Some Seminar Notes

Niven Achenjang

Spring 2021

These are my course notes for "Class name" at School name. Each lecture will get its own "chapter." These notes are live-texed or whatever, so there will likely to be some (but hopefully not too much) content missing from me typing more slowly than one lectures. They also, of course, reflect my understanding (or lack thereof) of the material, so they are far from perfect.[1] Finally, they contain many typos, but ideally not enough to distract from the mathematics. With all that taken care of, enjoy and happy mathing.

The instructor for this class is Prof name, and the course website can be found by clicking this link. Extra extra read all about it

Contents

List of Figures

List of Tables

[1]In particular, if things seem confused/false at any point, this is me being confused, not the speaker

1 Melanie Wood (2/23/2022) – Overview of paper for next few talks

Our goal is understanding the paper of Lie-W.-Zureick-Brown on distributions of unramified extensions of global fields.

Remark 1.1 (Cohen-Lenstra-Martinet Heuristics). For a finite group Γ, gave a conjectural distribution for Cl'_K for K a random Γ-extension of $\mathbb{Q}$ (or K_0). Here,

$$\mathrm{Cl}'_K = \mathrm{Cl}_K \otimes_{\mathbb{Z}} \mathbb{Z}[|\Gamma|^{-1}]$$

(primes dividing $|\Gamma|$ are harder to understand).

There are many sort of issues with their conjecture.

- Malle's numerical computations suggested that these were wrong at primes $p \mid \#\mu_{K_0}$ (e.g. $p = 2$ over $\mathbb{Q}$)
- Bartel-Lenstra found 2 more issues, proved cases of CLM false
  - An issue that Disc isn't a good ordering, suggested instead using product of ramified primes
  - Seems too much to ask for all (but finitely many) Sylow-p subgroups at once (maybe just ask at finitely many p)

We want to think about non-abelian generalizations (+ simultaneous corrections?) of their work.

Remark 1.2. $\mathrm{Cl}_K = \mathrm{Gal}(K^{un,ab}/K) = \mathrm{Gal}(K^{un}/K)^{ab}$.

Question 1.3. *What is the distribution of* $\mathrm{Gal}(K^{un}/K)$*?*

Keep in find that this group is profinite and sometimes infinite.

Open Question 1.4. *Is* $\mathrm{Gal}(K^{un}/K)$ *topologically finitely generated?*

Remark 1.5. $\mathrm{Gal}(K^{un}/K) = \pi_1^{\text{ét}}(\operatorname{spec} \mathscr{O}_K)$. If $K/\mathbb{F}_q(t)$ is the function field of the smooth projective curve C_K, then $\mathrm{Gal}(K^{un}/K) = \pi_1^{\text{ét}}(\operatorname{spec} \mathscr{O}_K) = \pi_1^{\text{ét}}(C_K)$.

A slightly less scary object to consider is the "**p-class tower group**," the pro-p completion $\mathrm{Gal}(K^{un}/K)^{pro-p} = \mathrm{Gal}(K^{un,pro-p}/K)$. Note this can be obtain by repeatedly taking the Hilbert p-class group of K.

1.1 Plan of paper

We want to try to give a conjectural distribution of (some large piece of) $\mathrm{Gal}(K^{un}/K)$, and give some theorems in the function field analogue so you believe the conjecture is true.

Notation 1.6. Let $Q = \mathbb{Q}$ or $Q = \mathbb{F}_q(t)$. Let Γ be a finite group, and assume $\gcd(|\Gamma|, q) = 1$ if $Q = \mathbb{F}_q(t)$. Let $K^{\#}$ be the maximal unramified, split completely at ∞,[2] degree prime to $|\Gamma|$, prime to $|\mu_Q|$, and prime to q if $Q = \mathbb{F}_q(t)$.

[2]This condition is added to make things more like the number field case. e.g. it makes the abelianization finite since otherwise it looks like the Picard group which has an infinite degree factor

For **totally real** (i.e. decomposition group at ∞ is trivial) Γ-extensions K/Q, they give a conjectural distribution for $\mathrm{Gal}(K^{\#}/K)$ (as a group with Γ-action).

Talks to hear (in some order)

(1) Prove some number theoretic facts about $\mathrm{Gal}(K^{\#}/K)$

These will lead to a random "model" with generators and random relations.

(2) We can find and describe distribution of random model

(3) Find moments of $\mathrm{Gal}(K^{\#}/K)$ for $Q = \mathbb{F}_q(t)$ and $q \to \infty$ "first"

(4) Moments (even through a limit) determine a unique distribution (Wang-W., Sawin)

This is good evidence for the conjecture. Also, in abelianization, suggests that we have found all the issues with Cohen-Lenstra-Martinet.

Remark 1.7. Their predicted distribution abelianizes to the C-L-M distribution in an appropriate sense (w/ three previous issues fixed).

Question 1.8. *What does it mean to give a distribution on (non-abelian) profinite groups?*

Let C be a finite set of finite Γ-groups. Let $\overline{C}$ be the 'variety' they generate (so $\overline{C}$ closed under direct product, subgroups, and quotients). If G is a profinite group, can define its **pro-$\overline{C}$ completion** $G^{\overline{C}} = \varprojlim_{G/N \in \overline{C}} G/N$. We topologize the set of groups by saying that the basic open sets are those of the form $\left\{G : G^{\overline{C}} \simeq H\right\}$ for each C, H. Get Borel σ-algebra, and use that to make sense of distributions.

Example. Is $G^{\mathrm{ab}}[p^\infty] \simeq \mathbb{Z}/p\mathbb{Z}$? To phrase such a question, take $C = \{\mathbb{Z}/p^2\mathbb{Z}\}$, so $G^{\overline{C}} = G^{\mathrm{ab}}/p^2G^{\mathrm{ab}}$. Group theory tells us that $G^{\mathrm{ab}}[p^\infty] \simeq \mathbb{Z}/p\mathbb{Z} \iff G^{\mathrm{ab}}/p^2G^{\mathrm{ab}} \simeq \mathbb{Z}/p\mathbb{Z}$, so we can ask for the measure of the basic open $\left\{G : G^{\overline{C}} \simeq \mathbb{Z}/p\mathbb{Z}\right\}$.

Fact. For $G = \mathrm{Gal}(K^{\#}/K)$, it will always be the case that $\#G^{\overline{C}} < \infty$ when $\overline{C}$ is finitely generated.

(key input: only finitely many unramified H-extensions of K for H any finite group)

1.2 Function Field Moments Primer

We want to say why talk **(3)** can be done by studying components of Hurwitz schemes. The moments are $\mathbb{E}[\#\,\mathrm{Sur}_\Gamma(\mathrm{Gal}(K^{\#}/K), H)]$ for finite group H w/ Γ-action.

The assumptions we've made will mean that the H-extension L/K corresponding to such a surjection will be an $H \rtimes \Gamma$ extension L/Q. This translates into counting $H \rtimes \Gamma$ extensions of Q. Each $\mathrm{Sur}_\Gamma(\mathrm{Gal}(K^{\#}/K), H)$ gives $[H : H^\Gamma]$ (counting splittings[3] $\Gamma \to H \rtimes \Gamma$) elements $\psi \in \mathrm{Sur}(\mathrm{Gal}(K^{\#}/Q), H \rtimes \Gamma)$. The moments will be $1/[H : H^\Gamma]$, so we want to show that ($*$ means unramified and split as necessary)

$$\frac{\sum_K \#\,\mathrm{Sur}^*(\mathrm{Gal}(K^{\#}/Q), H \rtimes \Gamma)}{\#\,\mathrm{Sur}^*(\mathrm{Gal}(\overline{Q}/Q), \Gamma)} \longrightarrow 1.$$

There is a Hurwitz space whose $\mathbb{F}_q$-points correspond to precisely the things that we want to count in the numerator and the denominator. Grothendieck-Lefschetz + a comparison theorem reduces the question (for $q \to \infty$ first limit) to counting the number of components of these Hurwitz spaces.

[3]something something conjugacy classes of such given by first cohomology group which vanishes since $\gcd(\#\Gamma, \#H) = 1$

2 Aaron: Model for non-abelian CL heuristics

(Following Lie, Wood, Zureick-Brown sections 2,3)

Note 1. About 3 minutes late

Setup. Let $Q = \mathbb{Q}$ or $Q = \mathbb{F}_q(t)$. For us, we'll imagine $Q = \mathbb{Q}$.

Let K/Q be a Γ-extension (so $\Gamma = \mathrm{Gal}(K/Q)$). Let $K^\#/K$ be the maximal unramified extension, prime to $|\mu_Q|\,|\Gamma|$.

The plan for today is

(1) $\mathrm{Gal}(K^\#/K)$ satisfies

- **(a)** admissibility
- **(b)** property E

(2) Model for $\mathrm{Gal}(K^\#/K)$

Definition 2.1. A **Γ-group** G is a profinite group w/ continuous Γ-action. It is **admissible** if $\gcd(|G|, |\Gamma|) = 1$ and it is generated topologically by elements of the form $g^{-1}\gamma(g)$ for $\gamma \in \Gamma$ and $g \in G$.

Why does $\mathrm{Gal}(K^\#/K)$ have a Γ-action (canonical up to conjugation)?

Theorem 2.2 (**Schur-Zassenhaus**). *Let $1 \to N \to G \to H \to 1$ be an exact sequence of groups with $(|N|, |H|) = 1$. Then, $G \simeq N \rtimes H$ (i.e. $G \to H$ has a splitting), and any two splittings are conjugate.*

Proof idea. Do some reduction to abelian groups (using one of N or H is solvable?). Whether this is a splitting is determined by an element of $\mathrm{H}^2(N, H)$ while the splittings up to conjugacy are parameterized by $\mathrm{H}^1(N, H)$. Both of these vanish since they're killed by $|N|$ and $|H|$. ∎

In the present context, consider the exact sequence

$$1 \longrightarrow \mathrm{Gal}(K^\#/K) \longrightarrow \mathrm{Gal}(K^\#/Q) \longrightarrow \Gamma \longrightarrow 1.$$

By Schur-Zassenhaus, this is a semi-direct product, so $\Gamma \curvearrowright \mathrm{Gal}(K^\#/K)$ by conjugation (after choosing a splitting).

2.1 Properties of $\mathrm{Gal}(K^\#/K)$

Proposition 2.3. $\mathrm{Gal}(K^\#/K)$ *is admissible*

Proof. We have $(\left|\mathrm{Gal}(K^\#/K)\right|, |\Gamma|) = 1$ (recall $\Gamma = \mathrm{Gal}(K/Q)$) by definition of $K^\#$.

Let $G = \mathrm{Gal}(L/K)$ for L/K a finite unramified extension with $([L : K], |\Gamma|) = 1$. Consider the subgroup of commutators $[G, \Gamma] \subset G \rtimes \Gamma$. Note that, since Γ acts by conjugation, we have

$$[G, \Gamma] = \langle g^{-1}\gamma g \gamma^{-1} \rangle = \langle g^{-1}\gamma(g) \rangle .$$

We want to show that $[G, \Gamma] = G$. We have $[G, \Gamma] \leq G$ since it's generated by things of the form $g^{-1}\gamma(g)$ and both $g^{-1}, \gamma(g)$ are in G. For the other containment, it suffices to show that $G/[G, \Gamma] = \mathrm{id}$. For this, let $H := (G \rtimes \Gamma)/[G,\Gamma] = G/[G,\Gamma] \rtimes \Gamma = G/[G,\Gamma] \times \Gamma$ since Γ acts trivially on the quotient $G/[G,\Gamma]$. Let L'/K be the (unramified) extension associated to $G \twoheadrightarrow G/[G,\Gamma]$. Since we got a product, this L' must be the compositum of K/Q and some M/Q. This M/Q will be unramified (since L'/K is), so $M = Q$ and $L' = K$, so $G = [G,\Gamma]$. ∎

What's this property E (E for extensions/embedding problem)?

Definition 2.4. Let H be a Γ-group. Then, H has **property E** if for all non-split extensions

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$$

($\mathbb{Z}/p\mathbb{Z}$ has trivial Γ-action and $(p, |\Gamma|) = 1$) of Γ-groups and surjections $H \twoheadrightarrow G$, there is a (surjective if you want) Γ-equivariant lift $H \twoheadrightarrow \widetilde{G}$.

Non-example. Let $G = (\mathbb{Z}/2\mathbb{Z})^2$ and say $\Gamma = \mathbb{Z}/3\mathbb{Z}$ acts on G by permuting the nontrivial vectors. Then, G is admissible. However, consider (Γ-action extends to Q_8 e.g. by permuting i, j, k)

$$1 \longrightarrow (\pm 1) \longrightarrow Q_8 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^2$$

Then, $G \overset{\sim}{\twoheadrightarrow} (\mathbb{Z}/2\mathbb{Z})$, but this does not lift to Q_8. Such a lift would be a splitting, but there is not such splitting (e.g. since any order 4 subgroup of Q_8 contains $\{\pm 1\}$).

Proposition 2.5. *$G = \mathrm{Gal}(K^{\#}/K)$ satisfies property E.*

Proof idea. Suppose we're given

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \widetilde{G} \rtimes \Gamma \longrightarrow G \rtimes \Gamma \longrightarrow 1$$

and we have $G_Q \twoheadrightarrow G \rtimes \Gamma$. We want to show there is a lift $\widetilde{\pi} : G_Q \to \widetilde{G} \rtimes \Gamma$ where inertia at $v \subset G_{Q_v}$ meets $\mathbb{Z}/p\mathbb{Z}$ trivially for all v (so still giving an unramified extension). Steps

(1) First show each $G_{Q_v} \subset G_Q \twoheadrightarrow G \rtimes \Gamma$ lifts

(2) Use appropriate local-global principal to show that G_Q lifts
(local-global principal for central embedding problems)

(3) Modify lift using class field theory to make inertia condition hold

∎

Corollary 2.6. $\mathrm{Gal}(K^{\#}/K)$ *is never* $(\mathbb{Z}/2\mathbb{Z})^2$ *with the* Γ*-action in the non-example.*

2.2 The model

The idea behind the model is to look at random groups of the form $\mathcal{F}_n/[y(S)]$ with the $\mathcal{F}_n$ giving admissibility and modding out by $[y(S)]$ gives property E.

Definition 2.7. Let $F_n(\Gamma)$ be the free profinite Γ-group on generators $\{x_{i,\gamma} : 1 \le i \le n, \gamma \in \Gamma\}$ where $\sigma \in \Gamma$ acts via $\sigma(x_{i,\gamma}) = x_{i,\sigma\gamma}$. Let $\mathcal{F}_n(\Gamma) \subset F_n(\Gamma)$ be the subgroup topologically generated by $\{x^{-1}\gamma(x) : x \in F_n(\Gamma), \gamma \in \Gamma\}$.

It's not obvious that $\mathcal{F}_n(\Gamma)$ is admissible, but it is.

Lemma 2.8. *$\mathcal{F}_n(\Gamma)$ is admissible. Moreover, letting $i : \mathcal{F}_n(\Gamma) \hookrightarrow F_n(\Gamma)$ be the inclusion, there exists some $q : F_n(\Gamma) \to \mathcal{F}_n(\Gamma)$ so that $qi = \mathrm{id} : \mathcal{F}_n(\Gamma) \to \mathcal{F}_n(\Gamma)$.*

Corollary 2.9. *Any quotient of $\mathcal{F}_n(\Gamma)$ is admissible.*

Definition 2.10. Fix a generating set $\gamma_1, \ldots, \gamma_d \in \Gamma$, and consider the map

$$\begin{array}{cccc} Y: & G & \longrightarrow & G^d \\ & g & \longmapsto & \left(g^{-1}\gamma_1(g), \ldots, g^{-1}\gamma_d(g)\right). \end{array}$$

For $S \subset G$, let $[Y(S)]$ be the closed normal subgroup of G generated by coordinates of $Y(r)$ for $r \in S$.

Definition 2.11. Let $\mathcal{C}$ be a finite set of finite Γ groups, and let $\overline{\mathcal{C}}$ be the smallest set of Γ-groups generated from $\mathcal{C}$ by quotients, subgroups, and products. Given G, we define

$$G^{\mathcal{C}} := \varinjlim_{N \triangleleft G : G/N \in \overline{\mathcal{C}}} G/N,$$

and say that G is **of level** $\mathcal{C}$ if $H^{\mathcal{C}} = H$.

Proposition 2.12. *Given Γ-equivariant surjection $\varphi : \mathcal{F}_n^{\mathcal{C}} \twoheadrightarrow H$, one has $\ker\varphi = [Y(S)]$ for some $S \subset G \iff H$ satisfies property E for Γ-groups of level $\mathcal{C}$.*

Now here's the model:

Let P be the set of admissible Γ-groups H (with order prime to $|\Gamma|$) so that H^C is finite for all $C \in \mathcal{C}$. Given P topology w/ basic opens

$$U_{\mathcal{C},H} = \left\{X \in P : X^{\mathcal{C}} \simeq H\right\}.$$

We set $X_{\Gamma,n} = \mathcal{F}_n/[y(S)]$ where S is a set of $(n+1)$-Haar random elements of $\mathcal{F}_n$. For A a Borel set in P, we set

$$\mu_n(A) = \Pr[X_{\Gamma,n} \in A] \text{ and } \mu(A) := \lim_{n\to\infty} \mu_n(A).$$

Next time we'll explain why the limit exists (and defines a measure).

Conjecture 2.13. *μ models the distribution of* $\mathrm{Gal}(K^{\#}/K)$

Fact.

(1) p-class tower groups are of the form $\mathcal{F}_n/[y(S)]$

(2) (Liu) $\mathrm{Gal}(K^{\#}/K)^{\mathcal{C}}$ of form $\mathcal{F}_n^{\mathcal{C}}/[y(S)]$.

3 Fabian (3/23): $M \to \mu$

Recall 3.1 (Notation)**.** Fix finite group Γ. Let $\mathcal{C}$ be a finite set of finite Γ-groups. Let $\overline{\mathcal{C}}$ be the variety generated by $\mathcal{C}$. For any Γ-group G, we define the **pro-$\mathcal{C}$-completion** $G^{\mathcal{C}} := \varprojlim_{G/N \in \overline{\mathcal{C}}} G/N$ and say G **has level** $\mathcal{C}$ if $G^{\mathcal{C}} = G$.

I missed a talk by Michael, but we've constructed measures μ_n on the set of finite level $\mathcal{C}$ groups. Apparently, to finish his construction, one needs to compute the exponents of some groups. We won't do that today. Instead, we'll use the moments from our desired probability measure in order to recover the measure.

Question 3.2. *How do we compute a (probability) measure* μ *from the moments*

$$M(H) := \sum_G \# \operatorname{Sur}_\Gamma(G, H) \cdot \mu(G).$$

This looks line a linear algebra problem, trying to compute the probabilities from the moments, except it linear algebra in an infinite dimensional space.

Remark 3.3. Following a paper by Sawin, not Melanie's paper

We'll start with some easier cases

(1) First consider some finite Γ-simple (i.e. no non-trivial normal Γ-stable subgroup) Γ-groups $G_1, \dots, G_r$. Let's determine $\mu(1)$, the probability we end up with the trivial group, assuming μ is supported on groups of the form $\prod_i G_i^{e_i}$ with $e_i \geq 0$.

Remark 3.4.

$$\# \operatorname{Sur}_\Gamma\left(\prod_i G_i^{e_i}, \prod_i G_i^{k_i}\right) = \prod_i \# \operatorname{Sur}_\Gamma(G_i^{e_i}, G_i^{k_i})$$

Remark 3.5. Let $h := \# \operatorname{Hom}_\Gamma(G, G)$. Then,

$$\# \operatorname{Sur}_\Gamma(G^e, G^k) = \begin{cases} \displaystyle\prod_{j=0}^{k-1} (h^e - h^j) & \text{if } G \text{ abelian} \\ \displaystyle\prod_{j=0}^{k-1} (e-j)(h-1)^k & \text{if } G \text{ nonabelian} \end{cases}$$

(These were apparently explained in Michael's talk)

Lemma 3.6. *There exists* $c(G, k)$ *so that*

$$\sum_{k \geq 0} c(G, k) \cdot \# \operatorname{Sur}_\Gamma(G^e, G^k) = \begin{cases} 1 & \textit{if } e = 0 \\ 0 & \textit{if } e \geq 1 \end{cases}$$

Corollary 3.7.

$$\mu(1) = \sum_{k_1, \dots, k_r \geq 0} \prod c(G_i, k_i) M\left(\prod G_i^{k_i}\right)$$

(in proving corollary, need to interchange sums and so need some nice convergence property)

Note that the sum in the lemma is finite (summand $= 0$ if $k > e$). This should reduce things to mainly usual linear algebra, and one gets

$$c(G,k) = \begin{cases} \dfrac{(-1)^k}{\prod_{j=1}^k (h^j-1)} & \text{if } G \text{ abelian} \\ \dfrac{(-1)^k}{k!(h-1)^k} & \text{if } G \text{ nonabelian} \end{cases}$$

Remark 3.8. When G nonabelian, the LHS of the theorem becomes $\sum_{k=0}^{e}(-1)^k\binom{e}{k} = (1-1)^e$. In the abelian case, use the 'q-binomial theorem' where $q = h$ here.

(2) Drop assumption about the support of the measure, but still only determine $\mu(1)$, i.e. we'll determine $\mu(1)$ in general.

Definition 3.9. For a Γ-group G, let $Q(G) := G \Big/ \bigcap_{L \subsetneq G} L$ where L ranges over 'proper, maximal Γ-normal Γ-subgroups'.

Remark 3.10. $Q(G) = 1 \iff G = 1$

Lemma 3.11. *There are finitely many Γ-simple Γ-groups $G_1, \dots, G_r$ such that for every level $\mathcal{C}$ group G, we can write*

$$Q(G) \simeq \prod_{i=1}^{r} G_i^{e_i} \text{ for some } e_i \geq 0.$$

(These G_i are the Γ-simple subquotients of groups in $\mathcal{C}$. Sounds like this comes from Jordan-Hölder)

Remark 3.12. Surjections $G \twoheadrightarrow \prod G_i^{k_i}$ factor through $Q(G)$, so

$$\#\operatorname{Sur}_\Gamma(G, \prod G_i^{k_i}) = \#\operatorname{Sur}_\Gamma(Q(G), \prod G_i^{k_i}).$$

The kernel of a map $G \to G_i$ is a maximal Γ-normal Γ-subgroup.

At this point, we can apply **(1)** (essentially ignore the fact that other groups could occur) using only the $\prod G_i^{k_i}$-moments.

(3) Now the general case, determining $\mu(H)$ for any H.

Idea. A surjection $G \twoheadrightarrow H$ is an isomorphism iff its kernel is trivial, so let's try to apply **(2)** to kernels of surjections.

We'll make an attempt to do this, but there will be a mistake in it.

Definition 3.13. Define the measure $\mu^H(N)$ = (expected number of surjections $G \twoheadrightarrow H$ with kernel N), i.e.

$$\mu^H(N) = \sum_{G} \sum_{\substack{\pi: G \twoheadrightarrow H \\ \ker \pi \cong N}} \mu(G).$$

Note that $\mu^H(1)$ is the expected number of isomorphisms between G and H, i.e.

$$\mu^H(1) = \mu(H) \cdot \#\operatorname{Aut}(H).$$

It remains to compute the moments

$$M^H(F) := \sum_N |\mathrm{Sur}_\Gamma(N, F)|\, \mu^H(F)$$

in terms of the moments of μ.

Remark 3.14. For any G, H and $\pi : G \twoheadrightarrow H$ with kernel $\ker \pi = N$, one has

$$\frac{\#\,\mathrm{Sur}_\Gamma(N, F)}{\#\,\mathrm{Aut}(F)} = \#\left\{U \triangleleft N : N/U \cong F\right\}.$$

Now consider the diagram

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r] \arrow[d, two heads] & G \arrow[r, "\pi"] \arrow[d, two heads] & H \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & N/U \arrow[r] \arrow[d, "\wr"] & G/U \arrow[r] \arrow[d, equal] & H \arrow[r] & 1 \\
 & F & Y & &
\end{tikzcd}$$

Imagine counting by first fixing the lower row (fixed G below):

$$\begin{aligned}
\sum_{\substack{\pi : G \twoheadrightarrow H \\ \ker \pi \cong N}} \frac{\#\,\mathrm{Sur}_\Gamma(N, F)}{\#\,\mathrm{Aut}(F)} &= \sum_{\substack{\pi : G \twoheadrightarrow H \\ \ker \pi = N}} \#\left\{U \triangleleft N : N/U \cong F\right\} \\
&= \sum_{\substack{Y, \tau : Y \twoheadrightarrow H \\ \ker \tau \cong F}} \#\left\{U \triangleleft G : G/U \cong Y\right\} = \sum_{Y, \tau} \frac{\#\,\mathrm{Sur}_\Gamma(G, Y)}{\#\,\mathrm{Aut}(Y)}
\end{aligned}$$

(really summing over iso classes of pairs (Y, τ), so the sum is finite (essentially, finitely many extensions of H by F with fin. many Γ-actions)).

Corollary 3.15.

$$\frac{M^H(F)}{\mathrm{Aut}(F)} = \sum_{\substack{Y, \tau \\ \ker \tau \cong F}} \frac{M(Y)}{\#\,\mathrm{Aut}(Y)}.$$

Warning 3.16. The issue above is that U might not be a normal subgroup of G, it's only guaranteed to be normal in N.

The way around this is to redefine moments to only count surjections whose kernel is normal in G. This changes the problem, so one then has to go back and redo steps **(1)**,**(2)**.

Remark 3.17. To figure out if a subgroup is normal, need to know the conjugation homomorphism $G \to \mathrm{Out}(N)$ (which will necessarily factor through H). Now the idea is to do **(1)**,**(2)** in the category of Γ-groups N equipped with a homomorphism $H \to \mathrm{Out}(N)$. This is what Will calls "$\Gamma - [H]$-groups" or something like that.

What's the conclusion?

Aaron constructed a sequence of measure μ_n on finite level $\mathcal{C}$ groups, and these have moments

I'm not sure what this u is here

$$M_n(H) = \frac{\#\operatorname{Sur}_\Gamma(F_n, H)}{\#\operatorname{Hom}(F_n, H)\cdot \#\operatorname{Hom}(F_u, H)},$$

computed by Michael. Sawin's method from today's talk then gives a method from reconstructing the measure μ_n from these moments M_n. If you let $n \to \infty$, then these moments converge to

$$M(H) = \frac{1}{\#\operatorname{Hom}(F_u, H)} = \frac{1}{[H : H^\Gamma]^u}.$$

You can apply Sawin to this in order to produce some measure μ. Natural to ask: does $\mu_n \to \mu$?

Fabian thinks the answer is yes by a dominated convergence argument. Will does something more complicated to justify it.

Warning 3.18. It's not a priori clear that the moments of μ are the $M(H)$'s. This is an additional thing one needs to check.

This can be done by looking at the Liu-Wood-Zureick-Brown (spelling?) paper.

Here's a picture of the situation

$$\begin{tikzcd}
\text{measure } \mu_n \arrow[r, bend left] \arrow[d, "n\to\infty", "\text{dominated convergence}"'] & \text{moments } M_n(H) \arrow[l, bend left, "\text{Sawin}"] \arrow[d, "n\to\infty"] \\
\text{measure } \mu \arrow[r, bend left, "\text{LWZB}"] & M(H) \arrow[l, bend left, "\text{Sawin}"]
\end{tikzcd}$$

Note that this implies in particular that $M(1) = 1$ which says that μ is in fact a probablity measure.

4 Jit Wu (4/13): Hurwitz Spaces and Lifting Invariants

H, Γ finite groups with $\gcd(\#H, \#\Gamma) = 1$. Assume H has some given Γ-action. Say $Q = \mathbb{F}_q(t)$ or $\mathbb{Q}$. Define

$$N(H, \Gamma, D, Q) := \#\left\{\varphi \in \operatorname{Sur}\left(\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), H \rtimes \Gamma\right) \;\middle|\; \begin{array}{c}\text{if } K \text{ is the corresponding extension, then} \\ \operatorname{Nm}\operatorname{rad}(\operatorname{Disc}(K/\mathbb{Q})) = D, K/K^H \text{ unram, and } K/Q \text{ split at } \infty\end{array}\right\}$$

Let G be a finite group, and let $c \subset G$ be closed under conjugation, invertible primes (i.e. $g^n \in c$ if $g \in c$ and $\gcd(n, \#\langle g\rangle) = 1$).

Let $R = \mathbb{Z}[|G|^{-1}]$. The paper constructs a scheme $\operatorname{Hur}^n_{G,c}$ over $\operatorname{spec} R$ so that

$$\operatorname{Hur}^n_{G,c}(\mathbb{F}_q) = N(H, \Gamma, q^n, \mathbb{F}_q(t)).$$

A bit on where this comes from

- First let Hur^n_G be the fiber category of tame Galois covers $X \xrightarrow{f} \mathbb{P}^1$ w/ n branch points and an action of G over $\mathbb{P}^1$.

  That is,
  $$\operatorname{Hur}^n_G(S) = \left\{(f, i) \mid X \xrightarrow{f} \mathbb{P}^1_S \text{ Tame Galois cover, and } i : G \xrightarrow{\sim} \operatorname{Aut} f\right\}.$$

This is a DM stack

- Consider the configuration space $\mathrm{Conf}^n(\mathbb{P}^1) = \left((\mathbb{P}^1_{\mathbb{Z}})^n - \Delta\right)/S_n$ where Δ is the **big diagonal**, tuples $(x_1, \ldots, x_n)$ with $x_i = x_j$ for some $i \neq j$.

  Here's a map $\mathrm{Hur}^n_G \to \mathrm{Conf}^n(\mathbb{P}^1)$ sending a cover to its branch locus. This map is étale.

- Let
$$\mathrm{Hur}^n_{G,1}(S) = \{(f, i, P) \mid (f, i) \in \mathrm{Hur}^n_G(S) \text{ and } P \in X(S) \text{ above } \infty\}.$$

- Let $\mathrm{Hur}^n_{G,*}(S) \subset \mathrm{Hur}^n_{G,1}(S)$ be the subset where ∞ is totally unramified.

  Theorem 4.1. *$\mathrm{Hur}^n_{G,*}$ is representable by a scheme, and $\pi : \mathrm{Hur}^n_{G,*} \to \mathrm{Conf}^n(\mathbb{A}^1)$ is étale*

- Finally, $\mathrm{Hur}^n_{G,c}$ will be the union of the components of $\mathrm{Hur}^n_{G,*}$ where an element of c generates the inertia groups at each (branch) point.

Take $g = H \rtimes \Gamma$. Let $c = \{g \in G \text{ whose image in } \Gamma \text{ has the same order}\}$.

Theorem 4.2. *With above choice of c,*

$$\#\mathrm{Hur}^n_{G,c}(\mathbb{F}_q) = N(H, \Gamma, q^n, \mathbb{F}_q(t)).$$

Proof Sketch. Looking at tame G-covers $X \to \mathbb{P}^1_{\mathbb{F}_q}$ with n branched points which are totally unramified at ∞. This will give $K/\mathbb{F}_q(t)$ where $\mathrm{Gal}(K/\mathbb{F}_q(t)) = H \rtimes \Gamma$ and $\mathrm{Nm}\,\mathrm{rad}(\mathrm{Disc}) = q^n$ since there are n branched points. We will have K/K^H unramified by the choice of c (inertia group in K^H has same size as inertia group in K). The choice of the marked point fixes some place of K above infinity so things are defined on the nose instead of up to conjugation. ■

The number of points will be controlled mainly by the number of Frob-fixed components defined over $\overline{\mathbb{F}}_q$, so we want to count components.

4.1 Topological description of $\mathrm{Hur}^n_{G,c}$

Let $V_n = \{(g_1, \ldots, g_n) : g_i \in c\}$, and let B_n be the braid group

$$B_n = \langle \sigma_1, \ldots, \sigma_{n-1} \,|\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ and } \sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } i - j \geq 2\rangle.$$

Note $B_n \curvearrowright V_n$ via
$$\sigma_i \cdot (g_1, \ldots, g_n) = (g_i, \ldots, g_{i-1}, g_i g_{i+1} g_i^{-1}, g_{i+2}, \ldots, g_n).$$

Fact. $\pi_1(\mathrm{Conf}^n\,\mathbb{C}) \cong B_n$, and $\mathrm{Hur}^n_{G,c}$ is a covering space of $\mathrm{Conf}^n(\mathbb{C})$ w/ fiber V_n

The connected components are then in bijection with V_n/B_n.

Definition 4.3. Let $U(G, c)$ be the group w/ generators $[g]$ for $g \in c$ and relations $[x][y][x]^{-1} = [xyx^{-1}]$.

You get maps $U(G, c) \to G$, $[g] \mapsto g$ as well as $U(G, c) \mapsto \mathbb{Z}^D$ (D the number of conjugacy classes) sending $[g] \mapsto$ generator for its conjugacy class.

Question: What?

Have a map $\pi : V_n \to U(G,c)$ sending $(g_1,\ldots,g_n) \mapsto [g_1]\ldots[g_n]$. One can check this is constant on B_n-orbits, so get induced $\pi : V_n/B_n \to U(G,c)$.

Let $V_n^G \subset V_n$ be subset where g_i's generate G.

Theorem 4.4. *There exists some $M > 0$ (independent of n) so that $\pi : V_n^G/B_n \to U(G,c)$ is bijetive for elements of $U(G,c)$ w/ coordinates in $\mathbb{Z}^D$ all $\geq M$.*

(If c generates G, maybe can replace V_n^G with V_n above?)

Proof idea. $V = \bigcup_{n\geq 1} V_n/B_n$ is a monoid by concatenation

$$(g)(g_1,\ldots,g_n) = \left(gg_1g^{-1},\ldots,gg_ng^{-1}\right)(g).$$

If $h_1\ldots h_n = 1$, then $(h_1)\ldots(h_n)$ is central. Let $v = \prod_{g\in c}(g)^{\mathrm{ord}(g)}$. Then, $V[v^{-1}]$ is a group and in fact $V[v^{-1}] \cong U(G,c)$. Use this + some more group theory.... ∎

Definition 4.5. Let $k = \overline{k}$ be a field. Set

$$\widehat{\mathbb{Z}}(1)_k = \varprojlim_{\gcd(m,p)=1} \mu_m(k) \text{ and } \widehat{\mathbb{Z}}_k = \varprojlim_{\gcd(m,p)=1} \mathbb{Z}/m\mathbb{Z}.$$

Let $\widehat{\mathbb{Z}}(1)_k^\times$ be the group of topological generators. If $\widehat{\mathbb{Z}}_k^\times \curvearrowright X$, we set

$$X\left\langle -1\right\rangle_k = \mathrm{Hom}_{\widehat{\mathbb{Z}}_k^\times}\left(\widehat{\mathbb{Z}}(1)_k^\times, X\right).$$

Note Frob will act on this twist by composition with $(-)^p : \widehat{\mathbb{Z}}(1)^\times \to \widehat{\mathbb{Z}}(1)^\times$.

Remark 4.6. Frobenius won't act on $U(G,c)$ (it's a fixed thing). The thing it naturally acts on is $U(G,c)\left\langle -1\right\rangle_k$.

Notation 4.7. If G is a finite group, $\alpha = (\alpha_m)_m \in \widehat{\mathbb{Z}}_k^\times$ and $g \in G$, then we set

$$g^\alpha := g^{\alpha_{\mathrm{ord}(g)}}.$$

This can be extended to an action on profinite G.

Let $\widehat{U}(G,c)$ be the profinite completion of the (infinite) group $U(G,c)$.

Fact. $U(G,c) = S_c \times_{G^{\mathrm{ab}}} \mathbb{Z}^D$ (whatever this means. smth smth 'Schur cover'? smth smth)

One concludes $\widehat{U}(G,c) = S_c \times_{G^{\mathrm{ab}}} \widehat{\mathbb{Z}}^D$ and that $U(G,c) \hookrightarrow \widehat{U}(G,c)$ (get injection since infinite part coming from this $\mathbb{Z}^D$).

Fact. For $\alpha \in \widehat{\mathbb{Z}}_k^\times$, the action

$$\alpha \star g := \left[g^{\alpha^{-1}}\right]^\alpha$$

preserves $U(G,c)$.

This action is equivariant for the projection $\widehat{U}(G,c) \to \widehat{\mathbb{Z}}^D$.

4.2 Defining the invariant

Let k be an algebraically closed field. Let $K/k(t)$ be a Galois extension. For $t_0 \in K$, looking at the inertia above $t - t_0$ gives a map

$$r_{t_0} : \widehat{\mathbb{Z}}(1)_k \cong \mathrm{Gal}\left(k\left(\left(z^{1/\infty}\right)\right)/k\left(\left(z\right)\right)\right) \longrightarrow \mathrm{Gal}(K/k(t))$$

defined up to conjugation.

Say $U \subset \mathbb{P}^1$ contains ∞. Let $\pi_1'(U, \infty)$ be the maximal prime-to-p quotient of $\pi_1^{\text{ét}}(U, \infty)$. Write $\mathbb{P}^1 \setminus U = \{e_1, \dots, e_n\}$. Then, $\pi_1'(U, \infty)$ contains $\gamma_1, \dots, \gamma_n$ with $\gamma_1 \dots \gamma_n = 1$ so that γ_1 topologically generates inertia at e_i and $\pi_1'(U, \infty)$ is free on $\gamma_1, \dots, \gamma_{n-1}$. Write $\gamma_i = r_{t_i}(\zeta_i)$.

Claim 4.8. *ζ_i's are all equal to some ζ.*

If $\Gamma = (\gamma_1, \dots, \gamma_n)$, set $I(\Gamma) = \zeta \in \widehat{\mathbb{Z}}_k(1)^\times$.

Theorem 4.9 (**Lifting Invariant**)**.** *Say we have a time G-cover $X \to \mathbb{P}^1_k$ with associated map*

$$\varphi : \pi_1'(U, \infty) \longrightarrow G.$$

Then, there is some $\chi \in U(G, c)\langle -1 \rangle$ such that

$$I(\Gamma) \mapsto Z(\Gamma) = [\varphi(\gamma_1)] \dots [\varphi(\gamma_n)].$$

This is well-defined independent of choice of γ_i's.

Theorem 4.10. *The Lifting invariant is constant on connected families.*

5 List of Marginal Comments

Index