# Presentations of Galois groups of maximal extensions with restricted ramification

Yuan Liu

University of Michigan

June 4, 2020

# Cohen-Lenstra Heuristics

For a number field $k$ and a prime $\ell$, denote $\mathrm{Cl}(k)[\ell^\infty]$ the Sylow $\ell$-subgroup of the class group $\mathrm{Cl}(k)$ of $k$.

## Question

How is $\mathrm{Cl}(k)[\ell^\infty]$ distributed when $k$ runs over quadratic number fields? For a finite abelian $\ell$-group $H$, what is

$$\lim_{X\to\infty} \frac{\#\{k \text{ imag./real quad. fields s.t. } |\mathrm{disc}(k)| \le X \text{ and } \mathrm{Cl}(k)[\ell^\infty] \simeq H\}}{\#\{k \text{ imag./real quad. fields s.t. } |\mathrm{disc}(k)| \le X\}}?$$

## Conjecture (Cohen–Lenstra, 1984)

*Let $\ell$ be an odd prime. There are two probability measures $\mu_{CL}^{\pm}$ on finite abelian $\ell$-groups such that, for any finite abelian $\ell$-group $H$, $\mu_{CL}^{\pm}(H)$ predicts the distribution of $\mathrm{Cl}(k)[\ell^\infty]$ as $k$ varies over imaginary/real quadratic number fields. Explicitly, the measures are given by*

$$\mu_{CL}^{+}(H) = \frac{1}{|\mathrm{Aut}(H)|}\prod_{i=1}^{\infty}(1-\ell^{-i}) \quad \textit{and} \quad \mu_{CL}^{-}(H) = \frac{1}{|\mathrm{Aut}(H)||H|}\prod_{i=2}^{\infty}(1-\ell^{-i}).$$

# More about Cohen-Lenstra Heuristics

- The $H$-*moment* version of the Cohen-Lenstra heuristics: Instead of the distribution of $\mathrm{Cl}(k)[\ell^\infty]$, one can consider the average size of $\#\mathrm{Sur}(\mathrm{Cl}(k)[\ell^\infty], H)$ for a finite abelian $\ell$-group $H$.

- Very few cases of the Cohen–Lenstra Heuristics are proven: The $\mathbb{Z}/3\mathbb{Z}$-moment for real quadratic fields is proven by Davenport–Heilbronn (1971).

- The function field analogous conjecture is established by Friedman–Washington (1989), with "$\mathbb{Q}$" replaced by "$\mathbb{P}^1_{\mathbb{F}_q}$", "quadratic fields" replaced by "double covers $C \to \mathbb{P}^1_{\mathbb{F}_q}$", and "$\mathrm{Cl}(k)$" replaced by "$\mathrm{Pic}^0(C)_{\mathbb{F}_q}$". This function field analog is proved (Achter 2004, Ellenberg–Venkatesh–Westerland 2016).

- The probability measures used in Cohen-Lenstra heuristics are well-understood.

## Theorem (Friedman–Washington, 1989)

$$\lim_{n\to\infty} \mathrm{Prob}\left(\mathbb{Z}_\ell^{\oplus n}/n + u \text{ random relations} \simeq H\right) = \frac{1}{|\mathrm{Aut}(H)||H|^u} \prod_{i=1}^{\infty}(1-\ell^{-i-u}).$$

# More about Cohen-Lenstra Heuristics

- The random abelian group model for Cohen-Lenstra heuristics is

$$\lim_{n\to\infty} \mathbb{Z}_\ell^{\oplus n} \big/ n+u \text{ random relations}$$

where $u = 0$ for the imaginary case and $u = 1$ for the real case.

- Ellenberg–Venkatesh (2010) explains this abelian random group model as follows:

$$\mathrm{Cl}(k) = \mathrm{coker}\left(\mathcal{O}_S^\times(k) \to I_S\right),$$

where

$$\begin{array}{rcl} S & : & \text{a sufficiently large finite set of primes of } k, \\ \mathcal{O}_S^\times(k) & : & \text{the } S\text{-units of } k, \\ I_S & : & \text{the group of fractional ideals of } k \text{ generated by } S. \end{array}$$

Note that

$$\begin{aligned} \operatorname{rank} I_S &= \#S, \\ \operatorname{rank} \mathcal{O}_S^\times(k) &= \begin{cases} \#S & \text{if } k \text{ is imag. quad.} \\ \#S+1 & \text{if } k \text{ is real quad.} \end{cases} \end{aligned}$$

This explains why $u = 0$ and $u = 1$ is the imaginary case and the real case respectively.

# Generalize Cohen-Lenstra Heuristics

Note that $\mathrm{Cl}(k)[\ell^\infty]$ is the Galois group of the maximal abelian $\ell$-extension $k_\emptyset^{\mathsf{ab},\ell}$ of $k$, so it's the $\ell$-abelianization of $G_\emptyset(k) := \mathrm{Gal}(k_\emptyset/k)$. One can ask for the distribution of other families of unramified Galois groups.

For the maximal pro-$\ell$ unramified extension $k_\emptyset^{\mathsf{pro}\text{-}\ell}$ of $k$, we have:

## Conjecture (Boston–Bush–Hajir, 2017/2018)

*They extend the Cohen-Lenstra heuristics to a nonabelian setting to predict the distribution of $\ell$-class tower groups $\mathrm{Gal}(k_\emptyset^{\mathsf{pro}\text{-}\ell}/k)$ of imaginary/real quadratic fields $k$, for odd $\ell$.*

- Boston–Wood (2017) proves the moment version of the function field analog of the Boston–Bush–Hajir heuristics.

# Liu–Wood–Zureick-Brown Conjecture

- Fix a finite group $\Gamma$.
- For a Galois $\Gamma$-extension $k/\mathbb{Q}$, we let $k^{\#}$ denote the maximal unramified extension of $k$ such that $[k^{\#} : k]$ is prime to $2|\Gamma|$. In other words, $\mathrm{Gal}(k^{\#}/k)$ is the maximal pro-prime-to-$(2|\Gamma|)$ quotient of $G_{\emptyset}(k)$.

## Conjecture (L.–Wood–Zureick-Brown, 2019)

*We construct a pro-prime-to-$(2|\Gamma|)$ random group model and compute the probability measure defined by it. We conjecture that this probability measure predicts the distribution of $\mathrm{Gal}(k^{\#}/k)$ as $k$ varies among all totally real Galois $\Gamma$-extensions of $\mathbb{Q}$.*

- Our probability measure agrees with the Cohen–Lenstra heuristics and the Boston–Bush–Hajir heuristics.
- The function field analog is similarly formulated, and we prove the moment version of the function field analog.
- We require $[k^{\#} : k]$ to be odd, because $\mathbb{Q}$ contains the 2nd roots of unity and it's known that the roots of unity in the base field would change the distribution in the Cohen–Lenstra setting.
- We require $k$ to be totally real. When $k$ is not totally real and $\Gamma \neq \mathbb{Z}/2\mathbb{Z}$, then the distribution of class groups is predicted by the Cohen–Martinet conjecture.
- We require $[k^{\#} : k]$ to be prime to $|\Gamma|$ because we need to avoid the situation in the Genus theory.

# Construction of random groups in LWZB conjecture

There are 3 important properties of $\mathrm{Gal}(k^{\#}/k)$:

- $\Gamma$-**action:** We obtain a $\mathrm{Gal}(k/\mathbb{Q}) = \Gamma$ action on $\mathrm{Gal}(k^{\#}/k)$ when we fix a homomorphic section of $\mathrm{Gal}(k^{\#}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(k/\mathbb{Q})$.
- **Admissibility:** $\mathrm{Gal}(k^{\#}/k) = \langle g^{-1}\gamma(g) \mid g \in \mathrm{Gal}(k^{\#}/k), \gamma \in \Gamma \rangle$.
- **Property E:** For any prime $\ell \nmid 2|\Gamma|$, $\mathrm{Gal}(k^{\#}/\mathbb{Q}) = \mathrm{Gal}(k^{\#}/\mathbb{Q}) \rtimes \Gamma$ does not admit a nonsplit central group extension by $\mathbb{Z}/\ell\mathbb{Z}$.

We need our random group to satisfy these 3 properties, so we construct

$$X_{\Gamma,u} := \lim_{n\to\infty} \mathcal{F}_n(\Gamma) \big/ [r^{-1}\gamma(r)]_{r\in B_n, \gamma\in\Gamma}$$

where

$$\begin{aligned} \mathcal{F}_n(\Gamma) &: \text{the free admissible } \Gamma\text{-group} \\ B_n &: \text{the set of } n+u \text{ random elements of } \mathcal{F}_n(\Gamma) \end{aligned}$$

We prove that $X_{\Gamma,u}$ satisfies all the above 3 properties and explicitly compute the probability measure defined by $X_{\Gamma,u}$. The computation of moments in the function field case implies that

$u$ should be chosen to be $1$.

# Pro-$\mathcal{C}$ completions

## Definition (Pro-$\mathcal{C}$ completion)

Let $\mathcal{C}$ be a set of finite $\Gamma$-groups. Let $\overline{\mathcal{C}}$ be the smallest set of $\Gamma$-groups that is closed under taking $\Gamma$-quotients, $\Gamma$-subgroups and finite direct products. For a profinite $\Gamma$-group $G$, the *pro-$\mathcal{C}$ completion of $G$* is defined to be

$$G^{\mathcal{C}} := \varprojlim_{M} G/M$$

where $M$ runs over all closed normal $\Gamma$-subgroups of $G$ such that $G/M \in \overline{\mathcal{C}}$.

**Example:** Let $\Gamma = 1$ and $\mathcal{C} = \{\mathbb{Z}/3\mathbb{Z}\}$. Then $\overline{\mathcal{C}} = \{\mathbb{Z}/3\mathbb{Z}, (\mathbb{Z}/3\mathbb{Z})^2, (\mathbb{Z}/3\mathbb{Z})^3, \cdots\}$. So

$$(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z})^{\mathcal{C}} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

**Important property of pro-$\mathcal{C}$ completions:** If $\mathcal{C}$ is a finite set, then

- $\mathcal{F}_n(\Gamma)^{\mathcal{C}}$ is a finite $\Gamma$-group
- the probability defined by

$$(X_{\Gamma,u})^{\mathcal{C}} = \lim_{n\to\infty} {\mathcal{F}_n(\Gamma)^{\mathcal{C}}}\Big/{[r^{-1}\gamma(r)]_{r\in B_n,\gamma\in\Gamma}}$$

  is supported on finite $n$'s.

# Main Theorem

## Theorem (L., 2020)

*Let $\mathcal{C}$ be a finite set of finite $\Gamma$-groups. For any totally real $\Gamma$-extension $k/\mathbb{Q}$, there exists $n$ and a set $B$ of $n+1$ elements of $\mathcal{F}_n(\Gamma)^{\mathcal{C}}$ such that*

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

**Why is this interesting?**

- $\mathrm{Gal}(k_\emptyset/k)$ is not always finite: Golod–Shafarevich (1964) constructed an infinite $\ell$-class tower group of a number field.
- Determining whether $\mathrm{Gal}(k_\emptyset/k)$ is finitely generated or not is a long-existing open question of Shafarevich.
- But this theorem says that $\mathrm{Gal}(k^{\#}/k)^{\mathcal{C}}$ is finite, and moreover, admits a presentation (as a profinite group) with $n(|\Gamma|-1)$ generators and $(n+1)(|\Gamma|-1)$ relations. Also, note that

$$\mathrm{Gal}(k^{\#}/k) = \varprojlim_i \mathrm{Gal}(k^{\#}/k)^{\mathcal{C}_i}$$

  when $\mathcal{C}_i$ is the set containing all $\Gamma$-groups of size $\leq i$.
- The function field analog of this theorem can be similarly formulated. It supports the Liu–Wood–Zureick-Brown conjecture.

# Proof of Main Thm (I): Finiteness of $\mathrm{Gal}(k^{\#}/k)^{\mathcal{C}}$

- **Baby example:** If $\mathcal{C} = \{\mathbb{Z}/\ell\mathbb{Z}\}$, then $\mathrm{Gal}(k_{\emptyset}/k)^{\mathcal{C}}$ is the Galois group of the maximal unramified extension of $k$ whose Galois group is a direct product of $\mathbb{Z}/\ell\mathbb{Z}$. So it's easy to see that $\mathrm{Gal}(k_{\emptyset}/k)^{\mathcal{C}}$ is a finite group.

- **Sketch of the proof:** By group theoretical properties of pro-$\mathcal{C}$ completions, there exists a finite sequence of normal subgroups

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_m = \mathrm{Gal}(k_{\emptyset}/k)^{\mathcal{C}}.$$

  such that $G_{i+1}/G_i$ is a direct product of finite simple groups. Then by the Hermite-Minkowski theorem, each layer $G_{i+1}/G_i$ is finite.

# Proof of Main Thm (II): Presentation of $\mathrm{Gal}(k^{\#}/k)^{\mathcal{C}}$

Since $\mathrm{Gal}(k^{\#}/k)^{\mathcal{C}}$ is finite, for sufficiently large $n$, there is a $\Gamma$-equivariant surjection

$$\pi : \mathcal{F}_n(\Gamma)^{\mathcal{C}} \twoheadrightarrow \mathrm{Gal}(k^{\#}/k)^{\mathcal{C}}$$

Let $M$ be the intersection of all proper maximal $\mathcal{F}_n(\Gamma)^{\mathcal{C}}$-normal subgroup of $\ker \pi$.

- Then $\ker \pi/M$ is a direct product of finite simple $(\mathcal{F}_n(\Gamma)^{\mathcal{C}}/M) \rtimes \Gamma$-groups. For each of these simple factors $A$, we denote the multiplicity of $A$ in $\ker \pi/M$ by $m(n, A)$, which does not depend on the choice of $\pi$.
- A subset $\{x_1, \cdots, x_i\} \subset \ker \pi$ normally generated $\ker \pi$ if and only if their images $\{\overline{x_1}, \cdots, \overline{x_i}\} \in \ker \pi/M$ normal generate $\ker \pi/M$. Moreover, the minimal number of relations of the presentation given by $\pi$ is determined by $m(n, A)$ for all finite simple abelian $A$.
- To compute/bound $m(n, A)$, it suffices to compute

$$\dim H^2(G_{\emptyset}(k), A)^{\Gamma} - \dim H^1(G_{\emptyset}(k), A)^{\Gamma}.$$

**Previous work on using group cohomology to study presentations:**

- If $G$ is a pro-$\ell$ group, then $\dim H^1(G, \mathbb{F}_\ell)$ (resp. $\dim H^2(G, \mathbb{F}_\ell)$) is the minimal number of generators (resp. relations).
- Lubotzky (2001) uses $\dim H^2(G, A) - \dim H^1(G, A)$ to study the difference between the number of generators and the number of relations in a finite presentation of $G$.

# Proof of Main Thm (III): Computation of $\dim H^2 - \dim H^1$

Generally, for a finite set $S$ of places of $k$, we want to compute

$$\delta_S(k, A) = \dim H^2(G_S(k), A)^\Gamma - \dim H^1(G_S(k), A)^\Gamma.$$

## Lemma (Generalized Global Euler-Poincaré Characteristic (L., 2020))

*Let $A$ be a finite simple $\mathbb{F}_\ell[\![\mathrm{Gal}(k_S/\mathbb{Q})]\!]$-module with $\gcd(\ell, |\Gamma|) = 1$. If $S$ contains all archimedean primes and primes above $\ell$, then*

$$\delta_S(k, A) = \dim \widehat{H}^0(\mathbb{R}, A') - \dim H^0(\mathbb{R}, A') - \dim A^{\mathrm{Gal}(k_S/\mathbb{Q})}$$

*where $A' = \mathrm{Hom}(A, \mu_\ell)$ and $\widehat{H}^0$ is the Tate cohomology.*

To study the case $S = \emptyset$, we recall the work of Koch (1970):

- Koch defined a group $\text{Б}_S(k)$ to be the Pontryagin dual of the Kummer group

$$\ker\left(k^\times/k^{\times\ell} \longrightarrow \prod_{\mathfrak{p}\in S} k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times\ell} \times \prod_{\mathfrak{p}\notin S} k_\mathfrak{p}^\times/U_\mathfrak{p} k_\mathfrak{p}^{\times\ell}\right)$$

- Then Koch used $\text{Б}_S(k)$ to compute $\dim H^1(G_S(k), \mathbb{F}_\ell)$ and $\dim H^2(G_S(k), \mathbb{F}_\ell)$, and hence determined the numbers of generators and relations of the pro-$\ell$ completion of $G_S(k)$.

# Proof of Main Thm (III): Computation of $\dim H^2 - \dim H^1$

We generalize the work of Koch by defining

## Definition

$$Б_S(k,A) := \operatorname{coker}\left(\prod_{\mathfrak{p}\in S} H^1(k_\mathfrak{p},A) \times \prod_{\mathfrak{p}\notin S} H^1_{nr}(k_\mathfrak{p},A) \longrightarrow H^1(k,A')^\vee\right)$$

- $Б_S(k,A)$ agrees with Koch's definition, that is $Б_S(k,\mathbb{F}_\ell) = Б_S(k)$.
- Almost all properties of $Б_S(k)$ in Koch's work also hold for our definition, although the failure of the Hasse principle ($Ш^1_S(k,A)$ might be nonzero) makes a difference. In particular, we have

  $$\#\, Ш^2_S(k,A) \leq \#\, Б_S(k,A)$$

  for every $A$, while when $A = \mathbb{F}_\ell$ we have $Ш^2_S(k,\mathbb{F}_\ell) \hookrightarrow Б_S(k,\mathbb{F}_\ell)$.
- By the generalized Euler-Poincaré Characteristic and working with $Б_S(k,A)$, we are able to give upper bound of $\delta_\emptyset(k,A)$. Then we can give upper bound of $m(n,A)$ and prove the main theorem.

# Application (I): When $\Gamma = 1$

Our method and techniques can also be applied to solve other interesting questions regarding the presentation of Galois groups with restricted ramification.

When $\Gamma = 1$, the following theorem follows by our result about

$$\dim H^2(G_S(k), A) - \dim H^1(G_S(k), A)$$

## Theorem (L., 2020)

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

Note that it's not know whether $G_S(k)$ is finitely generated or not. When $k$ is a global function field, $G_\emptyset(k)$ is always finitely generated, and Shusterman (2018) shows that $G_\emptyset(k)$ admits a finite presentation in which the number of relations is exactly the same as the number of generators.

# Application (II): Exceptional cases

Our method can be applied to study the pro-$\ell$ completion $G_\emptyset(k)(\ell)$ of $G_\emptyset(k)$ in the following two cases that are not covered by the LWZB conjecture.

- **When $Q$ is a fixed number field not containing $\mu_\ell$ and $k/Q$ is a $\Gamma$-extension:** The multiplicities for $G_\emptyset(k)(\ell)$ are determined by the decomposition subgroup $\Gamma_\infty$ of $k/Q$ at each archimedean places. This is interesting and potentially useful because $\Gamma_\infty$ plays an important role in the Cohen-Martinet conjecture (the modification of Cohen-Lenstra in this case).

- **When $Q$ contains $\mu_\ell$ and $k/Q$ is a $\Gamma$-extension:** The function field case and the number field case do NOT match! For example, letting $\ell > 3$, the multiplicities for $G_\emptyset(k)(\ell)$ are not the same between $Q = \mathbb{Q}(\zeta_\ell)$ and $Q = \mathbb{F}_q(t, \zeta_\ell)$.

  This supports Malle's observation (2010) that his conjecture regarding the class groups of number fields does not easily match the result for function fields.

Hopefully, these results would help us construct random group models for these exceptional cases.

THANK YOU