrightarrow
\end{array}
\begin{array}{c}
H^2(G_0(K\overline{K})(\ell), \mathbb{Z}_p(1)) \\ \cap \uparrow \sim
\end{array}
\begin{array}{c}
\longrightarrow
\end{array}
\begin{array}{c}
\mathbb{Z}_p
\end{array}
\]

where the trace map \( \text{tr} \) in the first row is obtained by taking the \(-1\)-Tate twist of the composition map

\[
H^2(G_0(K\overline{K})(\ell), \mathbb{Z}_p(2)) \xrightarrow{\text{inf}} H^2(G_0(K\overline{K}), \mathbb{Z}_p(2)) \xrightarrow{\text{tr}} H^2_\ell(X_{\overline{K}}, \mathbb{Z}_p(2)) \xrightarrow{\text{tr}_X} \mathbb{Z}_p(1).
\]

By taking the inverse limit of the pro-\( \ell \) analogue of Lemma 2.11, the homomorphism \([\lambda \mapsto I(\overline{g})] \in H^1(\ker\varpi, \mathbb{Z}_p(1))\) (which is defined as the homomorphism \( \ker\varpi \to \mathbb{Z}_p(1) \) that sends \( \lambda \) to \( I(\overline{g}) \)) is mapped to \(-|\Gamma|\) in the upper-right entry of the above diagram. By our definition of \( \lambda \) and \( g \) in the lemma, the preimage of \([\lambda \mapsto I(\overline{g})]\) in the lower-left entry is the homomorphism \([\lambda \mapsto -|\Gamma|]\), whose image in the lower-middle entry has \( \text{tr}_X \) exactly \(-|\Gamma|\). So we finish the proof. \( \square \)

Next, we will show that the invariant \( \omega_{L/K,\ell} \) associated to \( L/K \) carries sufficient information to determine the image of Weil pairing.

**Definition 3.5** (The image of the Weil pairing). Assume that \( k \) contains \( \mu_{\ell^n} \). Let \( L/K \) be a subextension of \( K_0^\#(\ell)/K \) such that \( L \) is Galois over \( k(t) \). Then, by the isomorphism between étale cohomology and Galois cohomology, the Weil pairing defines a symplectic pairing

\[
f_{K,\ell^n} : H^1(G_0'(K), \mu_{\ell^n}) \times H^1(G_0'(K), \mu_{\ell^n}) \to \mu_{\ell^n}.
\]

Then the restriction of \( f_{K,\ell^n} \) gives a pairing

\[
f_{L/K,\ell^n} : H^1(\text{Gal}(L/K), \mu_{\ell^n}) \times H^1(\text{Gal}(L/K), \mu_{\ell^n}) \to \mu_{\ell^n},
\]

where the Frobenius \( \text{Frob}_k \) acts trivially on each term as it acts trivially on \( \text{Gal}(L/K) \). We call \( f_{L/K,\ell^n} \) the image of the Weil pairing associated to \( L/K \).

For the rest of this section, we assume that \( L \) and \( n \) are as described in Definition 3.5. Consider compatible \( \ell \)-Schur coverings of \( \text{Gal}(K_0'(\ell)/\overline{k}(t)) \) and \( \text{Gal}(L\overline{k}/\overline{k}(t)) \) (such compatible stem extensions exist by Lemma 2.14):

\[
\begin{array}{c}
1 \\
\downarrow
\end{array}
\begin{array}{c}
\ker\pi_\ell \\
\downarrow
\end{array}
\begin{array}{c}
\tilde{G}_\ell \\
\downarrow
\end{array}
\begin{array}{c}
\pi_\ell \\
\downarrow
\end{array}
\begin{array}{c}
\ker(\text{Gal}(K_0'(\ell)/\overline{k}(t)) \\
\downarrow
\end{array}
\begin{array}{c}
1
\end{array}
\]

\[
\begin{array}{c}
1 \\
\downarrow
\end{array}
\begin{array}{c}
\ker\pi'_\ell \\
\downarrow
\end{array}
\begin{array}{c}
S_\ell \\
\downarrow
\end{array}
\begin{array}{c}
\pi'_\ell \\
\downarrow
\end{array}
\begin{array}{c}
\ker(\text{Gal}(L\overline{k}/\overline{k}(t)) \\
\downarrow
\end{array}
\begin{array}{c}
1
\end{array}
\]

where the rows are \( \ell \)-Schur coverings, the last vertical map is the quotient of Galois groups, and the first vertical map is the composition of

\[
\ker\pi_\ell \xrightarrow{d_{\pi_\ell}^{-1}} H_2(\text{Gal}(K_0'(\ell)/\overline{k}(t)), \mathbb{Z})(\ell) \xrightarrow{\text{coinf}} H_2(\text{Gal}(L\overline{k}/\overline{k}(t)), \mathbb{Z})(\ell) \xrightarrow{d_{\pi'_\ell}^{-1}} \ker\pi'_\ell.
\]
By restricting $\pi_\ell$ and $\pi'_\ell$ to extensions of $G_\ell(K\bar{K})(\ell)$ and $\text{Gal}(L\bar{K}/K\bar{K}) \simeq \text{Gal}(L/K)$ respectively, we obtain the following compatible extensions

$$
\begin{array}{c}
1 \longrightarrow \ker \varpi_\ell \longrightarrow \bar{H}_\ell \xrightarrow{\varpi_\ell} G_\ell(K\bar{K})(\ell) \longrightarrow 1 \\
\downarrow \quad \downarrow \alpha \\
1 \longrightarrow \ker \varpi'_\ell \longrightarrow T \xrightarrow{\varpi'_\ell} \text{Gal}(L/K) \longrightarrow 1,
\end{array}
$$

where $\bar{H}_\ell := \pi_\ell^{-1}(G_\ell(K\bar{K})(\ell))$, $\varpi_\ell := \pi_\ell|_{\bar{H}_\ell}$, $T := \pi'_\ell^{-1}(\text{Gal}(L\bar{K}/K\bar{K}))$ and $\varpi'_\ell := \pi'_\ell|_T$. These rows are $\Gamma$-equivariant when we choose compatible splittings of $\text{Gal}(K'_{\ell}(\ell)/\bar{K}(t)) \to \text{Gal}(K\bar{K}/\bar{K}(t))$ and $\text{Gal}(L\bar{K}/\bar{K}(t)) \to \text{Gal}(L\bar{K}/\bar{K}(t))$.

**Proposition 3.6.** Use the notation above. Let $\zeta$ be a generator of $\mathbb{Z}_ell(1)$ and $\zeta_n$ the image of $\zeta$ in $\mu_{\ell^n}$. Let $\{y_1, \ldots, y_r\}$ be a set of generators of $\text{Gal}(L/K)$ such that $\text{Gal}(L/K)^{ab}$ is the direct products of the images of $\{y_i\}$ for all $i$. Then there exists a corresponding basis $\{y_1^{\nu}, \ldots, y_r^{\nu}\}$ of $H^1(\text{Gal}(L/K), \mu_{\ell^n})$ such that $y_i^{\nu}(y_j) = 0$ for $i \neq j$. Also, $\{y_1, \ldots, y_r\}$ lifts to a minimal set of generators $\{\tilde{y}_1, \ldots, \tilde{y}_r\}$ of $T$ in (3.14).

Let $\lambda_L$ denote the image of $\zeta^{-|\Gamma|}$ under the following composition map

$$
\mathbb{Z}_\ell(1) \xrightarrow{\omega_{L/K, \ell}} H_2(\text{Gal}(L\bar{K}/\bar{K}(t)), \mathbb{Z}_\ell)(\ell) \xrightarrow{d_{\ell}' L} \ker \pi'_\ell = \ker \varpi'_\ell, 
$$

where $\omega_{L/K, \ell}$ is the invariant defined in Remark 2.16(3) and $d_{\ell}'$ is the differential map defined by $\pi'_\ell$. Then $\lambda_L$ can be expressed in the form of

$$
\lambda_L = \prod_{1 \leq i < j \leq r} \left[ \tilde{y}_i, \tilde{y}_j \right]^{b_{ij}} : \chi_L', \quad \chi_L' \in T^{(3)}, \ b_{ij} \in \mathbb{Z}_\ell.
$$

With respect to the basis $y_1^{\nu}, \ldots, y_r^{\nu}$, the image of the Weil pairing $f_{L/K, \ell^n}$ is given by

$$
f_{L/K, \ell^n}(y_i^{\nu}, y_j^{\nu}) = \begin{cases} 
(y_i^{\nu}(y_i^{\nu}(y_j))^{b_{ij}} & \text{if } i < j \\
(y_i^{\nu}(y_i^{\nu}(y_j)))^{b_{ij}} & \text{if } i > j \\
0 & \text{if } i = j.
\end{cases}
$$

**Proof.** There exist elements $t_1, \ldots, t_r$ of $\text{Gal}(L/K)^{ab}$ such that $\text{Gal}(L/K)^{ab} = \langle t_1 \rangle \times \cdots \times \langle t_r \rangle$. So there exists a basis $\{y_1^{\nu}, \ldots, y_r^{\nu}\}$ of $H^1(\text{Gal}(L/K), \mu_{\ell^n}) = H^1(\text{Gal}(L/K)^{ab}, \mu_{\ell^n})$ such that $y_i^{\nu}(t_j) = 0$ for $i \neq j$. We pick $y_i \in \text{Gal}(L/K)$ to be a lift of $t_i$. By the Burnside basis theorem, $y_1, \ldots, y_r$ form a minimal set of generators of $\text{Gal}(L/K)$. Since $T$ is a stem extension of $\text{Gal}(L/K)$, we have $T^{ab} \simeq \text{Gal}(L/K)^{ab}$ and hence $\{\tilde{y}_1, \ldots, \tilde{y}_r\}$ is a minimal set of generators of $T$.

Let $\lambda$ be defined in Lemma 3.4(2). So $\lambda_L$ is $\alpha(\lambda)$, where $\alpha$ is the middle vertical arrow in (3.14). We let $M_\ell$, $\chi_\ell$, $m_{ij}$ and $a_{ij}$ be as defined in Corollary 3.3 for $1 \leq i, j \leq 2g$, then let $\chi_i[n]$ denote the composition of $\chi_i$ and $\mathbb{Z}_\ell \to \mu_{\ell^n}$ (defined by $1 \mapsto \zeta_n$). Let $D = [d_{ij}]$ be a $2g \times r$ $\mathbb{Z}_\ell$-entry matrix such that

$$
\alpha(x_i) \equiv \prod_{j=1}^r ([\tilde{y}_j])^{d_{ij}} \mod T^{(2)},
$$

and let $E = [e_{ij}]$ be a $2g \times r$ $\mathbb{Z}_\ell$-entry matrix such that

$$
y_i^{\nu} = \sum_{i=1}^{2g} e_{ij} \chi_i[n].$$
We compute $y_j^\lambda(\alpha(x_i))$ by viewing $y_j^\lambda$ as a homomorphism from $\tilde{H}_\ell$ to $\mu_\ell^n$ that factors through $\text{Gal}(L/K)$. On one hand, we have
\[
y_j^\lambda(\alpha(x_i)) = y_j^\lambda \left( \prod_{s=1}^{r} (\tilde{y}_s)^{d_{is}} \right) = y_j^\lambda (\tilde{y}_j)^{d_{ij}},
\]
and on the other hand,
\[
y_j^\lambda(\alpha(x_i)) = y_j^\lambda (x_i) = \prod_{s=1}^{2g} \chi_s[n](x_i)^{e_{sj}} = (\zeta_n)^{\epsilon_{ij}}.
\]
So we see that $E = D\Delta$, where $\Delta$ is the $r \times r$ diagonal matrix whose $(i, i)$-entry is $\log_{\zeta_n} y_i^\lambda(y_i)$. By $\lambda_L = \alpha(\lambda)$ and Corollary 3.3, we have
\[
\lambda_L = \prod_{1 \leq i < j \leq 2g} [\alpha(\alpha(x_i), \alpha(x_j))]^{a_{ij}} \cdot \lambda' \quad \text{for some } \lambda' \in T^{(3)}
\]
\[
= \prod_{1 \leq i < j \leq 2g} \left[ \prod_{s=1}^{r} (\tilde{y}_s)^{d_{is}}, \prod_{t=1}^{r} (\tilde{y}_t)^{d_{jt}} \right]^{a_{ij}} \cdot \lambda'' \quad \text{for some } \lambda'' \in T^{(3)}
\]
\[
= \prod_{1 \leq s < t \leq r} [\tilde{y}_s, \tilde{y}_t]^{-\sum_{1 \leq i, j \leq 2g} d_{is} d_{jt} e_{ij}} \cdot \lambda''
\]
So we see that $-b_{st}$ is the $(s, t)$-entry of $D^T M_\lambda D$ for $1 \leq s < t \leq r$. Then by Corollary 3.3 and Lemma 3.4(2)
\[
f_{L/K, \ell^n}(y_i^\lambda, y_j^\lambda) = f_{L/K, \ell^n} \left( \sum_{s=1}^{2g} e_{is} \chi_s[n], \sum_{t=1}^{2g} e_{jt} \chi_t[n] \right) = (\zeta_n)^{(i, j)} \text{-entry of } E^T M_\lambda E,
\]
which proves the proposition. \qed

4. The function field moments as $q \to \infty$

In this section, we study the relationship between the $\omega$-invariant $\omega_{L/K}$ and the EVW-W lifting invariant. Building on the strategy of the work [LWZ19] of Wood, Zureick-Brown and the author, we give the proof of Theorem 1.1 by counting rational points on Hurwitz schemes with prescribed $\omega$-invariant.

4.1. Revisit: Hurwitz schemes and a lifting invariant of Ellenberg–Venkatesh–Westerland and Wood. In [Woo21], Wood defined and proved basic properties of a lifting invariant of covers of $\mathbb{P}^1$ over an algebraically closed field, which was introduced by Ellenberg, Venkatesh, and Westerland. Let $G$ be a finite group and $c$ a subset of $G$ closed under conjugation by elements of $G$ and closed under invertible powering. Let $c/G$ denote the set of conjugacy classes of elements in $c$.

Let $U(G, c)$ be the group defined by presentation with generators $[g]$ for $g \in c$, and relations $[x][y][x]^{-1} = [xyz^{-1}]$ for $x, y \in c$. Then there is a natural surjection $U(G, c) \to G$ mapping $[g] \to g$ and a natural surjection $U(G, c) \to \mathbb{Z}[G]$ mapping $[g]$ to a generator for the conjugacy class of $g$. These two surjections induce the same map $U(G, c) \to G^{ab}$ to the abelianization of $G$, so we obtain a homomorphism $U(G, c) \to G \times_{G^{ab}} \mathbb{Z}[G]$. This homomorphism is actually a surjection, and [Woo21, Thm.2.5] proves that $U(G, c)$ is isomorphic to the fiber product $S_c \times_{G^{ab}} \mathbb{Z}[G]$, where $S_c$ is a reduced Schur covering for $G$ and $c$ defined as follows. A reduced Schur covering $S_c \to G$ is defined to be the quotient of a Schur covering $\phi : S \to G$ by the normal subgroup generated by the set of commutators
\[
\{ [\tilde{x}, \tilde{y}] \mid \tilde{x}, \tilde{y} \in S, \phi(\tilde{x}) \in c, \text{ and } [\phi(\tilde{x}), \phi(\tilde{y})] = 1 \}.
\]
Via the isomorphic differential map $H_2(G, \mathbb{Z}) \to \ker \phi$, the kernel of a reduced Schur covering is isomorphic to a quotient of $H_2(G, \mathbb{Z})$, which we denote by $H_2(G, c)$; and one can prove by definition that $H_2(G, c)$ does not depend on the choice of the Schur covering that we start with. Thus, the kernel of the natural quotient map $U(G, c) \to G$ is isomorphic to $H_2(G, c) \times \mathbb{Z}^{c/G}$, and we denote this kernel by $K(G, c)$.

Let $p$ be a prime not dividing $|G|$. There is an action of $\hat{\mathbb{Z}}(p)_\gamma$, on the set of elements of $K(G, c)$. Let $S_c \to G$ be a reduced Schur covering for $G$ and $c$. Then elements of $K(G, c)$ can be written in the form $(g, m)$ for $g \in \ker(S_c \to G)$ and $m \in \mathbb{Z}^{c/G}$. For each conjugacy class $\gamma \in c/G$, we pick an element $x_\gamma$ in $\gamma$ and a lift $\hat{x_\gamma}$ of $x_\gamma$ in $S_c$. Then for each $\alpha \in \hat{\mathbb{Z}}(p)_\gamma$ and $\gamma \in c/G$, we define $w_\alpha(\gamma) = \hat{x_\gamma}^{-\alpha} \hat{x_\gamma} \in \ker(S_c \to G)$, where $\hat{x_\gamma}$ is the picked lift of the element in the conjugacy class of $\gamma^\alpha$. Then we define a group homomorphism $W_\alpha : \mathbb{Z}^{c/G} \to \ker(S_c \to G)$ by sending the generators for the conjugacy class $\gamma$ to $w_\alpha(\gamma)$. It was shown in [Woo21, §4] that $W_\alpha$ does not depend on the choice of the lifts $\hat{x_\gamma}$. Then, for each $\alpha \in \hat{\mathbb{Z}}(p)_\gamma$, we define an action of $\alpha$ on the set $K(G, c)$ by

$$\alpha * (g, m) = (g^\alpha W_\alpha(m), m^\alpha),$$

where $g^\alpha$ is the $\alpha$th power of $g$ and $m^\alpha$ is a rearranging of the coordinates of $m$ by sending the coordinate of $\gamma$ to the coordinate of $\gamma^\alpha$. This action of $\alpha$ is not a group homomorphism.

Let $k$ be an algebraically closed field of characteristic $p$ such that $p \nmid |G|$ if $p \neq 0$ (here we include the case $p = 0$). A branched $G$-cover $X$ of $\mathbb{P}^1$ over $\overline{k}$ that is ramified at $\{P_1, \ldots, P_m\}$ defines a surjection

$$\varphi : \pi_1^\text{et}(\mathbb{P}^1_k - \{P_1, \ldots, P_m\})_{(p)'} \to G.$$ 

Assume that all the inertia groups of the cover are generated by elements in $c$. We let $g = (g_1, \ldots, g_m)$ be a system of inertia generators for $\pi_1^\text{et}(\mathbb{P}^1_k - \{P_1, \ldots, P_m\})_{(p)'}$ and let $I(g)$ be the corresponding generator of $\hat{\mathbb{Z}}(1)_{(p)'}$. Then $EVW$-W lifting invariant associated to this cover $X/\mathbb{P}^1_k$ is defined to be the $\hat{\mathbb{Z}}(p)_\gamma$-equivariant map of sets

$$\delta : \hat{\mathbb{Z}}(1)_{(p)'} \to K(G, c)$$

$$I(g) \mapsto [\varphi(g_1)] \cdots [\varphi(g_m)].$$

There is a Hurwitz scheme $\text{Hur}_{G,c}^n$ defined over $\mathbb{Z}[|G|^{-1}]$, whose points represent tame Galois covers $X/\mathbb{P}^1$ with $n$ branch points (i.e., the degree of each geometric fiber of $D \to \text{Spec}(\mathbb{Z}[|G|^{-1}])$ is $n$, where $D \subset \mathbb{P}^1$ is the branch loci of the cover $X/\mathbb{P}^1$) together with a choice of identification $\text{Gal}(X/\mathbb{P}^1) \simeq G$ and a choice of point over infinity, such that all inertia subgroups are generated by elements in $c$ and the place at $\infty$ is unramified (see [LWZB19, §11] for more details about this Hurwitz scheme). For each geometric point $\overline{\pi}$ on $\text{Hur}_{G,c}^n$ whose residue field has characteristic $p$, we can attach to it the lifting invariant $\delta_{\overline{\pi}}$ as defined above. The lifting invariant is actually a component invariant: for any algebraically closed field $k$, the $k$-points of $(\text{Hur}_{G,c}^n)_k$ in the same component have the same lifting invariant ([LWZB19, Cor.12.2]). Moreover, when $M$ is sufficiently large, there is a bijection between the set $\mathcal{K} := \{(g, m) \in K(G, c) | \text{coordinates of } m \text{ are at least } M \text{ and sum up to } n\}$ and the components of $(\text{Hur}_{G,c}^n)\mathbb{F}_q$ (and similarly, the components of $(\text{Hur}_{G,c}^n)\mathbb{C}$) whose lifting invariant has image in $\mathcal{K}$. In particular, by [LWZB19, Thm.12.1], if $\overline{\pi}$ is a $\mathbb{F}_q$-point of $(\text{Hur}_{G,c}^n)\mathbb{F}_q$, then for a $\zeta \in \hat{\mathbb{Z}}(1)_{(q)'}$, we have

$$\delta_{\text{Frob}(\overline{\pi})}(\zeta) = q^{-1} * \delta_{\overline{\pi}}(\zeta),$$

where $\text{Frob}$ is the Frobenius map $\text{Frob}_{(\text{Hur}_{G,c}^n)\mathbb{F}_q}$ and the * operator is as defined in (4.1).
In order to compute the number of $\mathbb{F}_q$-points of $\text{Hur}^n_{G,c}$ acting on $(\text{Hur}^n_{G,c})_{\mathbb{F}_q}$, by the Grothendieck–Lefschetz trace formula, it is crucial to understand the number of $\text{Frob}_{(\text{Hur}^n_{G,c})_{\mathbb{F}_q}}$-fixed components of $(\text{Hur}^n_{G,c})_{\mathbb{F}_q}$, which we denote by $\pi_{G,c}(q,n)$. For integers $n$ and $M$, we write $\mathbb{Z}^{c,G}_{\equiv q,n\geq M}$ for the subset of $\mathbb{Z}^{c,G}$ consisting of elements satisfying: 1) the coordinates are constant on each set of conjugacy classes of $c/G$ that can be obtained from one another by taking $q$th powers, 2) the coordinates sum up to $n$, and 3) each coordinate is at least $M$. Then there is a homomorphism $\mathbb{Z}^{c,G}_{\equiv q,n\geq M} \rightarrow G^{ab}$ that is the restriction of the natural map $\mathbb{Z}^{c,G} \rightarrow G^{ab}$. Then by [LWZB19, Prop.12.7], the number of $\text{Frob}_{(\text{Hur}^n_{G,c})_{\mathbb{F}_q}}$-fixed components of $(\text{Hur}^n_{G,c})_{\mathbb{F}_q}$ has the following estimation

$$
\pi_{G,c}(q,n) = b(G,c,q,n) + O_G(n^{d_G,c(q)-2}),
$$

(4.3)

where $d_{G,c}(q)$ is the number of orbits of $q$th powering on the conjugacy classes in $c/G$ and

$$
b(G,c,q,n) := \sum_{h \in \ker(S_c \rightarrow G)} \# \left\{ m \in \ker\left( \mathbb{Z}^{c,G}_{\equiv q,n\geq 0} \rightarrow G^{ab} \right) \left| W_{q-1}(m)^q = h^{q-1} \right. \right\}.
$$

The definition of $b(G,c,q,n)$ above appears differently from but agrees with the one in [LWZB19] (see the proof of [LWZB19, Prop.12.7]).

4.2. Relationship between the EVW-W lifting invariant and the invariant $\omega_{L/K}$. In this subsection, we will prove in Proposition 4.3 that the $\omega$-invariant $\omega_{L/K}$ equals the prime-to-$|\Gamma|$-torsion part the EVW-W lifting invariant. Throughout this subsection, we consider the EVW-W lifting invariants when $G$ is a semidirect product $H \rtimes \Gamma$ with $\gcd(|H|,|\Gamma|) = 1$ and $c$ is the set consisting of elements of $G\setminus\{1\}$ that have the same order as their image in $\Gamma$.

Lemma 4.1. Let $\Gamma$ be a finite group and $H$ a $|\Gamma|$-$\Gamma$-group. Suppose that there is a stem extension of groups

$$1 \rightarrow A \rightarrow \bar{H} \rtimes \Gamma \xrightarrow{\pi} H \rtimes \Gamma \rightarrow 1,
$$

such that $A$ has order prime to $|\Gamma|$. Let $x$ and $y$ be two elements of $H \rtimes \Gamma$ such that $[x,y] = 1$ and $x$ has order equal to the order of its image in $\Gamma$. Then $[\bar{x},\bar{y}] = 1$ for any lifts $\bar{x} \in \pi^{-1}(x)$ and $\bar{y} \in \pi^{-1}(y)$.

Proof. We let $\gamma$ denote the image of $\bar{x}$ in $\Gamma$. By the Schur–Zassenhaus theorem, we can pick a homomorphic splitting $s : \Gamma \rightarrow \bar{H} \rtimes \Gamma$ such that $s(\gamma) = \bar{x}$. We can redefine the group $\bar{H} \rtimes \Gamma$ as the semidirect product $\bar{H} \rtimes s(\Gamma)$, and then using the notation of elements in semidirect product, we write $\bar{x}$ as $(1,\gamma)$ and write $\bar{y}$ as $(b,\sigma)$ for $b \in \bar{H}$ and $\sigma \in \Gamma$. So $[\bar{x},\bar{y}] = \bar{x}^{-1}\bar{y}^{-1}\bar{x}\bar{y} = (\gamma^{-1} \circ \sigma^{-1}(b^{-1}\gamma(b)), [\gamma, \sigma])$. Since $[x,y] = 1$, we have that $[\gamma, \sigma] = 1$ and $b^{-1}\gamma(b) \in \ker\pi$, and it’s left to show that $b^{-1}\gamma(b) = 1$.

We consider the action of the subgroup $\langle \gamma \rangle$ of $\Gamma$ on the exact sequence

$$1 \rightarrow A \rightarrow \bar{H} \rightarrow H \rightarrow 1.
$$

For a $\langle \gamma \rangle$-group $G$, we denote $Y_\gamma(G) := \{ g^{-1}\gamma(g) \mid g \in G \}$. It follows by [LWZB19, Lem.3.5 and Lem.3.6] that $|[A] = |A^{(\gamma)}||Y_\gamma(A)|$, $|Y_\gamma(A)||Y_\gamma(H)| = |Y_\gamma(\bar{H})|$, and the elements of $Y_\gamma(\bar{H})$ are equidistributed in $Y_\gamma(H)$. Thus, because $\Gamma$ acts trivially on $A$, we see that $A^{(\gamma)} = A$, so $Y_\gamma(A) = 1$ and therefore $Y_\gamma(\bar{H}) \cap A = 1$. Then it follows that if $b^{-1}\gamma(b) \in \ker\pi$ for some $b \in \bar{H}$, then $b^{-1}\gamma(b) = 1$, which finishes the proof of the lemma.

Lemma 4.2. Let $p$ be a prime, $\Gamma$ a finite group, and $H$ a finite admissible $\Gamma$-group such that $p \parallel |H||\Gamma|$. Let $\mathbb{C}_p$ be the set $\Gamma \setminus \{1\}$. Let $G := H \rtimes \Gamma$ and $cg_G$ the set of elements of $G\setminus\{1\}$ that have the same order as their image in $\Gamma$.

30
(1) The order of the kernel of the quotient map $H_2(G, \mathbb{Z}) \to H_2(G, cG)$ has order supported on the set of prime divisors of $|\Gamma|$.

(2) The quotient map $G \to \Gamma$ induces a surjection $H_2(G, cG) \to H_2(\Gamma, c\Gamma)$, and the kernel of this surjection has order prime to $|\Gamma|$.

In particular, combining the two statements above, we have

$$H_2(G, cG) \cong H_2(G, \mathbb{Z})_{(p|\Gamma)'} \oplus H_2(\Gamma, c\Gamma). \quad (4.4)$$

Proof. Let $\pi : S \to G$ be a Schur covering of $G$, and $\pi_{cG} : S_{cG} \to G$ its reduced Schur covering associated to $cG$. By taking quotient of $S$ modulo the $|\Gamma|$-part of $\ker \pi$, we have a stem extension

$$1 \to (\ker \pi)(|\Gamma)') \to S' \to G \to 1. \quad (4.5)$$

Then by Lemma 4.1, the image of $\ker(S \to S_{cG})$ in $S'$ is trivial, so $\pi_{cG}$ factors through $S'$, which proves the statement (1).

By the proof of [LWZB19, Lem.12.10], there are compatible Schur coverings of $G$ and $\Gamma$

$$S \longrightarrow G \hspace{1cm} \downarrow \hspace{1cm} \downarrow \hspace{1cm} \downarrow \hspace{1cm} \Gamma$$

where the left vertical surjection is obtained by taking quotient of $S$ by the prime-to-$|\Gamma|$ part of $\ker(S \to G)$. By definition of $cG$ and $c\Gamma$, one can check that the diagram above defines the following compatible reduced Schur coverings, where the kernel of the left vertical map has order prime to $|\Gamma|$, which proves the statement (2) in the proposition.

$$S_{cG} \longrightarrow G \hspace{1cm} \downarrow \hspace{1cm} \downarrow \hspace{1cm} \downarrow \hspace{1cm} \Gamma$$

Finally, by a basic fact that a Schur covering group of $\Gamma$ (resp. $G$) has order supported on prime divisors of $|\Gamma|$ (resp. $|G|$), we have that $H_2(G, \mathbb{Z})_{(p|\Gamma)'}$ is the prime-to-$|\Gamma|$ completion of $H_2(G, cG)$ and $H_2(\Gamma, c\Gamma)$ is the $|\Gamma|$-completion of $H_2(G, cG)$, so the equality (4.4) follows.

**Proposition 4.3.** Let $k$, $K$, $p$, $\Gamma$ and $L$ be as described in Definition 2.13. Let $G$ denote the Galois group of $L\overline{k}/\overline{k}(t)$, and $c$ the set of elements of $G\backslash\{1\}$ that have the same order as their image in $\Gamma$ (where the quotient map $G \to \Gamma$ is defined by the tower of fields $L\overline{k}/K\overline{k}/\overline{k}(t)$). Then the composition map

$$\hat{\mathbb{Z}}(1)^{(p)\prime} \xrightarrow{\delta} K(G, c) \longrightarrow H_2(G, c) \longrightarrow H_2(G, \mathbb{Z})_{(p|\Gamma)'}$$

extends to the $\omega$-invariant $\omega_{L/K} : \hat{\mathbb{Z}}(1)^{(p|\Gamma)'} \to H_2(G, \mathbb{Z})_{(p|\Gamma)'}$ associated to $L/K$. Here $\delta$ is the EVW-W lifting invariant associated to $L\overline{k}/\overline{k}(t)$, the second map is the projection of from $K(G, c) = H_2(G, c) \times \mathbb{Z}^{c/G}$ to the first coordinate, and the last map is the prime-to-$(p|\Gamma)$ completion map, which is well-defined by Lemma 4.2 (1).

Proof. Let $\pi : S \to G$ be a Schur covering, and $\pi_{c} : S_{c} \to G$ its reduced Schur covering associated to $c$. Let $S' \to G$ be as defined in (4.5). The elements in $c$ have order dividing $|\Gamma|$. For each conjugacy class in $c/G$, we pick one element $x$ in this class, and then pick one preimage $\hat{x}$ of $x$ in $S_{c}$ such that the image of $\hat{x}$ in $S'$ is the unique preimage of $x$ whose order equals $\text{ord}(x)$. For any other element $y = g^{-1}xg$ in this conjugacy class, we define $\hat{y} := \hat{g}^{-1}\hat{x}\hat{g}$ for some preimage $\hat{g}$ of $g$ in $S_{c}$ (by [Woo21, Lem.2.3], $\hat{y}$ is independent of the choice of $\hat{g}$). By [Woo21, Thm.2.5], there is an
isomorphism from \( U(G, c) \) to \( S_c \times_{G^{ab}} \mathbb{Z}^c/G \) defined by mapping the generator \([x]\) for each \( x \in c\) to \((\tilde{x}, e_x)\), where \( e_x \) is the generator corresponding to the conjugacy class of \( x \).

Let \( q = (g_1, \ldots, g_m) \) be a system of inertia generators associated to \( K \), and \( \varphi \) and \( \tilde{\varphi} \) denote the surjections, defined in Corollary (4.3).

**Proof of Theorem**

We have shown in the next paragraph that this composition map extends to a group homomorphism \( \mathbb{Z}(1)_{(p)}(x) \to \ker(S' \to G) \), although \( \mathbb{Z}(1) \) is only a \( \mathbb{Z}(p) \)-equivariant map of sets. Then the proposition follows by composing the map (4.6) with the inverse of the differential map \( H_2(G, \mathbb{Z})(p) \to \ker(S' \to G) \).

For each \( x \in c \), we let \( \tilde{x} \) denote the unique preimage of \( x \) in \( S' \) such that \( \text{ord}(\tilde{x}) = \text{ord}(x) \). Recall that the lift \( \tilde{x} \) of \( x \) in \( S_c \) that we’ve picked has image \( \tilde{x} \) in \( S' \).

For each \( \alpha \in \mathbb{Z}(1)_{(p)}(x) \), we have \( \tilde{x}^\alpha = \tilde{x}^\alpha \), and hence \( \tilde{x}^a \bmod x^\alpha \) is contained in \( \ker(S_c \to S') \) for any \( x \in c \). So for any element \((g, m) \in K(G, c)\) (using notation in (4.1)), the image of \( \alpha \bmod (g, m) \) under the map \( K(G, c) \to \ker(S' \to G) \) equals the \( \text{ord} \) of the image of \((g, m)\). So we proved that (4.6) can extend to a group homomorphism \( \mathbb{Z}(1)_{(p)}(x) \to \ker(S' \to G) \).

4.3. **Proof of Theorem 1.1.** Throughout this subsection, we assume that \( \Gamma \) is a finite group and \( H \) is a finite admissible \( \Gamma \)-group. We define \( G := H \bowtie \Gamma \), let \( c_2 \) denote the set \( \Gamma \}\{1\}, and \( c_1 \) the set of elements of \( G\}\{1\} \) that have the same order as their image in \( \Gamma \). Let \( q \) be a power of a prime number \( p \) such that \( p \nmid |G| \).

By Lemma 4.2, there exists a commutative diagram of surjections

\[
\begin{array}{ccc}
S' & \xrightarrow{\pi'} & G \\
\downarrow{\pi^1} & & \downarrow{\rho} \\
S^2 & \xrightarrow{\pi^2} & \Gamma
\end{array}
\]

(4.7)

where \( \pi^1 \) is a reduced Schur covering of \( G \) and \( c_1 \), \( \pi^2 \) is a reduced Schur covering of \( \Gamma \) and \( c_2 \), and \( \pi' \) is a \((q\Gamma)'\)-Schur covering of \( G \). Moreover, since \( \text{gcd}(\text{ker} \circ \pi'|, \text{ker} \pi^2) = 1 \), \( S^2 \) is the fiber product \( S' \times_{\Gamma} S^2 \).

For a positive integer \( n \) and a group homomorphism \( \delta : \mathbb{Z}(1)_{(q\Gamma)'} \to \ker \pi' \), we let \( \pi^2_{G,c_1}(q, n) \) denote the number of \( \text{Frob}_G \) fixed components of \( \text{Frob}_G \) whose corresponding \( \omega \)-invariant is the composition of \( \delta \) with the inverse of the differential map of \( \pi' \). We pick a \( \zeta \in \mathbb{Z}(1)_{(q\Gamma)'} \) and let \( \eta := \delta(\zeta) \). Define the quantity \( b(G, c_1, q, n; \delta) \) as follows, which is independent of the choice of \( \zeta \).

\[
b(G, c_1, q, n; \delta) := \sum_{h \in \text{ker} \pi^1, s.t. \phi(h) = \eta} \# \left\{ m \in \text{ker} \left( \frac{\mathbb{Z}^{c_1/G}}{m, n} \to G^{ab} \right) \mid W_{q-1}(m)^q = h^{q-1} \right\}
\]

**Lemma 4.4.** Given an element \( a \in \left( \frac{\mathbb{Z}}{|G|^2} \right)^x \), there is a positive integer \( M_a \) and a non-empty set \( E_a \) of residues modulo \( M_a \), and positive numbers \( r_{a,b}^q \) for \( b \in E_a \), such that for a prime power \( q \equiv a \pmod{|G|^2} \) and a non-negative integer \( n \) the following holds.
\[(1) \text{ If } \text{ord}(\eta) | q - 1 \text{ and } n (\text{mod } M_a) = b \in E_a, \text{ then} \]
\[
\pi^\delta_{G,c_1}(q,n) = b(G,c_1,q,n;\delta) + O_G(n^{d_{G,c_1}(q)-2}) = r_{a,b}n^{d_{G,c_1}(q)-1} + O_G(n^{d_{G,c_1}(q)-2}).
\]

\[(2) \text{ If } \text{ord}(\eta) \nmid q - 1 \text{ or } n (\text{mod } M_a) \notin E_a, \text{ then} \pi^\delta_{G,c_1}(q,n) = b(G,c_1,q,n;\delta) = 0.
\]

**Proof.** By Proposition 4.3 and [LWZB19, Cor.12.6], $\pi^\delta_{G,c_1}(q,n)$ can be approximated by the number of $\hat{\mathbb{Z}}^{\times}_{(p)'}$-equivariant maps of sets $\mathfrak{z} : \hat{\mathbb{Z}}(1)_{(p)'} \rightarrow K(G,c_1)$ such that $\mathfrak{z}$ reduces to $\delta$ and all coordinates of the image of $\mathfrak{z}$ composition with the projection $K(G,c_1) \rightarrow \mathbb{Z}^{c_1/G}$ is at least $M$ for a sufficiently large $M$. Then the lemma follows from the proof of Proposition 12.7 and Corollary 12.9 of [LWZB19].

**Lemma 4.5.** For any group homomorphism $\delta : \hat{\mathbb{Z}}(1)_{(p|\Gamma)'} \rightarrow \ker \pi'$ such that $\text{ord}(\text{im } \delta) | q - 1$, we have
\[
b(G,c_1,q,n;\delta) = b(\Gamma,c_2,q,n).
\]

**Proof.** By definition of $c_1$ and $c_2$, the quotient map $\rho : G \rightarrow \Gamma$ sends each element $c_1$ to an element in $c_2$. Moreover, as $\text{gcd}(|H|,|\Gamma|) = 1$, by the Schur–Zassenhaus theorem, for each element of $c_2$, all of its lifts in $c_1$ are conjugate to each other, thus there is a natural bijective correspondence $\mathbb{Z}^{c_1/G} \rightarrow \mathbb{Z}^{c_2/\Gamma}$ induced by $\rho$. Since $H$ is an admissible $\Gamma$-group, we have $G^{ab} = \Gamma^{ab}$, so the restriction of this bijection gives a natural isomorphism $\ker(\mathbb{Z}^{c_1/G} \rightarrow G^{ab}) \simeq \ker(\mathbb{Z}^{c_2/\Gamma} \rightarrow \Gamma^{ab})$.

We write the group homomorphisms $W_{\alpha}^1 : \mathbb{Z}^{c_1/G} \rightarrow \ker(S^1 \xrightarrow{\pi_1} G)$ and $W_{\alpha}^2 : \mathbb{Z}^{c_2/\Gamma} \rightarrow \ker(S^2 \xrightarrow{\pi_2} \Gamma)$

\[
\begin{array}{ccc}
\mathbb{Z}^{c_1/G} & \xrightarrow{W_{\alpha}^1} & \ker(S^1 \xrightarrow{\pi_1} G) \\
\sim & & \downarrow \bar{\rho} \\
\mathbb{Z}^{c_2/\Gamma} & \xrightarrow{W_{\alpha}^2} & \ker(S^2 \xrightarrow{\pi_2} \Gamma)
\end{array}
\]

Pick a $\zeta \in \hat{\mathbb{Z}}(1)_{(p|\Gamma)'}$ and let $\eta := \delta(\zeta)$. Considering the diagram (4.7) and the isomorphism $S^1 \simeq S^\prime \times_{\Gamma} S^2$, we obtain the following identity of sets
\[
\left\{ h \in \ker(S^1 \xrightarrow{\pi_1} G) \middle| \phi(h) = \eta \right\} \overset{1-1}{\longleftrightarrow} \ker(S^2 \xrightarrow{\pi_2} \Gamma) \quad h \longmapsto \bar{\rho}(h).
\]

Therefore, combining everything, we have
\[
b(G,c_1,q,n;\delta) = \sum_{h \in \ker(S^1 \xrightarrow{\pi_1} G) \atop \text{s.t. } \phi(h) = \eta} \# \left\{ m \in \ker \left(\mathbb{Z}^{c_1/G}_{\equiv q,n \geq 0} \rightarrow G^{ab} \right) \middle| W_{q-1}^1(m)^q = h^{q-1} \right\} \\
= \sum_{h \in \ker(S^2 \xrightarrow{\pi_2} \Gamma)} \# \left\{ m \in \ker \left(\mathbb{Z}^{c_2/\Gamma}_{\equiv q,n \geq 0} \rightarrow \Gamma^{ab} \right) \middle| W_{q-1}^2(m)^q = h^{q-1} \right\} \\
= b(\Gamma,c_2,q,n).
\]

\[\square\]
By the correspondence between smooth projective curves and their function fields, $\text{Hur}_{G,c_1}^a(\mathbb{F}_q)$ parametrizes the pairs $(L,\iota)$, where $L$ is an extension of $\mathbb{F}_q(t)$ that is split completely at $\infty$ and has $\mathrm{rDisc} L = q^n$, and $\iota$ is an isomorphism $\text{Gal}(L/\mathbb{F}_q(t)) \sim G$ such that each inertia subgroup of $L/\mathbb{F}_q(t)$ is generated by an element in $c_1$. We fix a surjection $\rho : G \to \Gamma$ as defined in the diagram (4.7). Then for each pair $(L,\iota)$, consider the subfield $K := L_{\ker(\rho \circ \iota)}$ of $L$. The surjection $\rho \circ \iota$ defines an isomorphism $\text{Gal}(K/\mathbb{F}_q(t)) \to \Gamma$, and moreover $L/K$ is unramified and $\mathrm{rDisc}(K) = q^n$. Then the restriction of $\iota$ to $\text{Gal}(L/K)$ gives an isomorphism $\text{Gal}(L/K) \to H$.

Lemma 4.6. There is a surjective map of sets

$$\text{Hur}_{G,c_1}^a(\mathbb{F}_q) \longrightarrow \coprod_{K \in E_\iota(q^n,\mathbb{F}_q(t))} \text{Sur}_\Gamma(G^\#_\iota(K), H)$$

(4.8)

where $\iota$ is given by

$$(L,\iota) \longmapsto \{ G^\#_\iota(K) \to \text{Gal}(L/K) \}.$$ 

Each element in the set on the right has $[H:H^\Gamma]$ preimages.

Proof. The lemma follows by the proofs of Lemmas 9.3 and 10.2 in [LWZB19]. \hfill \Box

Let $q$ be a prime power such that $\gcd(q,|G|) = 1$ and $\mathrm{ord}(\mathrm{im}\delta)|q-1$. Then taking $q$th power on $\mathrm{im}\delta$ is the identity map. So by the Frobenius action on lifting invariants in (4.2) and Proposition 4.3, if there is a $\mathbb{F}_q$-point of a connected component of $(\text{Hur}_{G,c_1}^a)_{\mathbb{F}_q}$ has $\omega$-invariant $\delta$, then all the $\mathbb{F}_q$-point of this component have $\omega$-invariant $\delta$. So we let $Z_{q,n}^\delta$ be the union of components of $(\text{Hur}_{G,c_1}^a)_{\mathbb{F}_q}$ whose $\mathbb{F}_q$-points have $\omega$-invariant $\delta$. By Lemma 4.6, we have

$$\frac{\#Z_{q,n}^\delta(\mathbb{F}_q)}{[H:H^\Gamma]} = \sum_{K \in E_\iota(q^n,\mathbb{F}_q(t))} \# \left\{ \pi \in \text{Sur}_\Gamma \left( G^\#_\iota(K), H \right) \mid \pi^* \circ \omega^\#_K = \delta \right\}.$$ 

By the Grothendieck–Lefschetz trace formula, since $(Z_{q,n})_{\mathbb{F}_q}$ is $n$-dimensional ([LWZB19, Lem.10.3]), we have

$$\#Z_{q,n}^\delta(\mathbb{F}_q) = \sum_{j=0}^{2n} (-1)^j \text{Tr}(\text{Frob}_{\mathbb{F}_q} | H^j_{c,\text{ét}}((Z_{q,n})_{\mathbb{F}_q}, \mathbb{Q}_\ell))$$

where $H^j_{c,\text{ét}}$ is the $j$th étale fundamental group with compact support. Here $\text{Tr}(\text{Frob}_{\mathbb{F}_q} | H^j_{c,\text{ét}}((Z_{q,n})_{\mathbb{F}_q}, \mathbb{Q}_\ell))$ is $\pi^\delta_{G,c_1}(q,n)q^n$ when $j = 2n$, and is at most $q^{j/2}C(n)$ when $0 \leq j < 2n$ by the comparison of étale and analytic cohomology of components of the Hurwitz scheme [LWZB19, Lem.10.3]. Here

$$C(n) = \max_{0 \leq j < 2n} \dim H^{2n-j}(Z_{\mathbb{C},n}^\delta, \mathbb{Q}),$$

where $Z_{\mathbb{C},n}^\delta$ is the union of components of $(\text{Hur}_{G,c_1}^a)_{\mathbb{C}}$ whose prime-to-$|\Gamma|$-torsion part of the EVW-W lifting invariant

$$\hat{\gamma}(1)^s \to K(G,c_1) \to H_2(G,\mathbb{Z})/(|\Gamma|)$$

is given by $\delta$. So we round down $N$ to the nearest integer whose residue mod $M_a$ is in $E_a$, and so we have

$$\sum_{n \leq N} \#Z_{q,n}^\delta(\mathbb{F}_q) = \pi^\delta_{G,c_1}(q,N)q^N + O_{N,G}(q^{N-1/2}).$$

Similarly, $E_\iota(q^n,\mathbb{F}_q(t)) = \#\text{Hur}_{1,c_2}^a(\mathbb{F}_q)$, and

$$\sum_{n \leq N} \#\text{Hur}_{1,c_2}^a(\mathbb{F}_q) = \pi_{1,c_2}(q,N)q^N + O_{N,\Gamma}(q^{N-1/2}).$$
Therefore, the fraction in the limits of the left-hand side of the equality in Theorem 1.1 equals
\[
\frac{1}{[H : H^1]} \sum_{n \leq N} \# \text{Hur}^\tau_{c_2}(\mathbb{F}_q) = \frac{1}{[H : H^1]} \sum_{n \leq N} \# \text{Hur}^\tau_{c_2}(\mathbb{F}_q) = \frac{1}{[H : H^1]} \left( \frac{\pi_{G,\sigma_1}(q, N)q^N + O_{N,G}(q^{N-1/2})}{\pi_{G,\sigma_2}(q, N)q^N + O_{N,G}(q^{N-1/2})} \right),
\]
where the last equality follows by Lemmas 4.4, 4.5 and [LWZB19, Prop.12.7]. Then the equality in Theorem 1.1 follows after taking limits.

5. A random pro-$\ell$ $\Gamma$-group for $\Gamma = \mathbb{Z}/2\mathbb{Z}$

In this section, we assume that $\Gamma = \mathbb{Z}/2\mathbb{Z}$, and $\ell$ is an odd prime that is not char$(k)$. We construct a random group to model the distribution of $G^\#_\mathbb{Q}(K)(\ell)$ as $K$ varies among all the quadratic extensions of $k(t)$ that is split completely at $\infty$.

Recall that $G^\#_0(K\overline{K})(\ell)$ is a pro-$\ell$ Demuškin group whose abelianization is free of rank $2g$, where $g$ is the genus of the curve over $\overline{k}$ corresponding to $K\overline{K}$. We’ve shown that $G^\#_0(K\overline{K})(\ell)$ has a $\Gamma$ action and a Frobn action, and it admits a $\Gamma$-equivariant and Frobn-equivariant stem extension (3.8) whose kernel is isomorphic to $\mathbb{Z}_2(1)$. Moreover, $G^\#_0(K)(\ell)$ is the maximal $\Gamma$-equivariant and Frobn-equivariant quotient of $G^\#_0(K\overline{K})(\ell)$ whose induced Frobn-action is trivial. So our strategy is to treat the Frobn action as a random automorphism of the stem extension. We start with a Demuškin group with desired properties, pick a random automorphism that acts on the kernel of the stem extension as taking the $|k|$-th powers. Then define the random group to be the maximal quotient fixed by this random automorphism, as the generating rank of the Demuškin group goes to infinity.

5.1. Construction of the random group. By the classification of Demuškin groups [NSW08, Thm.(3.9.11)], if a Demuškin group has abelianization isomorphic to $\mathbb{Z}_2^{2n}$, then it is isomorphic to $\langle x_1, \ldots, x_{2n} \mid [x_1,x_2][x_3,x_4] \cdots [x_{2n-1},x_{2n}] \rangle$. In the following lemma, we show that there is a unique (up to isomorphism) $\mathbb{Z}/2\mathbb{Z}$-action on this type of Demuškin group such that the Demuškin group is an admissible $\mathbb{Z}/2\mathbb{Z}$-group.

Lemma 5.1. Let $G$ be a pro-$\ell$ group and $\sigma_1, \sigma_2 \in \text{Aut}(G)$ have the same order which is prime to $\ell$. Assume that $\pi : G \to H$ is a surjection such that ker $\pi \subset [G,G]$, and that $\sigma_1, \sigma_2$ preserve ker $\pi$ and induce the same automorphism on $H$. Then there exists $\tau \in \text{Aut}(G)$ such that $\sigma_1 = \tau^{-1} \circ \sigma_2 \circ \tau$ and $\tau$ preserves ker $\pi$ and induces the trivial action on $H$.

Proof. Consider the subgroup Aut$(G,\pi)$ of Aut$(G)$ consisting of all the automorphisms of $G$ preserving ker $\pi$. There is a natural map $\alpha : \text{Aut}(G,\pi) \to \text{Aut}(H)$. Since ker $\pi \subset [G,G]$, by [Gor80, Chap.5, Thm.3.5], the kernel of $\alpha$ is a pro-$\ell$ group. The assumptions in the lemma imply that $\alpha(\sigma_1)$ equals $\alpha(\sigma_2)$ and has order prime to $\ell$. Then by the Schur–Zassenhaus theorem, $\sigma_1$ and $\sigma_2$ are conjugate in Aut$(G,\pi)$ (and hence in Aut$(G)$) by an element in ker $\alpha$. \hfill $\square$

Lemma 5.2. Let $n$ be a positive integer and $\mathcal{G}_n$ a Demuškin group whose abelianization is isomorphic to $\mathbb{Z}_2^n$. Then $\mathcal{G}_n$ admits a Schur covering (unique up to isomorphism)
\[
1 \longrightarrow \mathbb{Z}_\ell \longrightarrow \widetilde{\mathcal{G}}_n \xrightarrow{\pi_n} \mathcal{G}_n \longrightarrow 1.
\]
There exists a $\mathbb{Z}/2\mathbb{Z}$ action on $\widetilde{\mathcal{G}}_n$ such that the action preserves and acts trivially on ker $\pi_n$ and its induced action on $\mathcal{G}_n^{ab}$ is taking inversion. Moreover, if $\sigma_1$ and $\sigma_2$ are two such $\mathbb{Z}/2\mathbb{Z}$ actions on $\widetilde{\mathcal{G}}_n$, then there exists an automorphism $\tau$ of $\widetilde{\mathcal{G}}_n$ such that $\sigma_1 = \tau^{-1} \circ \sigma_2 \circ \tau$, and $\tau$ preserves $[\widetilde{\mathcal{G}}_n, \widetilde{\mathcal{G}}_n]$ and induces the trivial action on $\mathcal{G}_n^{ab}$.
Proof. Consider the pro-$\ell$ group defined by the following presentation
\[ G := \langle x_1, \ldots, x_{2n} \mid x_1^{-1} x_2^{-1} \cdots x_{2n}^{-1} x_1 x_2 \cdots x_{2n} \rangle. \] (5.1)

Let $F$ denote the free pro-$\ell$ generated by $x_1, \ldots, x_{2n}$, and let $R$ denote the closed normal subgroup of $F$ generated by $x_1^{-1} \cdots x_{2n}^{-1} x_1 \cdots x_{2n}$. Note that
\[
x_1^{-1} \cdots x_{2n}^{-1} x_1 \cdots x_{2n} \equiv [x_1, x_2] [x_1 x_2, x_2] \cdots [x_1 x_2, x_{2n}] [x_1 x_{2n}, x_{2n}] \cdots [x_2, x_{2n}] \mod F(3).\]

By repeating this process, we have $x_1^{-1} \cdots x_{2n}^{-1} x_1 \cdots x_{2n} \equiv \prod_{1 \leq i < j \leq 2n} [x_i, x_j] \mod F(3)$. So by [NSW08, Prop.3.9.13(ii)], the cup product $H^1(G, \mathbb{Z}_\ell) \times H^1(G, \mathbb{Z}_\ell) \to H^2(G, \mathbb{Z}_\ell)$ is non-degenerate. Moreover, $G^{ab}$ is free of rank $2n$. So $G$ is a Demuškin group whose abelianization is isomorphic to $\mathbb{Z}_\ell^{2n}$ and hence is isomorphic to $\tilde{G}_n$, and we will use this presentation (5.1) of $\tilde{G}_n$ in the rest of the proof.

The existence and uniqueness of the Schur covering $\pi_n$ follow immediately from $H_2(G, \mathbb{Z}) \simeq \mathbb{Z}_\ell$ and $\text{Ext}^1_{\mathbb{Z}}(G^{ab}, \mathbb{Z}_\ell) = 0$. We define $\sigma \in \text{Aut}(F)$ by $\sigma(x_i) = x_i^{-1}$. We will show next that $\sigma$ induces a $\mathbb{Z}/2\mathbb{Z}$ action on $\tilde{G}_n$ as described in the lemma. First, because
\[ \sigma(x_1^{-1} \cdots x_{2n}^{-1} x_1 \cdots x_{2n}) = x_1 \cdots x_{2n} x_1^{-1} \cdots x_{2n}^{-1} = (x_1^{-1} \cdots x_{2n}^{-1} x_1 \cdots x_{2n}) x_1^{-1} \cdots x_{2n}^{-1}, \] (5.2)

the automorphism $\sigma$ stabilizes $R$. So $\sigma$ induces an automorphism $\overline{\sigma}$ of $G$, and $\overline{\sigma}$ acts on $G^{ab}$ by inversion. The presentation of $G$ defines a stem extension of $G$ with kernel isomorphic to $\mathbb{Z}_\ell$

\[ 1 \to R/[F, R] \to F/[F, R] \to G \to 1, \]

where the image of $x_1^{-1} \cdots x_{2n}^{-1} x_1 \cdots x_{2n}$ generates the kernel $R/[F, R]$. So (5.2) shows that $\sigma$ preserves $[F, R]$, and hence it induces an automorphism of $F/[F, R]$, and moreover this automorphism acts trivially on $R/[F, R]$. So we proved the existence of the $\mathbb{Z}/2\mathbb{Z}$ action on $\tilde{G}_n$ as described in the lemma.

Suppose that $\sigma_1$ and $\sigma_2$ are two $\mathbb{Z}/2\mathbb{Z}$ actions on $\tilde{G}_n$ as described in the lemma. Then since they induce the same automorphism on $G^{ab}$, the last statement of the lemma follows by Lemma 5.1. □

Definition 5.3 (Definition of the random group). Let $n$ be a positive integer, $\mathcal{G}_n$, $\tilde{\mathcal{G}}_n$, $\pi_n$ and the $\Gamma = \mathbb{Z}/2\mathbb{Z}$ action on them be as defined in Lemma 5.2, and $q$ be a positive integer such that $\ell \nmid q$. We fix a generator $\xi_n$ of $\ker \pi_n$. Let $\text{Aut}(\tilde{\mathcal{G}}_n \rtimes \Gamma, \pi_n; q)$ denote the set of automorphisms of $\tilde{\mathcal{G}}_n \rtimes \Gamma$ that preserves and acts as multiplication by $q$ on $\ker \pi_n$. Let $\phi$ be a random element of $\text{Aut}(\tilde{\mathcal{G}}_n \rtimes \Gamma, \pi_n; q)$ with respect to the “Haar” measure. We let $1 - \phi$ denote the quotient map from $\tilde{\mathcal{G}}_n \rtimes \Gamma$ to its maximal $\Gamma$-equivariant quotient on which the induced $\phi$ action is trivial. Then we define the random group $X_{q, n}$ as
\[ X_{q, n} := (1 - \phi)(\tilde{\mathcal{G}}_n \rtimes \Gamma)/(1 - \phi)(\ker \pi_n). \] (5.3)

Moreover, we fix a homomorphic splitting of $\tilde{\mathcal{G}}_n \rtimes \Gamma \to \Gamma$ and hence an action of $\Gamma$ (by conjugation) on $\tilde{\mathcal{G}}_n$. Then $\ker (X_{q, n} \to \Gamma)$ naturally obtains an action of $\Gamma$. We define the following random $\Gamma$-group
\[ Y_{q, n} := \ker (X_{q, n} \to \Gamma). \]

Remark 5.4. (1) We need to explain what the “Haar” measure is in the definition. Since $\tilde{\mathcal{G}}_n \rtimes \Gamma$ is a finitely generated profinite group, $\text{Aut}(\tilde{\mathcal{G}}_n \rtimes \Gamma)$ is profinite by [RZ10, Cor.4.4.4]. The subgroup $\text{Aut}(\tilde{\mathcal{G}}_n \rtimes \Gamma, \pi_n; 1)$ consisting of all automorphisms that stabilizes and acts trivially on $\ker \pi_n$ is a closed subgroup of $\text{Aut}(\tilde{\mathcal{G}}_n \rtimes \Gamma)$, so it is a profinite group, and hence has a Haar measure. Then since $\text{Aut}(\tilde{\mathcal{G}}_n \rtimes \Gamma, \pi_n; q)$ is a coset of $\text{Aut}(\tilde{\mathcal{G}}_n \rtimes \Gamma, \pi_n; 1)$
in \( \text{Aut}(\hat{G}_n \rtimes \Gamma) \), it obtains a measure from the measure on \( \text{Aut}(\hat{G}_n \times \Gamma, \pi_n; 1) \), which is the “Haar” measure in the definition.

(2) Since \( \ell \) is odd, \( \hat{G}_n \) is a characteristic subgroup of \( \hat{G}_n \rtimes \Gamma \) and then \( \phi \) preserves \( \hat{G}_n \). Any action on \( \mathbb{Z}/2\mathbb{Z} \) is trivial, so \( \ker(1 - \phi) \) is contained in \( \hat{G}_n \) for any \( \phi \).

5.2. Computing the moment of the random group.

**Lemma 5.5.** Consider the Schur covering \( 1 \to \mathbb{Z}_\ell \to \hat{G}_n \xrightarrow{\pi_n} G_n \to 1 \). Let \( \xi_n \) be a generator of \( \ker \pi_n \). Let \( H \) be a pro-\( \ell \)-group, \( \varpi : \tilde{H} \to H \) a Schur covering of \( H \), and \( \rho : \hat{G}_n \to H \) a group surjection.

1. Then \( \rho \) can be lifted to a surjection \( \tilde{\rho} : \hat{G}_n \to \tilde{H} \) such that \( \varpi \circ \tilde{\rho} = \rho \circ \pi_n \). Moreover, the image \( \tilde{\rho}(\xi_n) \) in \( \tilde{H} \) does not depend on the choice of the lift \( \tilde{\rho} \).

2. Given \( \rho_1, \rho_2 \in \text{Sur}(\hat{G}_n, H) \), let \( \tilde{\rho}_1, \tilde{\rho}_2 \in \text{Sur}(\hat{G}_n, \tilde{H}) \) be their lifts respectively. Assume that \( \tilde{\rho}_1(\xi_n) = \tilde{\rho}_2(\xi_n) \). Then for any \( q \in \mathbb{Z}_\ell^\times \), \( \text{ord}(\tilde{\rho}_1(\xi_n)) = q - 1 \), there exists \( \tilde{\varphi} \in \text{Aut}(\hat{G}_n) \) such that
   (a) \( \tilde{\varphi} \) preserves \( \ker \pi_n \) and induces \( \varphi \in \text{Aut}(G_n) \) such that \( \rho_1 = \rho_2 \circ \varphi \), and
   (b) \( \tilde{\varphi}(\xi_n) = \xi_n^q \).

We will give the proof of this lemma in \( \S 5.3 \), which heavily uses the method in [Lab67] of successive approximation on the filtration of lower \( \ell \)-central series of pro-\( \ell \)-groups.

Let \( H \) be a finite \( \ell \)-group with an action of \( \Gamma \), and let \( \pi \in \text{Sur}(X_{q,n}, H \rtimes \Gamma) \) (or \( \pi \in \text{Sur}(Y_{q,n}, H) \) when we fix the action of \( \Gamma \) on \( G_n \)). Consider the composition map \( \hat{G}_n \rtimes \Gamma \xrightarrow{1/\phi} X_{q,n} \xrightarrow{\pi} H \rtimes \Gamma \) and let \( \varpi : \tilde{H} \rtimes \Gamma \to H \rtimes \Gamma \) be an \( \ell \)-Schur covering. By Lemma 2.14, there is a surjection \( \hat{G}_n \rtimes \Gamma \to \tilde{H} \rtimes \Gamma \) satisfying the following commutative diagram

\[
\begin{array}{cccc}
1 & \to & \mathbb{Z}_\ell & \to \hat{G}_n \rtimes \Gamma & \xrightarrow{\pi_n} G_n \rtimes \Gamma & \to 1 \\
\downarrow & & \downarrow & & \downarrow & & \\
1 & \to & \ker \varpi & \to \tilde{H} \rtimes \Gamma & \xrightarrow{\varpi} H \rtimes \Gamma & \to 1,
\end{array}
\]

such that the first vertical arrow in the diagram is the composition of

\[
\begin{align*}
\mathbb{Z}_\ell & \xrightarrow{d_{\mathbb{Z}_\ell}^{-1}} H_2(\hat{G}_n \rtimes \Gamma, \mathbb{Z})(\ell) & \xrightarrow{\text{coinf}} H_2(H \rtimes \Gamma, \mathbb{Z})(\ell) & \xrightarrow{d_{\mathbb{Z}_\ell}} \ker \varpi,
\end{align*}
\]

where the middle map \( \text{coinf} \) is induced by the quotient map \( \pi \circ (1 - \phi) \). We denote the composition of the first two maps by \( \pi_\dag : \mathbb{Z}_\ell \to H_2(H \rtimes \Gamma, \mathbb{Z})(\ell) \). Because the sequence is \( \phi \)-equivariant, \( \pi_\dag \) factors through \( \mathbb{Z}_\ell \to \mathbb{Z}_\ell/(q - 1)\mathbb{Z}_\ell \).

**Theorem 5.6.** Let \( H \) be a finite \( \ell \)-group with an action of \( \Gamma = \mathbb{Z}/2\mathbb{Z} \) that acts on \( H^{ab} \) as inversion. Let \( n \) be a sufficiently large integer such that there exists a \( \Gamma \)-equivariant surjection from \( \hat{G}_n \) to \( H \). Let \( \delta \) be a group homomorphism \( \mathbb{Z}_\ell \to H_2(H \rtimes \Gamma, \mathbb{Z})(\ell)[q - 1] \). Then

\[
\mathbb{E}(\# \{ \pi \in \text{Sur}(X_{q,n}, H \rtimes \Gamma) \mid \pi_\dag = \delta \}) = 1
\]

Also, if we fix a homomorphic splitting of \( \hat{G}_n \rtimes \Gamma \to \Gamma \) (that is, we fix the action of \( \Gamma \) on \( \hat{G}_n \)), then

\[
\mathbb{E}(\# \{ \pi \in \text{Sur}(Y_{q,n}, H) \mid \pi_\dag = \delta \}) = \frac{1}{[H : H^{ab}]}.
\]

**Proof.** For any \( \pi \in \text{Sur}(\hat{G}_n \rtimes \Gamma, H \rtimes \Gamma) \), by Lemma 2.14, there exists \( \tilde{\pi} \in \text{Sur}(\hat{G}_n \rtimes \Gamma, \tilde{H} \rtimes \Gamma) \) such that \( \pi \circ \pi_n = \varpi \circ \tilde{\pi} \). Let’s prove that there is a unique such \( \tilde{\pi} \). Let \( S \) be the closed subgroup of \( \hat{G}_n \rtimes \Gamma \) generated by all elements of order 2. Then \( S \) is normal because the set of all the order-2 elements are closed under conjugation. The quotient \( \hat{G}_n \rtimes \Gamma / S \) is a \( \Gamma \)-equivariant pro-\( \ell \) quotient.
Thus, the probability in \( \bar{\pi} \) induces the same action on \( \Gamma \) and \( \bar{\pi} \) must map each order-2 element \( x \) of \( \bar{G}_n \times \Gamma \) to the unique lift of \( \pi \circ \pi_n(x) \), which finishes the proof of the uniqueness of \( \bar{\pi} \). So for each \( \pi \in \text{Sur}(G_n \times \Gamma, \bar{H} \times \Gamma) \), we let \( \bar{\pi} \) denote its unique lift \( \text{Sur}(G_n \times \Gamma, \bar{H} \times \Gamma) \).

Next, we prove the first equality in the theorem. Let \( h = d_\omega \circ \delta(\xi_n) \). Note that

\[
\mathbb{E} (\# \{ \pi \in \text{Sur}(X_{q,n}, H \times \Gamma) \mid \pi_\parallel = \delta \}) = \sum_{\pi \in \text{Sur}(G_n \times \Gamma, H \times \Gamma) \atop \text{s.t. } \pi(\xi_n) = h} \text{Prob} (\phi \in \text{Aut}(\bar{G}_n \times \Gamma, \pi_n, q) \mid \ker (1 - \phi) \subseteq \ker \bar{\pi}). \tag{5.4}
\]

The condition \( \ker (1 - \phi) \subseteq \ker \bar{\pi} \) is equivalent to \( \bar{\pi} \circ \phi = \bar{\pi} \). We let \( \text{Sur}(G_n \times \Gamma, H \times \Gamma; \xi_n \mapsto h) \) denote the set of \( \pi \) as described under the sum in (5.4), and let \( \pi \in \text{Sur}(G_n \times \Gamma, H \times \Gamma; \xi_n \mapsto h) \). Each \( \phi \in \text{Aut}(\bar{G}_n \times \Gamma, \pi_n, q) \) passes \( \bar{\pi} \) to another surjection \( \bar{\pi} \circ \phi \in \text{Sur}(\bar{G}_n \times \Gamma, \bar{H} \times \Gamma) \), and the assumption \( \text{ord}(h) \mid q - 1 \) implies that \( \bar{\pi} \circ \phi(\xi_n) = h \), so \( \bar{\pi} \circ \phi \) induces a surjection in \( \text{Sur}(G_n \times \Gamma, H \times \Gamma; \xi_n \mapsto h) \).

In other words, \( \text{Aut}(\bar{G}_n \times \Gamma, \pi_n, q) \) acts on the set \( \text{Sur}(G_n \times \Gamma, H \times \Gamma; \xi_n \mapsto h) \), and in particular, the stabilizer of \( \pi \) by this action is exactly the set of \( \phi \in \text{Aut}(\bar{G}_n \times \Gamma, \pi_n, q) \) such that \( \ker (1 - \phi) \subseteq \ker \bar{\pi} \). Thus, the probability in (5.4) is the inverse of the size of the orbit containing \( \pi \). In the rest of the proof, we will prove that the set \( \text{Sur}(G_n \times \Gamma, H \times \Gamma; \xi_n \mapsto h) \) contains only one orbit. After proving that, it immediately follows that (5.4) equals 1, and hence we finish the proof of the theorem.

Let \( \pi_1, \pi_2 \in \text{Sur}(G_n \times \Gamma, H \times \Gamma; \xi_n \mapsto h) \), and let \( \bar{\pi}_1 \) and \( \bar{\pi}_2 \) denote the lifts of \( \pi_1 \) and \( \pi_2 \) respectively. Let \( \rho_1 \) (resp. \( \rho_2 \)) be the restriction of \( \pi_1 \) (resp. \( \bar{\pi}_i \)) onto \( G_n \) (resp. \( \bar{G}_n \)) for \( i = 1, 2 \). Then \( \bar{\rho}_i(\xi_n) = \bar{\pi}_i(\xi_n) = h \), so by Lemma 5.5(2), there exists \( \bar{\varphi} \in \text{Aut}(\bar{G}_n) \) satisfying (2a) and (2b). This automorphism \( \bar{\varphi} \) is not necessarily \( \Gamma \)-equivariant, however, we will show below that we can modify \( \bar{\varphi} \) to make it \( \Gamma \)-equivariant. Let \( \varphi \in \text{Aut}(G_n) \) be as described in Lemma 5.5(2a). The automorphism \( \varphi \) passes the action of \( \gamma \) (the non-trivial element of \( \Gamma \)) on \( G_n \) to an action of \( \bar{\varphi} \gamma \) which is defined by

\[
\bar{\varphi} \gamma (g) = \varphi \circ \gamma \circ \varphi^{-1}(g) \quad \text{for } g \in G_n.
\]

Because of \( \rho_2 \circ \varphi = \rho_1 \) and that \( \rho_1, \rho_2 \) extend to \( \pi_1, \pi_2 \), it follows that \( \gamma \) and \( \bar{\varphi} \gamma \) both preserve \( \ker \rho_2 \) and they induce the same action on \( H \) via the quotient map \( \rho_2 \), where the latter is because for any \( g \in G_n \)

\[
\rho_2 \circ \varphi \circ \gamma \circ \varphi^{-1}(g) = \rho_1 \circ \gamma \circ \varphi^{-1}(g) = \gamma \circ \rho_1 \circ \varphi^{-1}(x) = \gamma \circ \rho_2(x) = \rho_2 \circ \gamma (x).
\]

Also, the actions of \( \gamma \) and \( \bar{\varphi} \gamma \) induce the same action on \( \tilde{G}_n^{ab} \) (which is taking inversion). So, we let \( M := [G_n, G_n] \cap \ker \rho_2 \), and we see that the actions of \( \gamma \) and \( \bar{\varphi} \gamma \) induce the same action on \( G_n/M \). By Lemma 5.1, there exists \( \tau \in \text{Aut}(G_n) \) such that \( \bar{\varphi} \gamma = \tau^{-1} \circ \gamma \circ \tau \) and \( \tau \) preserves \( M \) and induces the trivial action on \( G_n/M \). Thus, \( \tau \circ \varphi \) is a \( \Gamma \)-equivariant automorphism of \( G_n \) such that \( \rho_2 \circ \tau \circ \varphi = \rho_1 \). Because \( \pi_n : \tilde{G}_n \rightarrow G_n \) is a Schur covering, by Lemma 5.5(1), there exists \( \bar{\tau} \in \text{Aut}(\bar{G}_n) \) such that \( \pi_n \circ \bar{\tau} = \tau \circ \pi_n \). Next, we consider the actions on \( \bar{G}_n \), and similarly to above arguments, \( \bar{\varphi} \) passes the action of \( \gamma \) on \( \bar{G}_n \) to an action of \( \bar{\varphi} \gamma \). Then because \( \bar{\varphi} \gamma = \tau^{-1} \circ \gamma \circ \tau \) as actions on \( G_n \), we have that \( \bar{\varphi} \gamma \) and \( \bar{\tau}^{-1} \circ \gamma \circ \bar{\tau} \) are two order-2 automorphisms of \( \bar{G}_n \) that preserve \( \ker \pi_n \) and induce the same automorphism on \( G_n \). So, by Lemma 5.1, there exists \( \sigma \in \text{Aut}(\bar{G}_n) \) such that \( \bar{\varphi} \gamma = \sigma^{-1} \circ \bar{\tau}^{-1} \circ \gamma \circ \bar{\tau} \circ \sigma \) and \( \sigma \) preserves \( \ker \pi_n \) and induces the trivial action on \( G_n \). Therefore,
we obtain an automorphism \( \varphi' := \tau \circ \sigma \circ \varphi \in \tilde{G}_n \) that respects the \( \Gamma \) action on \( \tilde{G}_n \), so \( \varphi' \) extends to an automorphism of \( \tilde{G}_n \times \Gamma \) sending \( \gamma \mapsto \gamma \). It’s only left to show that \( \varphi' \in \text{Aut}(\tilde{G}_n \times \Gamma, \pi_n; \rho) \). Indeed, \( \varphi' \) preserves \( \ker \pi_n \) because all of \( \tau, \sigma \) and \( \varphi \) preserve \( \ker \pi_n \); and \( \varphi' \) mapping \( \xi_n \) to \( \xi'_n \) follows by applying the following claim to \( \kappa := \tau \circ \sigma \) and by the fact that \( \varphi(\xi_n) = \xi'_n \).

**Claim:** Suppose that \( \kappa \) is an automorphism of \( \tilde{G}_n \) that preserves \( \ker \pi_n \) and induces the trivial automorphism on \( \tilde{G}_n^{ab} \). Then \( \kappa(\xi_n) = \xi_n \).

We use the usual presentation \( G_n = \langle x_1, \ldots, x_{2n} \mid [x_1, x_2], \ldots, [x_{2n-1}, x_{2n}] \rangle \), and consider the short exact sequence defined by this presentation

\[
1 \longrightarrow R \longrightarrow F_{2n} \longrightarrow G_n \longrightarrow 1,
\]

where \( F_{2n} \) is the free pro-\( \ell \) group on \( x_1, \ldots, x_{2n} \) and \( R \) is the closed normal subgroup generated by \( \lambda := [x_1, x_2], \ldots, [x_{2n-1}, x_{2n}] \). Then it gives the map \( \pi_n \) via

\[
1 \longrightarrow R/[R, F_{2n}] \longrightarrow F_{2n}/[R, F_{2n}] \simeq \tilde{G}_n \xrightarrow{\pi_n} G_n \longrightarrow 1. \tag{5.5}
\]

The automorphism \( \kappa \) of \( \tilde{G}_n \) lifts to an automorphism \( \tilde{\kappa} \) of \( F_{2n} \). Since \( \tilde{G}_n^{ab} = G_n^{ab} = F_{2n}^{ab} \), \( \tilde{\kappa} \) induces the trivial automorphism on \( F_{2n}^{ab} \). So the element \( y_i := x_i^{-1}\tilde{\kappa}(x_i) \) is contained in \( F_{2n}^{(2)} \) for each \( i \). Then \( \tilde{\kappa}(\lambda) = [x_1 y_1, x_2 y_2], \ldots, [x_{2n-1} y_{2n-1}, x_{2n} y_{2n}] \equiv [x_1, x_2], \ldots, [x_{2n-1}, x_{2n}] \mod F_{2n}^{(3)} \). As \( R \subset F_{2n}^{(2)} \), we have that \( [R, F_{2n}] \subset F_{2n}^{(3)} \), and then the quotient map \( R/[R, F_{2n}] \rightarrow R/(R \cap F_{2n}^{(3)}) \) is an isomorphism since both of them are isomorphic to \( \mathbb{Z}_\ell \). So \( \tilde{\kappa}(\lambda) \equiv \lambda \mod F_{2n}^{(3)} \) implies \( \kappa \) acts trivially on \( \ker \pi_n \), which proves the claim and hence proves the first equality in the theorem.

To prove the second equality, we consider the following expression of the moment that is similar to (5.4)

\[
\mathbb{E} \left( \# \{ \pi \in \text{Sur}_T(Y_{q,n}, H) \mid \pi_1 = \delta \} \right) = \sum_{\pi \in \text{Sur}(G_n \times \Gamma, \pi_n; \rho) \text{ s.t. } \pi(\xi_n) = h \text{ and } \pi|_{\tilde{G}_n} \text{ is } \Gamma\text{-equivariant}} \text{Prob}(\phi \in \text{Aut}(\tilde{G}_n \times \Gamma, \pi_n; \rho) \mid \ker(1 - \phi) \subseteq \ker \pi_1). \tag{5.6}
\]

By the Schur–Zassenhaus theorem, any two homomorphic splittings of \( H \times \Gamma \rightarrow \Gamma \) are conjugate by an element of \( H \), and therefore, the conjugation gives an automorphism of \( H \times \Gamma \) that maps one splitting to the other. Also, because the conjugations of \( H \times \Gamma \) acts transitively on the set of all splittings, the number of splittings is exactly \( [H : H^\Gamma] \). So we have

\[
\# \{ \pi \in \text{Sur}(G_n \times \Gamma, H \times \Gamma) \mid \pi(\xi_n) = h \} = [H : H^\Gamma] \# \{ \pi \in \text{Sur}(G_n \times \Gamma, H \times \Gamma) \mid \pi(\xi_n) = h \text{ and } \pi|_{\tilde{G}_n} \text{ is } \Gamma\text{-equivariant} \}.
\]

Thus, the second equality in the theorem follows by the first equality, (5.4) and (5.6). \( \square \)

### 5.3 Proof of Lemma 5.5.

Let \( F_{2n} \) denote the free pro-\( \ell \) group on \( 2n \) generators \( x_1, \ldots, x_{2n} \). Then there is a presentation of \( G_n \)

\[
1 \longrightarrow R \longrightarrow F_{2n} \xrightarrow{\pi} G_n \longrightarrow 1, \tag{5.7}
\]

and it induces a Schur covering of \( G_n \)

\[
1 \longrightarrow R/[R, F_{2n}] \longrightarrow F_{2n}/[R, F_{2n}] \longrightarrow G_n \longrightarrow 1. \tag{5.8}
\]

It follows by [Kar93, Chap.11, Thm.2.3(iii) and (iv)(b)] that \( F_{2n}/[R, F_{2n}] \) can be identified with \( \tilde{G}_n \). We denote the composition of the quotient map \( \pi \) in (5.7) and \( \rho \) by \( \kappa : F_{2n} \rightarrow H \), and denote \( N := \ker \kappa \). For each \( i = 1, \ldots, 2n \), we denote \( h_i := \kappa(x_i) \) and we pick an element \( h_i^* \in \pi^{-1}(h_i) \). Then the map \( \tilde{\kappa} : F_{2n} \rightarrow H \) defined by \( x_i \mapsto h_i^* \) is a homomorphism since \( F_{2n} \) is free, and moreover it is surjective by Lemma 2.5. By [Kar93, Chap.11, Thm.2.3(iv)(b)], \( \ker \tilde{\kappa} \) contains \( [N, F_{2n}] \), so
Lemma 5.7. Then the map sending \( \rho \) induces a surjection \( \tilde{\rho} : \tilde{G}_n \to \tilde{H} \) such that \( \varpi \circ \tilde{\rho} = \rho \circ \pi_n \), which proves the existence of \( \tilde{\rho} \) in the statement (1).

\[
\begin{array}{ccc}
F_{2n} & \xrightarrow{\pi} & G_n \\
& \searrow^{\pi_n} \downarrow{} & \nearrow_{\phi} \nwarrow^{\rho} \\
\tilde{G}_n & \xrightarrow{\tilde{\rho}} & \tilde{H}
\end{array}
\]

Without loss of generality, we assume \( \xi_n \) is the image of \([x_1, x_2] \cdots [x_{2n-1}, x_{2n}]\) in \( \tilde{G}_n \). Then for any \( \tilde{\rho} \) satisfying the desired requirements, we have that \( \tilde{\rho} \) maps the image of \( x_i \) to \( h_i \delta_i \) for some \( \delta_i \in \ker \varpi \). However, \( \ker \varpi \) is in the center of \( \tilde{H} \), so \([h_1, h_2] \cdots [h_{2n-1}, h_{2n}] = [h_1 \delta_1, h_2 \delta_2] \cdots [h_{2n-1} \delta_{2n-1}, h_{2n} \delta_{2n}] \). Thus, \( \tilde{\rho}(\xi_n) \) does not depend on the choice of \( \rho \), which finishes the proof of (1).

Let \( \rho_i \) and \( \tilde{\rho}_i \), \( i = 1, 2 \), be as defined in the statement (2). We use the surjections from \( F_{2n} \) to \( G_n \) and \( \tilde{G}_n \) defined in (5.7) and (5.8). Taking compositions with \( \rho_i \) and \( \tilde{\rho}_i \), we obtain surjections \( \kappa_i : F_{2n} \to H \) and \( \tilde{\kappa}_i : F_{2n} \to \tilde{H} \) such that \( \varpi \circ \tilde{\kappa}_i = \kappa_i \) for each \( i \). For an ordered 2n-tuple \( z = (z_1, \ldots, z_{2n}) \in F_{2n}^n \), we denote \( \lambda(z) := [z_1, z_2] \cdots [z_{2n-1}, z_{2n}] \). We write \( x \) for the tuple of generators \( (x_1, \ldots, x_{2n}) \). We will prove the statement (2) in the lemma by proving the following claim.

Claim: There exists \( \theta \in \text{Aut}(F_{2n}) \) such that \( \kappa_1 = \kappa_2 \circ \theta \) and \( \lambda(\theta(x)) = \lambda(x)^q \). Here \( \theta(x) \) denotes the tuple \( (\theta(x_1), \ldots, \theta(x_{2n})) \).

We now explain how the claim implies the statement (2). In the presentation (5.7) of \( G_n \), the kernel \( R \) is the closed normal subgroup generated by \( \lambda(x) \). So if \( \lambda(\theta(x)) = \lambda(x)^q \), then \( R \) is also generated by \( \lambda(\theta(x)) \) as \( q \in \mathbb{Z}_\ell^\times \). It follows that \( \theta(R) = R \), and hence \( \theta \) induces \( \varphi \in \text{Aut}(G_n) \), and also \( \bar{\varphi} \in \text{Aut}(\tilde{G}_n) \) by the description of \( \tilde{G}_n \) in (5.8). The automorphisms \( \varphi \) and \( \bar{\varphi} \) satisfy the condition (2a) because \( \kappa_1 = \kappa_2 \circ \theta \) and \( \kappa_i \) factors through \( \tilde{\rho}_i \) and \( \rho_i \) for each \( i = 1, 2 \). And the condition (2b) is satisfied, because \( \xi_n \) is assumed to be the image of \( \lambda(x) \) and then \( \bar{\varphi}(\xi_n) \) is the image of \( \lambda(\theta(x)) \).

In the remainder of the proof, we will prove the claim by induction on the lower \( \ell \)-central series \( \{F_{2n}^{(j)}\} \) of \( F_{2n} \), which is defined as

\[
F_{2n}^{(1)} = F_{2n} \quad \text{and} \quad F_{2n}^{(n+1)} := [F_{2n}, F_{2n}^{(n)}](F_{2n}^{(n)})^\ell.
\]

Explicitly, we will show the following.

(*) For each \( j \in \mathbb{Z}_{\geq 1} \), there exists a tuple \( y^{(j)} = (y_1^{(j)}, \ldots, y_{2n}^{(j)}) \) formed by a set of generators \( \{y_i^{(j)}\}_{i=1}^{2n} \) of \( F_{2n} \) such that \( \lambda(y^{(j)}) \equiv \lambda(x)^q \mod F_{2n}^{(j+1)} \) and \( \kappa_1(x_i) = \kappa_2(y_i^{(j)}) \) for each \( i = 1, \ldots, 2n \). Moreover, \( y_i^{(j+1)} \equiv y_i^{(j)} \mod F_{2n}^{(j)} \).

Then the map sending \( x_i \) to the inverse limit of \( \{y_i^{(j)} \mod F_{2n}^{(j)}\} \) as \( j \to \infty \) defines an automorphism \( \theta \) satisfying all conditions in the claim.

Lemma 5.7. For \( j = 2 \), the tuple \( y^{(2)} \) as in (*) exists.

Proof. Note that \( F_{2n}/F_{2n}^{(2)} \) is the Frattini quotient of \( F_{2n} \), so it is the dual of \( H^1(F_{2n}, \mathbb{F}_\ell) \). The element \( \lambda(x) \) defines a symplectic pairing on \( H^1(F_{2n}, \mathbb{F}_\ell) \)

\[
(-, -) : H^1(F_{2n}, \mathbb{F}_\ell) \times H^1(F_{2n}, \mathbb{F}_\ell) \xrightarrow{\cup} H^2(G_n, \mathbb{F}_\ell) \xrightarrow{\text{tr}_\lambda(x)} \mathbb{F}_\ell,
\]

40
where \( \text{tr}_\lambda(x) \) is the trace map induced by \( \lambda(x) \). For each \( r = 1, 2 \), the surjection \( \kappa_r \) induces inflation map \( \kappa_r^*: H^1(H, \mathbb{F}_\ell) \inj H^1(F_{2n}, \mathbb{F}_\ell) \), and then we obtain a bilinear and alternating pairing on \( H^1(H, \mathbb{F}_\ell) \). By the assumption that \( \tilde{\kappa}_1(\lambda(x)) = \tilde{\kappa}_2(\lambda(x)) \) has order dividing \( q - 1 \) and the argument similar to Proposition 3.6, the two pairings defined by \( \kappa_1^* \) and \( \kappa_2^* \) are the same and \((\alpha, \alpha') = q(\alpha, \alpha') \) for any \( \alpha, \alpha' \in H^1(H, \mathbb{F}_\ell) \). So we can choose a basis \( e_1, \ldots, e_{n\cdot\ell}, f_1, \ldots, f_a \) of \( H^1(H, \mathbb{F}_\ell) \) for some \( a, b \geq 0 \), such that \((e_i, e_j) = (f_i, f_j) = 0 \) for all \( i, j \) and \((e_i, f_j) = 1 \) if \( i = j \) and 0 otherwise.

Consider the fiber product \( P := H \times_{H/H(2)} F_{2n}/F_{2n}^{(2)} \) defined by the natural surjection \( H \rightarrow H/H(2) \) and \( F_{2n}/F_{2n}^{(2)} \). For each \( i = 1, \ldots, 2n \), we let \( z_i \) denote the element in \( P \) whose first coordinate is \( \kappa_1(x_i) \) and the second coordinate is the preimage under \( \beta^\vee \) of the image of \( x_i \) in \( F_{2n}/F_{2n}^{(2)} \) (these two coordinates have the same image in \( H/H(2) \) because of the diagram above, so \( z_i \) is a well-defined element in \( P \)). Since \( \kappa_2 \) factors through a surjection \( \kappa^\Delta_2 : F_{2n} \rightarrow P \) obtained by quotienting \( F_{2n} \) by \( \ker \kappa_2 \cap F_{2n}^{(2)} \), by [Lub01, Lem.2.1], there exist elements \( y_1, \ldots, y_{2n} \) in \( F_{2n} \) that generate \( F_{2n} \) and \( \kappa^\Delta_2(y_i) = z_i \). It follows that \( \kappa_1(x_i) = \kappa_2(y_i) \) and \( \beta^\vee \) sends the image of \( y_i \) to the image of \( x_i \). Moreover, letting \( \chi_i \) and \( \chi'_i \) denote the dual of \( x_i \) and \( y_i \), respectively in \( H^1(F_{2n}, \mathbb{F}_\ell) \), we have \( \beta(\chi_i) = \chi'_i \), and hence \( (\chi_i, \chi_j) = q(\chi'_i, \chi'_j) \). Therefore, by [NSW08, Prop.3.9.13][ii)], we have \( \lambda(x)^q = \prod_{i=1}^{2n} y_i \mod F_{2n}^{(3)} \), so the tuple \( y^{(2)} := (y_1, \ldots, y_{2n}) \) satisfies (*) for \( j = 2 \).

**Lemma 5.8.** Suppose that there exists \( y^{(j)} \) in (*) for some \( j > 1 \). Then \( y^{(j+1)} \) exists.

**Proof.** We will prove that there exist \( t_1, \ldots, t_{2n} \in F_{2n}^{(j)} \cap \ker \kappa_2 \) such that the tuple \( y^{(j+1)} \) obtained by setting \( y_i^{(j+1)} = \lambda(x)^q \mod F_{2n}^{(j+2)} \) and \( \kappa_1(x_i) = \kappa_2(y_i^{(j+1)}) \) as \( t_i \in F_{2n}^{(j)} \cap \ker \kappa_2 \). So it suffices to consider the requirement \( \lambda(y^{(j+1)}) = \lambda(x)^q \mod F_{2n}^{(j+2)} \). Let’s denote \( D := \lambda(x)^q \lambda(y^{(j)}) \). Since \( \lambda(x) \) and \( \lambda(y^{(j)}) \) are both contained in \([F_{2n}, F_{2n}]\), we have \( D \in F_{2n}^{(j+1)} \cap [F_{2n}, F_{2n}] \). Also, assuming that \( \xi_n \) is the image of \( \lambda(x) \), we have

\[
\tilde{\kappa}_2(\lambda(x)^q) = \tilde{\rho}_2(\xi_n)^q = \tilde{\rho}_1(\xi_n) = \tilde{\kappa}_2(\lambda(y^{(j)})),
\]

where the first and the third equalities follow by definition of \( \tilde{\kappa}_1 \) and \( \tilde{\kappa}_2 \), the second one follows by the assumption in the proposition that \( \tilde{\rho}_1(\xi_n) = \tilde{\rho}_2(\xi_n) \) has order dividing \( q - 1 \), and the last one is because of the statement (1) in the proposition and the induction hypothesis \( \kappa_1(x_i) = \kappa_2(y_i^{(j)}) \).

So we have that \( D \) is contained in \( F_{2n}^{(j+1)} \cap [F_{2n}, F_{2n}] \cap \ker \tilde{\kappa}_2 \).
The lower $\ell$-central series $\{F_{2n}^{(j)}\}$ induces a Lie algebra $\gr(F_{2n}) := \sum_i \gr_i(F_{2n})$ over $\mathbb{F}_\ell$, where $\gr_i(F_{2n}) := F_{2n}^{(j)}/F_{2n}^{(j+1)}$ and the Lie bracket for homogenous elements of $\gr(F_{2n})$ is induced by the commutator: if $a = \bar{x} \in \gr_r(F_{2n})$ and $b = \bar{y} \in \gr_s(F_{2n})$, then $[a, b]$ is the image of the commutator $\{x, y\}$ in $\gr_{r+s}(F_{2n})$. So

$$\lambda(y^{(j+1)}) = [y_1^{(j+1)}, y_2^{(j+1)}] \cdots [y_{2n-1}^{(j+1)}, y_{2n}^{(j+1)}]$$

$$= [y_1^{(j)} t_1, y_2^{(j)} t_2] \cdots [y_{2n-1}^{(j)} t_{2n-1}, y_{2n}^{(j)} t_{2n}]$$

$$\equiv \lambda(y^{(j)})[t_1, y_2^{(j)}][y_1^{(j)}, t_2] \cdots [t_{2n-1}, y_{2n}^{(j)}][y_{2n-1}^{(j)}, t_{2n}] \mod F_{2n}^{(j+2)}.$$

We write the group action of $\gr_i(F_{2n})$ additively, and define

$$d_j(t_1, \ldots, t_{2n}) := [\tau_1, \sigma_2] + [\tau_2, \sigma_1] + \cdots + [\tau_{2n-1}, \sigma_{2n}] + [\tau_{2n}, \sigma_{2n-1}] \in \gr_{j+1}(F_{2n}),$$

where $\tau_i$ is the image of $t_i$ in $\gr_{j+1}(F_{2n})$ and $\sigma_i$ is the image of $y_i^{(j)}$ in $\gr_1(F_{2n})$.

Considering the short exact sequence $1 \rightarrow N \rightarrow F_{2n} \xrightarrow{\kappa_2} H \rightarrow 1$ defined by $\kappa_2$, by [Kar93, Chap.11, Thm.2.3(iii) and (iv)(b)], $[N, F_{2n}]$ is $[F_{2n}, F_{2n}] \cap \ker \kappa_2$. So, the image of $F_{2n}^{(j+1)} \cap [F_{2n}, F_{2n}] \cap \ker \kappa_2 = F_{2n}^{(j+1)} \cap [N, F_{2n}]$ in $\gr_{j+1}(F_{2n})$ is generated by $[a, b]$ for some $a \in \gr_r(F_{2n})$ and $b \in \gr_{j+1-r}(F_{2n})$ such that $a$ is the image of some element of $N$. If $b = c^\ell$ for some $c \in \gr_{j-r}(F_{2n})$, then $[a, b] = [a^\ell, c]$ and $a^\ell$ is the image in $\gr_{j+1}(F_{2n})$ of some element of $N$. If $b = [c, d]$, then $[a, b] = [[d, a], c] + [[a, c], d]$ and each of $[d, a]$ and $[a, c]$ is the image of some element of $N$ and of degree strictly larger than $r$. It follows that the image of $F_{2n}^{(j+1)} \cap [N, F_{2n}]$ in $\gr_{j+1}(F_{2n})$ is generated by $[a, b]$ where $a \in \gr_{j+1}(F_{2n})$, $b \in \gr_1(F_{2n})$, and $a$ is the image of some element of $N$. Because $y_1^{(j)}, \ldots, y_{2n}^{(j)}$ form a generating set of $F_{2n}$, we have that $\sigma_1, \ldots, \sigma_{2n}$ generate $\gr_1(F_{2n})$, and hence the argument above shows that there exist $t_1, \ldots, t_{2n} \in F_{2n}^{(j)} \cap \ker \kappa_2$ such that $d_j(t_1, \ldots, t_{2n})$ equals the image of $D$ in $\gr_{j+1}(F_{2n})$. Then for such a choice of $t_1, \ldots, t_{2n}$, we have the tuple $y^{(j+1)}$ satisfying $\lambda(y^{(j+1)}) \equiv \lambda(x)^q$, and hence we finish the proof.

6. Conjectures and Evidences

In §6.1, we give the statements of all of the conjectures made in this paper, which include the moment conjectures in both the function field case and the number field case, and also the conjectures regarding the existence and uniqueness of the probability measure with desired moments. Then in §6.2 and §6.3, we discuss the presentation of $G_0(K)$ and positively ramifications, and how they support the moment conjecture in the number field case.

6.1. Statements of the conjectures. We first recall the notion of pro-$\mathcal{C}$ completion of a $\Gamma$-group defined in [LWZB19]. Let $\mathcal{C}$ be a set of isomorphism classes of finite $\Gamma$-groups, and define $\overline{\mathcal{C}}$ to be the smallest set of isomorphism classes of $\Gamma$-groups containing $\mathcal{C}$ that is closed under taking finite direct product, $\Gamma$-quotient and $\Gamma$-subgroup. Then for a given profinite $\Gamma$-group $G$, the pro-$\mathcal{C}$ completion of $G$ is defined to be

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

where the inverse limit runs over all closed normal $\Gamma$-subgroup $M$ of $G$ such that $G/M \in \overline{\mathcal{C}}$. We say that a group $G$ is pro-$\mathcal{C}$ if $G = G^{\mathcal{C}}$.

Let $q$ be a positive integer such that $\gcd(q, |\Gamma|) = 1$. We consider pairs $(H, h)$ for a profinite admissible $q'$-$\Gamma$-group $H$ and an element $h \in H_2(H \rtimes \Gamma, \mathbb{Z})/(|\Gamma|) \cdot [q - 1]$. We say that two such pairs $(G, g)$ and $(H, h)$ are isomorphic if there exists an $\Gamma$-equivariant isomorphism $G \simeq H$ such that its induced coinflation map $H_2(G \rtimes \Gamma, \mathbb{Z})/(|\Gamma|) \cdot [q - 1] \rightarrow H_2(H \rtimes \Gamma, \mathbb{Z})/(|\Gamma|)$ sends $g \mapsto h$. We define a
topological space $\mathcal{P}_{\Gamma,q}$, whose underlying space is the set of isomorphism classes of pairs $(H,h)$ as described above and basic opens are the sets

$$ U_{C,H,h} := \left\{ (G,g) \in \mathcal{P}_{\Gamma,q} \mid \begin{array}{l} \text{there is a } \Gamma\text{-equivariant surjection } e : G \to H \text{ s.t.} \\ e \text{ induces an isom. } G^C \simeq H \text{ and the coinj map sending } g \mapsto h \end{array} \right\}, $$

for each finite set $C$ of finite $(q|\Gamma)|'-\Gamma$-groups and each pair $(H,h) \in \mathcal{P}_{\Gamma,q}$ such that $H$ is finite pro-$C$. For a measure $\mu$ on $\mathcal{P}_{\Gamma,q}$, we use the following notation to denote the average number of surjections to a pair $(H,h)$

$$ E_\mu \# \operatorname{Sur}_\Gamma(*,(H,h)) := \sum_{(G,g) \in \mathcal{P}_{\Gamma,q}} \# \left\{ \pi \in \operatorname{Sur}_\Gamma(G,H) \mid \begin{array}{l} \text{the coinj map induced by } \pi \text{ sends } g \mapsto h \end{array} \right\} \mu(G,g). $$

**Conjecture 6.1** (Existence and uniqueness of the limit probability measure with the desired moments). For a finite group $\Gamma$ and a positive integer $q$ satisfying $\gcd(q,|\Gamma|) = 1$, there exists a unique probability measure $\mu_{\Gamma,q}$ on the topological space $\mathcal{P}_{\Gamma,q}$, such that for each $(H,h) \in \mathcal{P}_{\Gamma,q}$, the following equality holds

$$ E_{\mu_{\Gamma,q}} \# \operatorname{Sur}_\Gamma(*,(H,h)) = \frac{1}{|H : H|}. $$

When $\Gamma = \mathbb{Z}/2\mathbb{Z}$, we’ve discussed in Section 5 that there is a random pro-$\ell$ group model $Y_{q,n}$ giving the desired moments. Next, we define a coarser topological space $\mathcal{P}_{\Gamma,q,\ell}$ on which our pro-$\ell$ version of the probability measure is defined, and then we conjecture that the limit of the random group model $Y_{q,n}$ as $n \to \infty$ gives the desired probability measure.

**Definition 6.2** (Definition of measures $\nu_{q,n,\ell}$ on pro-$\ell$ $\mathbb{Z}/2\mathbb{Z}$-groups). Let $\Gamma = \mathbb{Z}/2\mathbb{Z}$ and $\ell$ an odd prime. We define a coarser topology $\mathcal{P}_{\Gamma,q,\ell}$ on the underlying space of $\mathcal{P}_{\Gamma,q}$, where the basic opens are all $U_{C,H,h}$ with an additional condition that $H$ is an $\ell$-group. For fixed $q,n$ satisfying $\gcd(2\ell,q) = 1$, we use the notation in Theorem 5.6, fix a generator $\xi_n$ of $H_2(\mathbb{G}_n, \mathbb{Z})(\ell)$, and define a probability measure $\nu_{q,\ell,n}$ on the space $\mathcal{P}_{\Gamma,q,\ell}$ by

$$ \nu_{q,\ell,n}(U_{C,H,h}) := \operatorname{Prob} \left( \begin{array}{l} \text{there exists } \pi \in \operatorname{Sur}_\Gamma(Y_{q,n},H) \text{ s.t.} \\ \pi \text{ induces an isom. } Y_{q,n}^C \simeq H \text{ and } \pi_1(\xi_n) = h \end{array} \right), $$

for each finite set $C$ of $\ell$-$\Gamma$-groups and pair $(H,h) \in \mathcal{P}_{\Gamma,q,\ell}$ such that $H$ is finite pro-$C$.

**Conjecture 6.3.** When $\Gamma = \mathbb{Z}/2\mathbb{Z}$, on the topological space $\mathcal{P}_{\Gamma,q,\ell}$, the probability measures $\nu_{q,\ell,n}$ have weak convergence to the measure $\mu_{\Gamma,q}$ in Conjecture 6.1, as $n \to \infty$.

Next, we give the probability and moment conjecture in the function field case.

**Conjecture 6.4** (Function field case). Let $\Gamma$ be a finite group and $q$ a prime power such that $\gcd(q,|\Gamma|) = 1$. Let $C$ be a finite set of finite $(q|\Gamma)|'-\Gamma$-groups, and $(H,h)$ a pair in $\mathcal{P}_{\Gamma,q}$ such that $H$ is finite pro-$C$. Fix a generator $\zeta$ of $\hat{\mathbb{Z}}(1)_{(q|\Gamma)|'}$, and we let $\delta$ denote the homomorphism $\hat{\mathbb{Z}}(1)_{(q|\Gamma)|'} \to H_2(\mathbb{G} \times \Gamma, \mathbb{Z}_{(\ell)})$ sending $\zeta \mapsto h$. Then

$$ \lim_{N \to \infty} \frac{1}{N} \sum_{n \leq N} \left\{ K \in \mathcal{E}_\Gamma(q^n, F_q(t)) \mid \begin{array}{l} \text{there exists } K \in \operatorname{Sur}_\Gamma(G^\#_\mathcal{O}(K),H) \text{ s.t.} \\ K \text{ induces an isom. } G^\#_\mathcal{O}(K)^C \simeq H \text{ and } \pi_* \circ \omega_K = \delta \end{array} \right\} = \mu_{\Gamma,q}(U_{C,H,h}). $$
and
\[ \lim_{N \to \infty} \frac{\sum_{n \leq N} \sum_{K \in E_{\Gamma}(q^n, \mathbb{F}_q(t))} \# \left\{ \pi \in \text{Sur}_{\Gamma} \left( G_{\mathbb{O}}^\#(K), H \right) \mid \pi \circ \omega_K^\# = \delta \right\} }{\sum_{n \leq N} \# E_{\Gamma}(q^n, \mathbb{F}_q(t))} = \frac{1}{[H : H^\Gamma]}. \]

To give the moment conjecture in the number field case, we need to first study how the action of taking quotient modulo \( u \) random elements changes the moments. This idea comes from [LST20], and Lemma 6.6 below is the analogue of [LST20, Lem.8.12] for our notion of the probability space.

**Definition 6.5.** Let \( \mu \) be a measure on \( \mathcal{P}_{\Gamma,q} \). For a positive integer \( t \), define the measure \( Q^t \mu \) on \( \mathcal{P}_{\Gamma,q} \) as obtained by taking the \( \Gamma \)-equivariant quotient of the random pair \( (H, h) \in \mathcal{P}_{\Gamma,q} \) according to \( \mu \) modulo \( t \) random elements. That is, for any \( (H, h) \), define
\[ Q^t \mu (H, h) := \sum_{(G, g) \in \mathcal{P}_{\Gamma,q}} \text{Prob} (G/[x_1, \ldots, x_t] \simeq H \text{ such that } g \mapsto h) \mu (G, g), \]
where \( x_1, \ldots, x_t \) are \( t \) random elements of \( G \) with respect to Haar measure, and the notation \([x_1, \ldots, x_t]\) represents the closed normal \( \Gamma \)-subgroup of \( G \) generated by \( x_1, \ldots, x_t \).

**Lemma 6.6.** Let \( \mu \) be a measure on \( \mathcal{P}_{\Gamma,q} \). Then for any \( (H, h) \in \mathcal{P}_{\Gamma,q} \), we have
\[ \mathbb{E}_{Q^t \mu} \# \text{Sur}_{\Gamma}(\ast, (H, h)) = \mathbb{E}_{\mu} \# \text{Sur}_{\Gamma}(\ast, (H, h)) / |H|^t. \]

**Proof.** It suffices to prove the lemma for \( t = 1 \). For two pairs \( (G_1, g_1), (G_2, g_2) \in \mathcal{P}_{\Gamma,q} \), we write \( \pi : (G_1, g_1) \to (G_2, g_2) \) if \( \pi \) is a \( \Gamma \)-equivariant group homomorphism \( G_1 \to G_2 \) whose induced coinflation maps \( g_1 \) to \( g_2 \), and we write \( \text{Sur}_{\Gamma}((G_1, g_1), (G_2, g_2)) \) for the set of surjections \( (G_1, g_1) \to (G_2, g_2) \). Then we have
\[
\begin{align*}
\mathbb{E}_{Q^t \mu} \# \text{Sur}_{\Gamma}(\ast, (H, h)) &= \sum_{(G, g) \in \mathcal{P}_{\Gamma,q}} \# \text{Sur}_{\Gamma}((G, g), (H, h)) \cdot Q^t \mu (G, g) \\
&= \sum_{(G, g) \in \mathcal{P}_{\Gamma,q}} \sum_{(E, e) \in \mathcal{P}_{\Gamma, q}} \# \text{Sur}_{\Gamma}((G, g), (H, h)) \cdot \text{Prob} (E/[x] \simeq G \text{ s.t. } e \mapsto g) \cdot \mu (E, e) \\
&= \sum_{(E, e) \in \mathcal{P}_{\Gamma,q}} \sum_{\pi \in \text{Sur}_{\Gamma}(E, e), (H, h))} \text{Prob} (\text{the random } x \in E \text{ is contained in } \ker \pi) \cdot \mu (E, e) \\
&= \sum_{(E, e) \in \mathcal{P}_{\Gamma,q}} \# \text{Sur}_{\Gamma}((E, e), (H, h)) \cdot \frac{1}{|H|} \cdot \mu (E, e) \\
&= \frac{\mathbb{E}_{\mu} \# \text{Sur}_{\Gamma}(\ast, (H, h))}{|H|}.
\end{align*}
\]

\( \square \)

**Conjecture 6.7** (Number field case). Let \( \Gamma \) be a finite group, \( Q \) a number field, and \( m \) the maximal integer such that the \( m \)-th roots of unity \( \mu_m \) is contained in \( Q \). Let \( G_{\mathbb{O}}^\#(K) := G_{\mathbb{O}}(K)(|\Gamma|G_{\mathbb{O}}(Q))' \), and \( H \) be a finite admissible \( \Gamma \)-group such that \( G_{\mathbb{O}}(Q) \) is pro-prime-to \( |H| \). Then, for any extension \( K/Q \),
\[ \lim_{B \to \infty} \frac{\sum_{D \leq B} \sum_{K \in E_{\Gamma}(D, Q)} \# \text{Sur}_{\Gamma}(G_{\mathbb{O}}^\#(K), H)}{\sum_{D \leq B} \# E_{\Gamma}(D, Q)} = \frac{\# H_2(H \times \Gamma, \mathbb{Z})(|\Gamma|)[m]}{|H : H^\Gamma| \cdot |H|^n}, \]
where \( u \) is the rank of the group of units in the ring \( \mathcal{O}_Q \) of algebraic integers of \( Q \).
Remark 6.8. (1) Although we will see in §6.3 that, for some number field $K$, we can define a lifting invariant that is analogous to the invariant $\omega^\#_K$ in the function field case, in general, we don’t know how to define such an invariant, so in Conjecture 6.7, we do not specify the “lifting invariant” and study only the distribution of $G^\#_0(K)$.

(2) We only make the conjecture in the moment version because in the number field case the characteristic is zero and then the distribution of $G^\#_0(K)$ is not a measure on $\mathcal{P}_{\Gamma,q}$ for any $q$. However, one can similarly define a topology on the set of pairs $(H,h)$ where $H$ is an admissible $\Gamma$-group and $h \in H_2(H \rtimes \Gamma, \mathbb{Z}[[\Gamma]]/[\Gamma])$, and conjecture that there exists a unique probability measure on this topological space that gives the desired moments.

6.2. Evidence I: Presentations of $G_\Omega(K)$. In this section, we fix a finite group $\Gamma$ and let $Q$ denote a global field that is either a number field or a function field.

We let $F_n(\Gamma)$ denote the free $|\Gamma|^\cdot\Gamma$-group on $n$ generators [LWZB19, §3.1], that is: $F_n(\Gamma)$ is the free pro-$|\Gamma|^\cdot\Gamma$ group on $\{x_{i,\gamma} \mid i = 1, \ldots, n \text{ and } \gamma \in \Gamma\}$ where $\sigma \in \Gamma$ acts on $F_n(\Gamma)$ by $\sigma(x_{i,\gamma}) = x_{i,\sigma\gamma}$.

Let $G$ be a finitely generated $|\Gamma|^\cdot\Gamma$-group. For a sufficiently large $n$, there exists a $\Gamma$-equivariant short exact sequence of $\Gamma$-groups

$$1 \rightarrow N \rightarrow F_n(\Gamma) \xrightarrow{\pi} G \rightarrow 1,$$

and we call such a short exact sequence a $\Gamma$-presentation of $G$. For a set $\mathcal{C}$ of isomorphism classes of $|\Gamma|^\cdot\Gamma$-groups, if $G$ is pro-$\mathcal{C}$, then the map $\pi$ factors through the pro-$\mathcal{C}$ completion map $F_n(\Gamma) \rightarrow F_n(\Gamma)^\mathcal{C}$. We call the induced short exact sequence

$$1 \rightarrow M \rightarrow F_n(\Gamma)^\mathcal{C} \xrightarrow{\pi^\mathcal{C}} G \rightarrow 1$$

a pro-$\mathcal{C}$ $\Gamma$-presentation of $G$.

For the rest of this section, we assume $\mathcal{C}$ is finite. For any $\Gamma$-extension $K$ of $Q$ that is split completely at $\infty$ or at all archimedean primes, by [Liu20, Thm.6.4], the pro-$\mathcal{C}$ completion of $G_\Omega(K)$ is finite, so $G^\#_\Omega(K)^\mathcal{C}$ is finite because $G^\#_\Omega(K)$ is a quotient of $G_\Omega(K)$ in both the number field case and the function field case. Then we can study a pro-$\mathcal{C}$ $\Gamma$-presentation

$$1 \rightarrow M \rightarrow F_n(\Gamma)^\mathcal{C} \xrightarrow{\pi^\mathcal{C}} G^\#_\Omega(K)^\mathcal{C} \rightarrow 1.$$  \hspace{1cm} (6.1)

The work [Liu20] studies the minimal number of elements that generates $M$ as a $\Gamma$-closed normal subgroup of $F_n(\Gamma)^\mathcal{C}$ in such a presentation, and gives an upper bound for this minimal number using Galois cohomology groups $H^i(G_\Omega(K), A)$ for $i = 1, 2$ and $A$ a finite simple $\text{Gal}(K_\Omega/Q)$-module. We will apply that result to number field case and function field case respectively, and show that the number field case needs $u$ more elements than the function field case to generate $M$, where $u$ is the rank of $O^\times_Q$ as defined in Conjecture 6.7.

We first recall the definition of multiplicities in [Liu20, Def.3.1]. Given a short exact sequence $1 \rightarrow N \rightarrow F \xrightarrow{\omega} H \rightarrow 1$ of $\Gamma$-groups, we let $N_0$ be the intersection of all maximal proper $F \rtimes \Gamma$-normal subgroups of $N$, and denote $\overline{N} = N/N_0$ and $\overline{F} = F/N_0$. Then $\overline{N}$ is a direct sum of finite irreducible $\overline{F} \rtimes \Gamma$-groups. For any finite irreducible $\overline{F} \rtimes \Gamma$-group $A$, we define the multiplicity $m(\omega, \Gamma, H, A)$ to be the multiplicity of $A$ appearing in $\overline{N}$.

Lemma 6.9. Let $Q$ be $\mathbb{F}_q(t)$ with $\gcd(q, |\Gamma|) = 1$ or a number field. Let $K$ be a $\Gamma$-extension of $Q$ such that each archimedean prime is unramified when $Q$ is a number field, and $\infty$ splits completely when $Q = \mathbb{F}_q(t)$. Let $\mathcal{C}$ be a finite set of $|\Gamma|^\cdot\Gamma$-groups when $Q = \mathbb{F}_q(t)$, and a finite set of $(|\Gamma||G_\Omega(Q)|)^\cdot\Gamma$-groups when $Q$ is a number field. Let $\ell$ be a prime such that $\ell \neq \text{char}(Q)$, $\ell \nmid |\Gamma|$, and $\ell \nmid |G_\Omega(Q)|$ when $Q$ is a number field. We consider a pro-$\mathcal{C}$ $\Gamma$-presentation (6.1) of $G^\#_\Omega(K)^\mathcal{C}$. 


Then for a finite simple $\mathbb{F}_\ell \bar{G}_0^\#(K)^C \rtimes \Gamma$-module $A$, we have

$$m(\pi^C, \Gamma, G^\#_0(K)^C, A) \leq \begin{cases} 
(n + 1) \dim_{\mathbb{F}_\ell} A - \xi(A) - 1_{\mathbb{F}_\ell}(A) & \text{if } Q \text{ is a function field} \\
(n + u + 1) \dim_{\mathbb{F}_\ell} A - \xi(A) - 1_{\mathbb{F}_\ell}(A) & \text{if } Q \text{ is a number field.}
\end{cases}$$

Here $\xi(A) := \dim_{\mathbb{F}_\ell} A^\Gamma / A^G_0(K)^C \rtimes \Gamma$; $1_{\mathbb{F}_\ell}(A)$ is 1 if $A = \mathbb{F}_\ell$ and $\mu_\ell \not\subset Q$, and 0 otherwise; and $u$ is the rank of $Q^\times_0$.

**Remark 6.10.** We take the pro-$C$ completions for a finite $C$ only because we want to work with a presentation with finitely many generators. If $G^\#_0(K)$ is finitely generated, then the pro-$C$ completions in the inequality can be removed. Also, we can take an ascending series of finite sets $\{C_i\}$ such that $\cup C_i$ contains all isomorphism classes of $|\Gamma|'$-$\Gamma$-groups, then $\lim_{\uparrow} G^\#_0(K)^C_i = G^\#_0(K)$. We will see in the discussion after the proof of this lemma that only the difference between the upper bounds in the number field case and the function field case is important, which does not depend on the choice of $C$.

**Proof.** We denote $G := G_0(K)$ and $G^\# := G_0^\#(K)$. By [Liu20, Prop.3.4 and Cor.5.3],

$$m(\pi^C, \Gamma, G^\#_0(K)^C, A) \leq \frac{n \dim_{\mathbb{F}_\ell} A - \xi(A) + \dim_{\mathbb{F}_\ell} H^2(G^\#, A)^\Gamma - \dim_{\mathbb{F}_\ell} H^1(G^\#, A)^\Gamma}{\dim_{\mathbb{F}_\ell} \text{Hom}_{(G^\#)^C \rtimes \Gamma}(A)} \quad (6.2)$$

where the $\Gamma$ actions on the cohomology groups are induced by the conjugation action of $\Gamma$ on $G^\#$.

We first prove the function field case. Note that $G^\#$ is the quotient of $G$ modulo the decomposition subgroup at $\infty$. So we can assume that $n$ is sufficiently large such that $\pi^C$ is the composition map $F_n(\Gamma)^C \xrightarrow{\pi^C} G^C \rightarrow (G^\#)^C$. Then we have a formula for $m(\pi^C, \Gamma, G^C, A)$ similar to (6.2).

Because $K/Q$ is split completely above $\infty$, the genus of $K$ is positive. By [Liu20, Prop.9.3(2)],

$$\dim_{\mathbb{F}_\ell} H^2(G, A)^\Gamma - \dim_{\mathbb{F}_\ell} H^1(G, A)^\Gamma = \dim_{\mathbb{F}_\ell} \text{Hom}_{\text{Gal}(K_0/Q)}(A, \mu_\ell) - \dim_{\mathbb{F}_\ell} A^{\text{Gal}(K_0/Q)}. \quad (6.3)$$

Here $A$ is a $(G^\#)^C \rtimes \Gamma$-module, and hence is a $\text{Gal}(K_0^\#/Q)$-module. Because $K_0^\# / Q$ is split completely over $\infty$, if $A = \mu_\ell$, then $\mu_\ell$ must be contained in $Q$, so $A$ is a trivial module and (6.3) is $1 - 1 = 0$. If $A = \mathbb{F}_\ell$, then (6.3) is $-1$ when $\mu_\ell \not\subset Q$ and is 0 otherwise. If $A$ is neither $\mathbb{F}_\ell$ nor $\mu_\ell$, then both terms in (6.3) are 0. So we have an upper bound: $m(\pi^C, \Gamma, G^C, A) \leq (n \dim A - \xi(A) - 1_{\mathbb{F}_\ell}(A)) \cdot (\dim \text{Hom}_{G^C \rtimes \Gamma}(A))^{-1}$. Recall that $G^\#$ is the $\Gamma$-equivariant quotient of $G$ modulo one element (a generator of the decomposition at $\infty$). By following the proof of [Liu20, Lem.10.6], we have $m(\pi^C, \Gamma, (G^\#)^C, A) = m(\pi^C, \Gamma, G^C, A) + \dim A \cdot (\dim \text{Hom}_{G^C \rtimes \Gamma}(A))^{-1}$, and hence we prove the lemma in the function field case.

When $Q$ is a number field, $G = G^\#$ because of the assumption that $C$ contains only groups whose order are prime to $|\Gamma||G_0(Q)|$. Let $T$ denote the set of all archimedean primes and all primes of $K$ above $\ell$. Let $S_{\infty}(Q)$ denote the set of all archimedean primes of $Q$. By [Liu20, Thm.7.1],

$$\log_\ell \chi_{K/Q,T}(A) := \sum_{i=0}^{2} (-1)^i \dim_{\mathbb{F}_\ell} H^i(G_T(K), A)^\Gamma$$

$$= \sum_{v \in S_{\infty}(Q)} \left( \dim_{\mathbb{F}_\ell} \hat{H}^0(Q_v, \text{Hom}(A, \mu_\ell)) - \dim_{\mathbb{F}_\ell} H^0(Q_v, \text{Hom}(A, \mu_\ell)) \right),$$

where $\hat{H}^0$ is the 0-th Tate cohomology of the group $G_{Q_v}$. We let $r_1$ and $r_2$ denote the number of real embeddings and complex embeddings of $Q$ respectively. If $v$ is imaginary, then $\dim H^0(Q_v, \text{Hom}(A, \mu_\ell)) = \dim_{\mathbb{F}_\ell} A^{\widehat{\text{Gal}(Q_v)}}.$
dim Hom\(A, \mu_\ell\) = dim A. When \(\ell\) is odd, \(G_{Q_v}\) is either trivial or \(Gal(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}\), so the Tate cohomology terms above are always 0 \([\text{NSW08}, \text{Prop.}(1.6.2)]\). Since \(K/Q\) is unramified at every archimedean prime, if \(v\) is real, then \(A\) as a \(G_{Q_v}\)-module is trivial but \(\mu_\ell\) is not trivial, so \(H^0(Q_v, \text{Hom}(A, \mu_\ell)) = \text{Hom}_{G_{Q_v}}(A, \mu_\ell) = 0\). When \(\ell = 2\), for each real place \(v\) of \(Q\), \(G_{Q_v}\) acts trivially on \(A\) and so on \(\text{Hom}(A, \mu_2)\). Since \(\text{Hom}(A, \mu_2)\) has exponent 2, its \(G_{Q_v}\)-norm map is zero, which implies that \(\tilde{H}^0(Q_v, \text{Hom}(A, \mu_2)) = H^0(Q_v, \text{Hom}(A, \mu_2))\). When \(\ell = 2\) and \(v\) is imaginary, \(G_{Q_v} = 1\), so the Tate cohomology term is trivial. Therefore, in every case, we have \(\log \chi_{K/Q,T}(A) = -r_2 \dim_{\ell^r} A\).

Then by \([\text{Liu20}, \text{Prop.9.4}]\),

\[
\dim_{\ell^r} H^2(G, A) = \dim_{\ell} H^1(G, A) \\
\leq -r_2 \dim_{\ell^r} A + \dim_{\ell^r} \text{Hom}_{Gal(K/Q)}(A, \mu_\ell) - \dim_{\ell^r} A^{Gal(K/Q)} + [K : Q] \dim_{\ell^r} A. \quad (6.4)
\]

Similarly to the function field case, if \(A = \mu_\ell\), then \(\mu_\ell \subset Q\) and \(\Delta := \dim \text{Hom}_{Gal(K/Q)}(A, \mu_\ell) - \dim A^{Gal(K/Q)} = 0\). If \(A\) is neither \(\mathbb{F}_\ell\) or \(\mu_\ell\), then \(\Delta = 0\). When \(A = \mathbb{F}_\ell\), \(\Delta = 0\) if \(\mu_\ell \subset Q\) and is \(-1\) when \(\mu_\ell \not\subset Q\). Finally, because \([K : Q] = r_1 + 2r_2\) and \(u = r_1 + r_2 - 1\), the lemma in the number field case follows by \((6.4)\).

The multiplicities computed in Lemma 6.9 are closely related to the minimal number of relators in the presentation \((6.1)\) (which is the minimal number of elements that generate \(M\) as a \(\Gamma\)-closed normal subgroup of \(F_n(\Gamma)^C\)). Let \(R\) and \(F\) be the quotients of \(M\) and \(F_n(\Gamma)^C\) respectively modulo the intersection of all maximal proper \(F_n(\Gamma)^C \rtimes \Gamma\)-normal subgroups of \(M\). Then

\[
R \simeq \bigoplus_A A^{m(\pi, C, \Gamma, G_{\hat{\Omega}}(K)^C, A)},
\]

where the direct sum runs over all finite simple \(F \rtimes \Gamma\)-groups \(A\). Then a set of elements generates \(M\) as a \(\Gamma\)-closed normal subgroup of \(F_n(\Gamma)^C\) if and only if the image of the set in \(R\) generates \(R\) as a \(\Gamma\)-closed normal subgroup of \(F\). By \([\text{LW20}, \text{Thm.5.1} \text{and} \text{Rmk.5.2}]\), for a non-abelian \(A\), the direct product of arbitrarily many copies of \(A\) can always be generated by 1 element; and for an abelian \(A\), the maximal \(m\) such that \(A^m\) can be generated by 1 element is \(\dim_{\ell^r} A \cdot (\dim_{\ell^r} \text{Hom}_{\hat{\Omega}}(A)^C, A)^{-1}\).

Thus, the upper bounds for the multiplicities given in Lemma 6.9 show that in the \(\pro C\) \(\Gamma\)-presentation \((6.1)\), the number field case needs \(u\) more relators than the function field case. If these \(u\) extra relators are random, then Conjecture 6.7 follows by Conjecture 6.4 and Lemma 6.6 (regardless of the “prime-to-\(q\)” condition in the function field case).

Of course, in Lemma 6.9, we give only upper bounds of the multiplicities, and if there exist better upper bounds, then one may wonder whether Conjecture 6.7 is still reasonable. \([\text{Liu20}]\) shows that the equality in Lemma 6.9 holds if and only if, in the number field case, \(H^2(G_{\hat{\Omega}}(K), A)\) and \(B_{\hat{\Omega}}(K, A)\) are in the same class of the Grothendieck group of \(\mathbb{F}_\ell[\text{Gal}(K/Q)]\)-modules (see the proof of \([\text{Liu20}, \text{Prop.9.4}]\)). Here \(B_{\hat{\Omega}}(K, A)\) is an abelian group defined in \([\text{Liu20}, \text{Def.8.1}]\). We don’t know to what extent this condition holds, so it’s unclear whether there are upper bounds that are generically better than the ones given in Lemma 6.9.

6.3. Evidence II: Positively ramified extensions of number fields. If Conjectures 6.4 and 6.7 are true, then one may expect that, for a number field \(K\), there exists some group associated to \(K\) such that: 1) it has group structure similar to the prime-to-char(\(k\)) part of the étale fundamental group of a smooth projective curve \(X\) over a finite field \(k\); and 2) \(G_{\hat{\Omega}}^\#(K)\) is a \(\Gamma\)-equivariant quotient of that group modulo \(u\) elements. In the function field case, for \(K\) satisfying Notation 2.1, we have seen that \(G_{\hat{\Omega}}^\#(K)\) is naturally a quotient of \(\pi_1^\#(\mathbb{X}) = G_{\hat{\Omega}}(K\bar{k})\). When we focus on the \(\pro \ell\) completions of Galois groups in the number field case, then the passage to the algebraic closure of constant field is analogous to taking the composition of \(K\) with the cyclotomic \(\mathbb{Z}_\ell\)-extension \(Q_\infty\) of
Q. However, the étale fundamental group $G_0(K)$ is too small to be an analogue of $\pi_1^{et}(X)$ because $Q_\infty$ is already ramified. Let $S$ be a set of primes of $K$ that contains all the archimedean primes and primes above $\ell$, and let $G_S(K)(\ell)$ denote the Galois group of the maximal pro-$\ell$ extension of $K$ that is unramified outside primes above $S$. It is well known that there exists a strong analogy between $G_S(K)(\ell)$ and $\pi_1^{et}(X - \{P_1, \ldots, P_m\})(\ell)$ when $\ell \neq \text{char}(k)$: both of them are Poincaré group at $\ell$ of dimension 2 and have the Poitou–Tate duality. Because the Riemann existence theorem shows that there is a natural surjection

$$\pi_1^{et}(X - \{P_1, \ldots, P_m\})(\ell) \twoheadrightarrow \pi_1^{et}(X)(\ell)$$

whose kernel is the free product of the inertia subgroups at $P_1, \ldots, P_m$. So if the analogue of $\pi_1^{et}(X)(\ell)$ exists, then it should be some group between $G_S(K)(\ell) \rightarrow G_Q(K)(\ell)$.

In the sequence of works by Wingberg and Schmidt [Win84, Win85, Sch95, Sch96], they introduced the notion of positively ramified extensions of number fields, and in some nice cases, they prove that there is a good analogy between the Galois group of the maximal positively ramified extension and $\pi_1^{et}(X)$. We briefly explain their ideas below. Let $\ell$ be an odd prime number, and $Q_\ell^{pre} := Q_\ell^{nr}(\zeta_\ell + \zeta_\ell^{-1})(odd)(\zeta_\ell)$, where $Q_\ell^{nr}$ is the maximal unramified extension of $Q_\ell$ and the notation $Q_\ell^{nr}(\zeta_\ell + \zeta_\ell^{-1})(odd)$ means the maximal pro-odd extension of $Q_\ell^{nr}(\zeta_\ell + \zeta_\ell^{-1})$. So $Q_\ell^{pre}$ is a $\mathbb{Z}/2\mathbb{Z}$-extension of $Q_\ell^{nr}(\zeta_\ell + \zeta_\ell^{-1})(odd)$, and we let $\rho$ denote the non-trivial element of its Galois group, which can be viewed as the $\ell$-adic version of the complex conjugation. A local field $k/Q_\ell$ is orientable if $k \subset Q_\ell^{pre}$ and if either $k = k^+ := k^{(\phi)}$ or $\zeta_\ell \in k^{nr}$. In other words, at each local place, Wingberg and Schmidt construct the structure that is similar to a CM-field. So the positively ramified extension is the analogue of the totally real field: a local extension $l/k$ is positively ramified (p.r.) if $l \subset Q_\ell^{pre}k$ (in $Q_2$ if $p = 2$) and the Galois closure of $l/k$ has at most pure wild ramification (i.e., the ramification index is a power of $\ell$). Then a number field extension $L/K$ is called positively ramified (p.r.) if its local completion is p.r. at each prime.

For an odd prime number $\ell$, a number field $K$ is called $\ell$-CM if, at every prime $p$ of $K$ lying above $\ell$, $K_p$ is orientable, $[K_p : K_p^+] = 2$ and $K_p$ contains an index-2 subfield $k$ such that $k = k^+$. We let $K_\text{pos}$ denote the maximal p.r. extension of $K$. Then by [Sch96, Thm.7.3], if $K$ is $\ell$-CM and contains $\mu_\ell$, then the followings hold (for analogous statements for $\pi_1^{et}(X)$, see [NSW08, Cor.(10.1.3)(i)(ii)]):

1. If $g_\ell(K) > 0$, then $\text{Gal}(K_{\text{pos}}/K)(\ell)$ is a Poincaré group of dimension 3 with dualizing module $\mu_\infty$.
2. If $g_\ell(K) = 0$, then $\text{Gal}(K_{\text{pos}}/K)(\ell)$ is a free pro-$\ell$ group.

Here $g_\ell(K)$ is the $\ell$-genus which can be computed by the rank of the positive ramified Picard group [Sch96, Prop.6.7]. Moreover, Schmidt [Sch96, Thm.8.3] proved the analogue of the Riemann existence theorem: kernel of $G_S(K)(\ell) \rightarrow \text{Gal}(K_{\text{pos}}/K)(\ell)$ is the free product of inertia subgroups.

Assume that $\ell$ is an odd prime number, $Q = \mathbb{Q}(\mu_\ell)$ such that $Q_0(\ell) = Q$ (equivalently, the $\ell$-part of the class group of $Q$ is trivial), and $\Gamma$ is a finite group with $\ell \nmid |\Gamma|$. Then $Q$ is $\ell$-CM. Assume that $K$ is a $\Gamma$-extension of $Q$ that is $\ell$-CM (for example, this holds when $K/Q$ is unramified at all primes lying above $\ell$). We let $K_\text{pos}(\ell)$ denote the maximal pro-$\ell$ p.r. extension of $K$. Then $KQ_\infty$ is a p.r. extension of $K$, and we have the following short exact sequence that is the analogue of (2.1)

$$1 \rightarrow \text{Gal}(K_{\text{pos}}(\ell)/KQ_\infty) \rightarrow \text{Gal}(K_{\text{pos}}(\ell)/K) \rightarrow \text{Gal}(KQ_\infty/K) \rightarrow 1,$$

where every term naturally has an action of $\Gamma$ (when we fix a splitting of $\text{Gal}(K_{\text{pos}}(\ell)/Q) \rightarrow \text{Gal}(K/Q)$). The Galois group $\text{Gal}(KQ_\infty/K) \simeq \mathbb{Z}_\ell$, which is a Poincaré group of dimension 1 with dualizing module $Q_\ell/\mathbb{Z}_\ell$. So by [NSW08, Thm.(3.7.4)], from the exact sequence above, we see that $\text{Gal}(K_{\text{pos}}(\ell)/KQ_\infty)$ is a pro-$\ell$ Poincaré group of dimension 2 with dualizing module $\mu_\infty$, and hence we have the analogue of Poincaré duality. Moreover, since $\mu_\infty \subset KQ_\infty$, by Kummer theory, the abelianization of $\text{Gal}(K_{\text{pos}}(\ell)/KQ_\infty)$ is free over $\mathbb{Z}_\ell$, so $\text{Gal}(K_{\text{pos}}(\ell)/KQ_\infty)$ is a pro-$\ell$ Demuškin
group in the form of \((x_1, \ldots, x_{2n} \mid [x_1, x_2] \cdots [x_{2n-1}, x_{2n}])\). So one can repeat the argument in the proof of Lemma 2.2 to show that there is a \(\text{Gal}(Q_\infty/Q)\)-equivariant isomorphism

\[
H_2(\text{Gal}(K_{\text{pos}}(\ell)/Q_\infty), \mathbb{Z})(\ell) \simeq \mathbb{Z}_\ell(1).
\] (6.6)

We let \(v\) denote the unique prime of \(Q\) lying above \(\ell\), let \(p\) be a prime of \(K\) lying above \(v\), and pick a prime \(\mathfrak{p}\) of \(K_{\text{pos}}(\ell)\) above \(p\). By [NSW08, Thm.(7.4.4)] and the assumption \(\ell \nmid |\Gamma|\), the group of principal units of \(K_p\) is isomorphic to

\[
U_{K_p}^1 \simeq \mathbb{Z}_\ell[\text{Gal}(K_{p}/Q_v)]^\ell-1
\]
as \(\text{Gal}(K_p/Q_v)\)-modules. Let \(a\) denote a generator of \(\text{Gal}(K_{Q_\infty}/K)\). The extension \(K_{Q_\infty}/K\) is completely wildly ramified at \(p\). Then by local class field theory, we can pick an element \(a_p\) of the inertia subgroup \(\text{Gal}(K_{\text{pos}}(\ell)/K)\) at \(\mathfrak{p}\), such that it maps to \(a\) under the quotient map in (6.5) and the \(\text{Gal}(K_p/Q_v)\)-closed subgroup of the abelianization of \(\text{Gal}(K_{\text{pos}}(\ell)\mathfrak{p}/K_p)\) generated by the image of \(a_p\) is isomorphic to \(\mathbb{Z}_\ell[\text{Gal}(K_p/Q_v)]\). Then for other prime \(p'\) of \(K\) above \(v\), we choose an element \(\gamma \in \text{Gal}(K/Q)\) such that \(\gamma(p) = p'\), and define \(a_{p'}\) to be \(\gamma(a_p)\). We define \(G_{\text{pos}}^\#(K)\) to be the quotient of \(\text{Gal}(K_{\text{pos}}(\ell)/K_{Q_\infty})\) modulo the \(\Gamma\)-closed normal subgroup generated by these elements \(a_p\)'s for all \(p \mid v\), and we denote the field extension corresponding to \(G_{\text{pos}}^\#(K)\) by \(K_{\text{pos}}^\#/K_{Q_\infty}\). The group \(G_{\text{pos}}^\#(K)\) is designed in the way such that it is a reasonable analogue of \(G_{\mathfrak{O}}^\#(K)\) in Notation 2.1. Indeed, we have to take the above approach to quotient out all the relevant lifts of \(\text{Gal}(K_{Q_\infty}/K)\) (which is the analogue of the Frobenius), because in the function field case the place \(\infty\) of \(K\) cannot further ramify or be further inert. For example, if \(v\) splits completely in \(K/Q\), then the elements \(a_p\)'s are lifts of \(a\) that are compatible with the \(\text{Gal}(K/Q)\) action on all the primes above \(v\), which is exactly the same situation as the function field case. So the quotient map \(\text{Gal}(K_{\text{pos}}(\ell)/Q_\infty) \rightarrow \text{Gal}(K_{\text{pos}}^\#/Q_\infty)\) induces a coinflation map, which gives the analogue of the invariant \(\omega_K^\#\) in Definition 2.13:

\[
\mathbb{Z}_\ell(1) \simeq H_2(\text{Gal}(K_{\text{pos}}(\ell)/Q_\infty), \mathbb{Z})(\ell) \rightarrow H_2(\text{Gal}(K_{\text{pos}}^\#/Q_\infty), \mathbb{Z})(\ell)
\]
and it's clear by our construction that this map factors through \(\mu_\ell\). We cannot recover the group theoretical description of the invariant as described in Proposition 2.6 and Corollary 2.15 because we don't have the analogue of the system of inertia generators for \(\Gamma\)-extensions of \(Q_\infty\). However, we can generalize the cohomological definition of the invariant in §2.2: we can define a trace map \(H^2(\text{Gal}(K_{\text{pos}}(\ell)/K_{Q_\infty}), \mathbb{Z}(1)) \rightarrow \mathbb{Z}_\ell\) and choose the isomorphism (6.6) such that it corresponds to the class of trace \(-|\Gamma|\).

By the discussion above, it's reasonable to consider \(G_{\text{pos}}^\#(K)\) for a number field \(K\) satisfying our assumptions as a good analogue of \(G_{\mathfrak{O}}^\#(K)\) for a function field \(K\). Then, for the number field case, we consider the natural quotient map

\[
G_{\text{pos}}^\#(K) \rightarrow G_{\mathfrak{O}}(K)(\ell),
\] (6.7)
whose kernel is the normal subgroup generated by the inertia subgroups of \(K_{\text{pos}}^\#/K\) at primes above \(v\). Let \(p\) be a prime of \(K\) above \(v\), and \(\mathfrak{p}\) a prime of \(K_{\text{pos}}^\#\) above \(p\). By definition of p.r., the local completion \((K_{\text{pos}}^\#)_{\mathfrak{p}}/K_p\) is a sub-\(\ell\)-extension of \(Q_\ell^\text{pre}/K_p\). As we assumed that \(K\) is \(\ell\)-CM, \(K_p^+\) has index 2 in \(K_p\) and \(\text{Gal}(K_p^+/Q_\ell^+) \cong \text{Gal}(K_p/Q_\ell)\). Recall that \(\rho\) is the \(\ell\)-complex conjugation, we let \((U_{K_p}^1)^{\rho}\) denote the \(\rho\)-invariant subgroup of the principal unit group \(U_{K_p}^1\). Then since \(U_{K_p}^1 \simeq \mathbb{Z}_\ell[\text{Gal}(K_p/Q_\ell)]\) as \(\text{Gal}(K_p/Q_\ell)\)-modules, we have the following isomorphism of Gal\((K_p/Q_\ell)\)-modules

\[
(U_{K_p}^1)^{\rho} \simeq \mathbb{Z}_\ell[\text{Gal}(K_p^+/Q_\ell)] \simeq \mathbb{Z}_\ell[\text{Gal}(K_p^+/Q_\ell)]^{\frac{\ell}{2}}.
\]
So by local class field theory, the maximal pro-$\ell$ abelian subextension of $K_p$ inside $Q^\text{pre}_\ell$ has Galois group isomorphic to $\mathbb{Z}_\ell[\text{Gal}(K_p/Q_v)] \to \mathbb{Z}$, where the extra term $\mathbb{Z}$ comes from the unramified part. Recall that when we define $G^\#_{\text{pos}}(K)$, we quotient out a copy of $\mathbb{Z}_\ell[\text{Gal}(K_p/Q_v)]$ that is generated by $a_p$. So we conclude that the Galois group of the maximal abelian subextension of $(K^\#_{\text{pos}})/K_p$ is a quotient of $\mathbb{Z}_\ell[\text{Gal}(K_p/Q_v)] \to \mathbb{Z}_\ell$. By the Burnside basis theorem for pro-$\ell$ groups, the inertia subgroup of $(K^\#_{\text{pos}})/K_p$ is the $\text{Gal}(K_p/Q_v)$-closed normal subgroup generated by $\frac{\ell-3}{2}$ well-chosen elements. Finally, we look at all the primes above $v$, and obtain that the kernel of the quotient map (6.7) is the $\text{Gal}(K/Q)$-closed normal subgroup generated by $\frac{\ell-3}{2}$ elements. The rank of $\mathcal{O}_{\tilde{\mathcal{O}}}$ is exactly $\frac{\ell-3}{2}$.

The construction above can be applied to other cases, for example, to the case that $Q = \mathbb{Q}(\mu_{\ell^m})$ and $K$ is $\ell$-CM. However, the situations that can be covered are rare because of the $\ell$-CM condition. It would be interesting to understand how to generalize the definition of $\ell$-CM to cover more cases.

**Appendix A. A Random Group Model for Random 3-Manifolds**

In the work [DT06], Dunfield and Thurston studied random orientable 3-manifolds constructed by a random Heegaard splitting, which means gluing two handlebodies by a random walk in the mapping class group of a surface. They compared the probabilities that the random 3-manifolds have finite covers of particular kinds to the analogous probabilities coming from random balanced presentations, and concluded that the fundamental groups of random 3-manifolds have many more finite quotients than the random group model defined by random balanced presentations. In this section, we use the results from Section 5 to construct a random group model to simulate the fundamental groups of 3-manifolds.

Let $\Sigma_g$ be a closed surface of genus $g$, and let $M_g$ be its mapping class group. Then the fundamental group $\pi_1(\Sigma_g)$ of $\Sigma_g$ has a presentation $\langle a_1, \ldots, a_g, b_1, \ldots, b_g \mid [a_1, b_1] \cdots [a_g, b_g] \rangle$, and $M_g$ is naturally isomorphic to an index-2 subgroup of $\text{Out}(\pi_1(\Sigma_g))$. For an element $\varphi \in M_g$, the 3-manifold $M$ obtained by gluing two copies of $\Sigma_g$ by $\varphi$ has fundamental group

$$
\pi_1(M) = \pi_1(\Sigma_g)/[a_1, \ldots, a_g, \varphi(a_1), \ldots, \varphi(a_g)]
$$

where $\varphi \in \text{Aut}(\pi_1(\Sigma_g))$ is a lift of $\varphi$, and $[a_1, \ldots, a_g, \varphi(a_1), \ldots, \varphi(a_g)]$ means the normal subgroup of $\pi_1(\Sigma_g)$ generated by those elements. Also, the map from $\Sigma_g$ to the classifying space $B\pi_1(\Sigma_g)$ defines a homology class in $H_2(\pi_1(\Sigma_g), \mathbb{Z})$, which is invariant under the action of $M_g$. For a finite group $H$, Dunfield and Thurston showed that, as $g \to \infty$, the expected number of covers with covering group $H$ of the random 3-manifold $M$ goes to $|H| H_2(H, \mathbb{Z})/|\text{Aut}(H)|$ ([DT06, Thm.6.21]). Therefore, when we compute the number of surjections from $\pi_1(M)$ to $H$, we have

$$
\lim_{g \to \infty} \mathbb{E}(\# \text{Sur}([H, H])) = |H| |H_2(H, \mathbb{Z})|.
$$

Recall that, $H_2(\pi_1(\Sigma_g), \mathbb{Z})$ can be identified with the kernel of a Schur covering of $\pi_1(\Sigma_g)$. We will explicitly give a pro-$\ell$ random group model that have the above moments for all $\ell$-groups $H$.

Let $\ell$ be a prime number. We use the notation in Section 5 to let $\mathcal{G}_n$ denote the pro-$\ell$ Demuškin group whose abelianization is $\mathbb{Z}_\ell^{2n}$ and let

$$
1 \to \mathbb{Z}_\ell \to \tilde{\mathcal{G}}_n \to \mathcal{G}_n \to 1
$$

denote the Schur covering of $\mathcal{G}_n$. We use the presentation $\mathcal{G}_n = \langle a_1, \ldots, a_n, b_1, \ldots, b_n \mid [a_1, b_1] \cdots [a_n, b_n] \rangle$, and let $\xi_n \in H_2(\mathcal{G}_n, \mathbb{Z}) \cong \ker \pi_n$ denote the image of $[a_1, b_1] \cdots [a_n, b_n]$.

**Proposition A.1.** Consider the random group

$$
Z_n := \tilde{\mathcal{G}}_n/[a_1, \ldots, a_n, \varphi(a_1), \ldots, \varphi(a_n)]
$$

where $\varphi$ is a random walk in $M_1$.
where $\phi$ is a random automorphism of $\widetilde{G}_n$ that preserves and acts trivially on $\ker \pi_n$. Then for any finite $\ell$-group $H$, we have
\[
\lim_{n \to \infty} \mathbb{E} \left( \# \text{Sur}(Z_n, H) \right) = |[H, H]| \cdot |H_2(H, \mathbb{Z})|.
\]

Proof. For an automorphism $\phi$ of $\widetilde{G}_n$, a surjection from $Z_n \to H$ defines a surjection $\widetilde{G}_n \to Z_n \to H$ whose kernel contains $a_i$ and $\phi(a_i)$ for all $i$. So we have
\[
\mathbb{E} \left( \# \text{Sur}(Z_n, H) \right) = \sum_{\phi \in \text{Aut}(\widetilde{G}_n, \pi_n; 1) \text{ s.t. } \pi(a_i) = 1 \forall i} \text{Prob} \left( \phi \in \text{Aut}(\widetilde{G}_n, \pi_n; 1) \left| \phi(a_i) \in \ker \pi, \forall i \right. \right),
\]
where $\text{Aut}(\widetilde{G}_n, \pi_n; 1)$ denote the closed subgroup of $\text{Aut}(\widetilde{G}_n)$ consisting of all automorphisms that preserve and act trivially on $\ker \pi_n$. Each $\pi$ as described in the sum factors through a surjection $\varpi \in \text{Sur}(G_n, H)$ because $\pi([a_1, b_1] \cdots [a_n, b_n]) = 1$. By Lemma 5.5, $\text{Aut}(\widetilde{G}_n, \pi_n; 1)$ acts transitively on the set $\{\varpi \in \text{Sur}(G_n, H) \mid \varpi_* (\xi_n) = 1\}$. Since $\phi(a_i) \in \ker \pi$ if and only if $\pi \circ \phi(a_i) = 1$, we have
\[
\text{Prob} \left( \phi \in \text{Aut}(\widetilde{G}_n, \pi_n; 1) \left| \phi(a_i) \in \ker \pi, \forall i \right. \right) = \frac{\#\{\rho \in \text{Sur}(\widetilde{G}_n, H) \mid \rho(a_i) = 1, \forall i\}}{\#\{\rho \in \text{Sur}(\widetilde{G}_n, H) \mid \rho_* (\xi_n) = 1\}}.
\]
The numerator equals the number of surjections from a free group on generators $b_i$’s to $H$, so it is approximately $|H|^n$ for large $n$. Let $F_{2n}$ denote the free pro-$\ell$ group on the generators $a_1, \ldots, b_n$, and $\bar{H} \to H$ is a Schur covering of $H$. Homomorphisms from $F_{2n}$ to $H$ lift to homomorphisms from $F_{2n}$ to $\bar{H}$. As $n \to \infty$, considering all homomorphisms from $F_{2n}$ to $H$, the image of $[a_1, b_1] \cdots [a_n, b_n]$ is nearly uniformly distributed in $[\bar{H}, H]$. So the denominator above is approximately $|H|^{2n}/|[\bar{H}, H]| = |H|^{2n}/\left(|[H, H]| \cdot |H_2(H, \mathbb{Z})|\right)$. Therefore, we obtain
\[
\mathbb{E} \left( \# \text{Sur}(Z_n, H) \right) \sim |H|^n \cdot \frac{|H|^{2n}}{|[H, H]| \cdot |H_2(H, \mathbb{Z})|},
\]
and the proposition follows after taking $n \to \infty$. \hfill \Box

References

[Ach06] Jeffrey D. Achter, The distribution of class groups of function fields, J. Pure Appl. Algebra 204 (2006), no. 2, 316–333. MR2184814

[Ach08] _____, Results of Cohen-Lenstra type for quadratic function fields, Computational arithmetic geometry, 2008, pp. 1–7. MR2459984

[AM15] Michael Adam and Gunter Malle, A class group heuristic based on the distribution of 1-eigenspaces in matrix groups, J. Number Theory 149 (2015), 225–235. MR3296009

[BB21] Nigel Boston and Michael R. Bush, Heuristics for 2-class towers of cyclic cubic fields, Experimental Mathematics 0 (2021), no. 0, 1–12.

[BBH17] Nigel Boston, Michael R. Bush, and Farshid Hajir, Heuristics for p-class towers of imaginary quadratic fields, Math. Ann. 368 (2017), no. 1-2, 633–669. MR3651585

[BBH21] _____, Heuristics for p-class towers of real quadratic fields, J. Inst. Math. Jussieu 20 (2021), no. 4, 1429–1452. MR4293801

[BW17] Nigel Boston and Melanie Matchett Wood, Non-abelian Cohen-Lenstra heuristics over function fields, Compos. Math. 153 (2017), no. 7, 1372–1390. MR3705261

[CL84] H. Cohen and H. W. Lenstra Jr., Heuristics on class groups of number fields, Number theory, Noordwijk-erhout 1983 (Noordwijk-erhout, 1983), 1984, pp. 33–62. MR756082

[CM87] H. Cohen and J. Martinet, Class groups of number fields: numerical heuristics, Mathematics of Computation 48 (1987), no. 177, 123–137.

[Del77] P. Deligne, Cohomologie étale, Lecture Notes in Mathematics, vol. 569, Springer-Verlag, Berlin, 1977. Séminaire de géométrie algébrique du Bois-Marie SGA 4 1/2. MR0463174

[DT06] Nathan M. Dunfield and William P. Thurston, Finite covers of random 3-manifolds, Invent. Math. 166 (2006), no. 3, 457–521. MR2257389
