Arithmetic statistics of function fields via Hurwitz spaces

Libby Taylor
November 18, 2019

1 Logistics

These are notes taken from the learning seminar on the arithmetic statistics of function fields via Hurwitz spaces at Berkeley in fall 2019. I plan to write up notes weekly, and will upload them to my website here: http://web.stanford.edu/~lt691/.

Each lecture will be labelled with the speaker for that week. Any errors in these notes, however, are mine; if you find any, whether mathematical or typographical, please email and let me know.


2.1 Arithmetic statistics of number fields

The main questions in the field known as “arithmetic statistics” have to do with counting number fields. More precisely, one can ask: for \( G \) a finite group, how many Galois extensions of \( \mathbb{Q} \) are there with Galois group \( G \) and discriminant at most \( X \), for \( X \) some real number? We denote this quantity as

\[
N_G(X) = \# \{ K/\mathbb{Q} \text{ with } Gal(K/\mathbb{Q}) \cong G \text{ and } |\text{disc}K| \leq X \}
\]

\( N_G(X) \) is always finite. One can consider the asymptotic behavior of \( N_G(X) \) for any fixed \( G \) as \( X \to \infty \).

Example. \( N_{\mathbb{Z}/2}(X) \sim c_2X \) with \( c_2 \) a positive constant. Informally, this says that the number of quadratic number fields of discriminant at most \( X \) is a quantity linear in \( X \).

Example. \( N_{\mathbb{Z}/3}(X) \sim c_3X^{1/2} \) for \( c_3 \) a positive constant. Informally, this means that the number of cyclic cubic number fields with discriminant at most \( X \) grows like \( \sqrt{X} \).

One can also ask: how many of these fields have certain properties? For example, in how many of these fields does the prime \( (7) \) split completely? In how many does \( (7) \) ramify? This type of question can be thought of as an inverse Cebotarev problem: instead of fixing a field and considering various primes, we fix a prime and vary the field.

Another interesting question is: For a fixed abelian group \( A \), how often is \( Cl(K) \cong A \)? How often is it true that \( Cl(K)[3] = 0 \), i.e. the class number is not divisible by 3?

2.2 Arithmetic statistics of function fields

One can ask very similar questions when \( \mathbb{Q} \) is replaced by the function field \( \mathbb{F}_q(t) \) for \( q \) some prime power. The polynomial subring \( \mathbb{F}_q[t] \) is a Dedekind domain, so we can ask all the familiar questions about whether primes ideals in \( \mathbb{F}_q[t] \) ramify, split, or remain inert. As in the number field case,
2.3 Relation to Hurwitz spaces

\( \mathcal{O}_K \) is the ring of integers of a function field \( K \), i.e. the integral closure of \( \mathbb{F}_q[t] \) inside \( \mathbb{F}_q(t) \). In the function field case, one has \( \text{disc} \mathcal{O}_K/\mathbb{F}_q[t] \) is an ideal in \( \mathbb{F}_q[t] \), rather than an integer. So, we define, for any finite group \( G \) and real number \( X \),

\[
N_G(X) = \# \{ \text{extensions } K/\mathbb{F}_q(t) \text{ with } \text{Gal}(K/\mathbb{F}_q(t)) \cong G \text{ and norm} (\text{disc} \mathcal{O}_K/\mathbb{F}_q[t] \leq X) \}
\]

We recall the following classical theorem about the equivalence between function fields and smooth projective curves:

**Theorem 2.1.** For \( k \) a field, there exists an equivalence of categories

\( \{ \text{finitely generated extensions } K/k \text{ of transcendence degree } 1 \}^{op} \iff \{ \text{regular projective curves over } k \} \)

The functor \( C \to k(C) \) sending a curve to its function field provides the right-to-left functor in this equivalence.

One can now ask questions about function field distributions: as \( K \) varies among \( G \)-number fields, i.e. number fields \( K \) with \( \text{Gal}(K/\mathbb{Q}) \cong G \), or \( G \)-function fields, i.e. fields \( K \) with \( \text{Gal}(K/\mathbb{F}_q(t)) \cong G \), how does \( \text{Cl}(K) \) vary?

**Remark 1.** \( \text{Cl}(K) \) comes equipped with a \( G \)-action, so one can think of it as a \( G \)-module.

Cohen-Lenstra-Martinet gave precise conjectures for all \( G \) in the number field case:

**Conjecture 2.2.** (Cohen-Lenstra-Martinet)

\[
\lim_{X \to \infty} \frac{\# \{ K \text{ below with } \text{Cl}(K)_{\text{odd}} \cong A \}}{\# \{ K/\mathbb{Q} \text{ real quadratic with } \text{disc}(K) \leq X \}} = \frac{c}{\# A \# \text{Aut } A}
\]

for \( c \) some absolute constant (which one can write down but I’m not going to).

2.3 Relation to Hurwitz spaces

Hurwitz spaces are moduli spaces of covers of \( \mathbb{P}^1 \) of fixed degree and fixed number of ramification points. By the equivalence between curves and function fields, one can rephrase many questions about the arithmetic statistics of function fields as questions about counting \( \mathbb{F}_q \) points of a suitable Hurwitz space. Let \( \mathcal{H}_{r,d} \) denote the Hurwitz space of degree \( d \) covers of \( \mathbb{P}^1 \) ramified over \( r \geq 3 \) points. \( \mathbb{F}_q \)-points on \( \mathcal{H}_{r,d} \) correspond to degree \( d \) extensions of \( \mathbb{F}_q(t) \), ramified over \( r \) places of \( \mathbb{F}_q(t) \). This approach allows one to use geometric techniques to solve arithmetic statistical problems.

3 Moments determining a distribution and class group counting as field counting: Thomas Browning. September 11.

**Main question:** For a finite group \( G \), we would like to find the distribution of class groups of \( G \)-extensions of \( \mathbb{F}_q(t) \). One can solve this problem by counting moments; this reduces to field counting and from there, reduces to curve counting, where we can use geometric techniques from Hurwitz spaces.
3.1 Moments

What is a moment: let $\mu$ is a probability distribution on the space of isomorphism classes of finite abelian groups, denoted $A$, i.e. $\sum_{A \in A} \mu(A) = 1$. Then for $B$ any finite abelian group, one can consider

$$\mathbb{E}(|\text{surj}(A, B)|) = \sum_{A \in A} \mu(A) \cdot |\text{surj}(A, B)|$$

which we define to be the moment of $B$. This is the expected number of surjections onto $B$ from a random element of $A$. Morally: moments determine a distribution. That is, if we know the moments of all $B \in A$, then we can recover $\mu$. In all the cases that we care about, this “moral philosophy” will be literally true.

Therefore, a new (equivalent) problem to the main question above is determining $\mathbb{E}(|\text{surj}(Cl_K, B)|)$ for each finite abelian group $B$, where $K$ runs through all $G$-extensions of $\mathbb{F}_q(t)$. More precisely, one should run over such $K$ with bounded discriminant, then send discriminant to $\infty$.

3.2 Reductions to different counting problems

By class field theory, the class group of $K$ can be realized as a Galois group: $Cl_K \cong \text{Gal}(H_K/K)$ where $H_K$ is the Hilbert class field of $K$, i.e. the maximal abelian everywhere-unramified extension of $K$ which is split completely at infinity.

Now, surjections $Cl_K \rightarrow B$ are identified with surjections $\text{Gal}(H_K/K) \rightarrow B$, which can in turn be identified with subgroups of $\text{Gal}(H_K/K)$ with quotient isomorphic to $B$.

Remark 2. This correspondence is off by a factor of $\text{Aut}(B)$, but we’re going to ignore this detail for now.

Our problem has now been reduced to counting:

$\{B$-extensions of $K$ that live inside $H_K$ $\}$

or

$\{\text{unramified, split-completely-at-}\infty, B$-extensions fo $K$ $\}$.

But, $K$ is still varying over all $G$-extensions, which makes it harder to count such $L$, i.e. $L$ that live in towers of the form

$$\begin{array}{ccccccc}
H_K & \downarrow & & & & & \\
\downarrow & & & & & & \\
L & \downarrow & & & & & \\
\downarrow & & & & & & \\
B & \downarrow & & & & & \\
K & \downarrow & & & & & \\
\downarrow & & & & & & \\
G & \downarrow & & & & & \\
\mathbb{F}_q(t) & \uparrow & & & & & \\
\end{array}$$

So, this count isn’t quite what we want to consider: it will also be necessary to keep track of the $G$-module structure on $Cl_K$. So instead, we count

$$\mathbb{E}(|\text{surj}_G(Cl_K, B)|)$$

for $B$ a finite $G$-module, where $\text{surj}_G(Cl_K, B)$ denotes the $G$-equivariant surjections $Cl_K$ to $B$. Equivalently, one can count:
\{\text{equivariant surjections}\}

or

\{G\text{-submodules of } Cl_K\}

or

\{B\text{-extensions of } K \text{ where the } G\text{-action on } B \text{ prescribed by the } G\text{-module structure agrees with the one given by conjugation}\}.

The action given by conjugation arises from the short exact sequence $1 \to \text{Gal}(L/K) \cong B \to \text{Gal}(L/F_q(t)) \to G \to 1$; since $B$ is abelian, $G$ acts on it by conjugation.

Suppose now that $\gcd(|G|,|B|) = 1$, and consider the last counting problem listed above. Schur-Zassenhaus implies that $\text{Gal}(L/F_q(t)) \cong B \times G$, where the map $G \to \text{Aut}(B)$ is the one prescribed by the $G$-module structure on $B$. The problem is now evidently equivalent to counting $B \times G$-extensions of $F_q(t)$. More precisely, we should count $B \times G$-extensions of $F_q(t)$ where the order of inertia is coprime to $|B|$ and where the order of the decomposition group at $\infty$ is divisible by $|B|$. These 2 conditions will respectively provide the condition on the extensions being everywhere unramified and split completely at $\infty$.

**Remark 3.** The condition about splitting completely at infinity will be relevant later on in constructing compactifications of the relevant moduli spaces.

At some point, we restricted to counting $G$-equivariant surjections, rather than all surjections. We now justify why this is a valid reduction:

**Claim:** the set $E(\mid \text{surj}_G(Cl_K, B) \mid)$ determine the set $E(\mid \text{surj}(Cl_K, G) \mid)$. That is, the moments of $G$-modules determine the moments of abelian groups.

To understand this claim: note that for any abelian group $C, C \times \cdots \times C$, where there are $|G|$ copies of $C$, has a $G$-module structure given by permuting the factors. This allows us to take any abelian group and use it to build an associated $G$-module.

Let $\varphi : \text{surj}(Cl_K, C) \to \text{Hom}(Cl_K, C \times \cdots \times C)$ be defined by $\varphi(f) = (c \mapsto (g \mapsto f(gc)))$. This map is injective, which follows from the fact that $f(c) = \varphi(f)(c)(1)$; in particular, $f$ can be recovered from $\varphi(f)$. Therefore to count $\text{surj}(Cl_K, C)$, it suffices to count its image in $\text{Hom}(Cl_K, \text{Hom}_{set}(G, C))$. We have that $\varphi(f)$ is $G$-equivariant for each $f$, so $\text{im}\varphi$ is a $G$-submodule of $\text{Hom}_{set}(G, C)$. Want to characterize $\text{im}\varphi$ so that we can count the image.

If $M = \text{im}(\varphi(f)) \subset \text{Hom}_{set}(G, C)$, then $\varphi(f)(c)(1) = f(c)$. $f$ is assumed surjective, so $\varphi(f)(c)$ ranges over all elements of $M$. This implies that $\{m(1) : m \in M\} = C$. This turns out to be the defining property of the image of $\varphi$. Define

$$\mathcal{F} := \{G - \text{submodules } M \subset \text{Hom}_{set}(G, C) \text{ such that } \{m(1) : m \in M\} = C\}.$$

**Claim:** $\mid \text{surj}(Cl_K, C) \mid = \sum_{M \in \mathcal{F}} \mid \text{surj}_G(Cl_K, M) \mid$. If this claim holds, then this proves that the moments can be recovered from the $G$-equivariant moments. In fact, the $G$-equivariant moments provide strictly more information than the ordinary moments, since they know what the class group distribution $\ast$together with its $G$-action$\ast$ look like; the ordinary moments don’t know the $G$-module structure on the class groups.

Throughout, let \( k = \mathbb{F}_q \) be a finite field; \( X/\text{Spec} k \) a finite type \( k \)-scheme; \( \overline{k} \) a fixed algebraic closure of \( k \); and \( G_k \) the absolute Galois group of \( k \). Let \( \phi \in \text{Gal}(\overline{k}/k) \) be the geometric Frobenius defined by \( \phi(x) = x^{1/q} \). Finally, let \( r = \dim(X) \).

**Main question:** How to count \( \# X(k) \), i.e. how do we count the number of \( k \)-points on \( X \)?

4.1 Lang-Weil bound

The first tool for counting \( \# X(k) \) is the Lang-Weil bound:

**Theorem 4.1.** If \( X \to \mathbb{P}^n \) is projective of degree \( d \) and \( X \) is geometrically integral, then \( |N_q| \leq (d-1)(d-2)q^{r-1/2} + A(n,d,r)q^{r-1} \). Here, \( A(n,d,r) \) is a constant depending on \( n,d \) and \( r \); in particular, this constant is independent of \( q \).

**Proof.** The idea of the proof is to induct on the dimension of \( X \). The base case is \( r = 1 \), i.e. \( X \) is a projective curve. In this case, the Riemann hypothesis for curves over finite fields gives

\[
|1 + q - N| \leq 2gq^{1/2}
\]

where \( g \) is the genus of \( X \). Let \( p_i := \# \mathbb{P}^i(k) \) denote the number of \( k \)-points on \( \mathbb{P}^i \). We now drop the hypothesis that \( r = 1 \) and let \( X \) be a projective variety of arbitrary dimension. Then

\[
p_nN = \sum_{H \subset \mathbb{P}^n} |(X \cdot H)(k)|
\]

where \( N := \# X(k) \) and \( H \) ranges over the rational hyperplanes in \( \mathbb{P}^n \), i.e. the hyperplanes defined over \( k \). Split the above sum into 2 terms:

\[
\sum_{H \subset \mathbb{P}^n} |(X \cdot H)(k)| = \sum_{H \in R} |(X \cdot H)(k)| + \sum_{H \notin R} |(X \cdot H)(k)|
\]

where \( R \) denotes the subset of hyperplanes in \( \mathbb{P}^n \) whose intersection with \( X \) is still geometrically irreducible, i.e. \( (X \cdot H)_R \) is still geometrically irreducible. By induction, we can control the behavior of \( \sum_{H \in R} |(X \cdot H)(k)| \), and one can show that the term \( \sum_{H \notin R} |(X \cdot H)(k)| \) has many fewer terms (morally, this means that “\( X \) remains geometrically irreducible after intersecting with most hyperplanes in \( \mathbb{P}^n \)”). \( \square \)

To see that the geometric irreducibility hypothesis is really necessary for the Lang-Weil estimate to hold, we consider a non-example:

**Example 4.2.** Take \( D \in k^\times \setminus (k^\times)^2 \) and consider the scheme \( X = V(x_0^2 - Dx_1^2) \subset \mathbb{P}^2 \). This is a one-dimensional irreducible degree 2 projective scheme on \( \mathbb{P}^2 \). If the Lang-Weil estimate holds, it would mean that \( |N - q| \leq A(n,d,r) \), where \( A(n,d,r) \) is independent of \( D \) and \( q \). In particular, letting \( q \to \infty \) would imply that \( N \to \infty \). One can check directly, though, that the only solution to the equation \( x_0^2 - Dx_1^2 = 0 \) is \([0 : 0 : 1]\), so clearly the Lang-Weil estimate is false. The problem here is that \( X \) is irreducible but not geometrically irreducible.
4.2 Counting points via fixed point formula

The second approach to counting points is inspired by topological trace formulas. The Galois group $G_k$ acts on $X(k)$ in the obvious way, by composing maps $\text{Spec}(k) \to X$ with the Galois action on $\text{Spec}(k)$. Recall the $G_k$ is generated by the Frobenius $\phi$, and note that $p \in X(k)$ is a $k$-point if and only if it is a fixed point of $\phi$, i.e. $p \circ \phi = p$. Therefore $X(k) = X(k)^{\phi(p) = p}$. The Lefschetz-Hopf theorem from topology states:

**Theorem 4.3.** Let $M$ be a compact triangulable topological space and let $f : M \to M$ be a self-map. Consider the Lefschetz number

$$L(f) = \sum (-1)^i \text{Tr}(f \mid H^i(M, \mathbb{Q})).$$

If $f$ has only finitely many fixed points, then

$$L(f) = \sum_{x \in \text{Fix}(f)} i(x; f).$$

This allows one to count fixed points of a topological self-map; one could dream that there is an algebraic analogue of this theorem that would allow one to count fixed points of an algebraic self-map (in particular, we are interested in the Frobenius as this algebraic self-map). It turns out that such an analogue does exist, and this is what motivated the creation of étale cohomology.

**Motivation for étale cohomology:** One of the main goals of étale cohomology is to “algebraize” singular cohomology. One of the defects of Zariski cohomology is that it doesn’t “see” any higher cohomology of constant sheaves; that is, $H^i(X, \Lambda) = 0$ for $i > 0$ and all constant sheaves $\Lambda$. Constant sheaves, though, certainly have higher singular cohomology. One of the virtues of étale cohomology is that it recovers singular cohomology, but is defined in an entirely algebraic way. To do this, one adds new open sets to the Zariski site to get a finer topology. (Strictly speaking, this is not a topology, but a Grothendieck topology.) The new opens that we will add to the topology will be the algebraic analogues of local homeomorphisms, i.e. covering spaces.

4.3 Crash course on étale cohomology

Most of the results stated in this section will be black-boxed. Let $Y$ denote a finite-type scheme over an arbitrary field $F$. Fix an algebraic closure $\overline{F}$ and let $G_F = \text{Gal}(\overline{F}/F)$. Let $\ell \neq \text{char}(k)$ a prime. All cohomology groups in this section are étale.

For each $\ell$, there are functors of $\mathbb{Q}_\ell$-vector spaces $H^i(Y_{\overline{F}}, \mathbb{Q}_\ell) \to H^i_c(Y_{\overline{F}}, \mathbb{Q}_\ell)$, where $H^i_c$ denotes cohomology with compact support. By functoriality of étale cohomology, these cohomology groups come equipped with a $G_F$ action, induced from the $G_F$ action on $Y(\overline{F})$. These $\mathbb{Q}_\ell$-vector spaces are finite-dimensional; let $h^i = H^i(Y_{\overline{F}}, \mathbb{Q}_\ell)$ and $h^i_c = H^i_c(Y_{\overline{F}}, \mathbb{Q}_\ell)$. By dimensional vanishing for étale cohomology, $h^i = h^i_c = 0$ if $i > 2\dim(Y)$.

**Theorem 4.4** (Grothendieck-Lefschetz trace formula).

$$\#X(k) = \sum_{i \geq 0} (-1)^i \text{Tr} (\phi : H^i_c(X_k, \mathbb{Q}_\ell)).$$

As a motivation for the use of compactly supported étale cohomology, recall that the classical Lefschetz-Hopf formula required the topological spaces to be compact polyhedra.

A priori, $\text{Tr}(\phi : H^i_c(X_k, \mathbb{Q}_\ell)$, motivating the following definition:

**Definition 1.** Let $\varepsilon \in \mathbb{Q}$ an algebraic number. $\varepsilon$ is said to be a $q$-Weil number, or simply $q$-number, if the absolute value $| \tau(\varepsilon) | = q^{1/2}$ for any embedding $\tau : \mathbb{Q} \to \mathbb{C}$.
Fact: The eigenvalues of $\phi$ acting on $H^i_c(X_{\overline{k}})$ are all $q^w$-Weil numbers for an integer $w \leq i$. In particular, $|\text{Tr}(\phi): H^i_c(X_{\overline{k}}) | \leq h^i q^{i/2}$. Moreover, if $X$ is assumed smooth and proper then all the eigenvalues are $q^i$-Weil numbers.

Suppose we want to compute the action of $\phi$ on $H^{2r}_c(X_{\overline{k}}, \mathbb{Q}_\ell)$. In the case that $X$ is smooth and geometrically connected, one can use Poincaré duality to say:

**Theorem 4.5** (Poincaré duality). There is a perfect pairing given by cup product

$$ H^i(X, \mathbb{Q}_\ell(r)) \times H^{2r-i}_c(X, \mathbb{Q}_\ell) \to H^{2r}_c(X, \mathbb{Q}_\ell(r)) = \mathbb{Q}_\ell $$

where $(r)$ denotes the $r$-th Tate twist, so $\mathbb{Q}_\ell(r) := \mathbb{Q}_\ell \otimes \mu_{\infty}^{\otimes r}(\overline{k})$, where $\mu_{\infty}$ denotes an inverse system with multiplication by $\ell$. Therefore to compute $H^{2r}_c(X_{\overline{k}}, \mathbb{Q}_\ell)$, it is equivalent to compute $H^0(X, \mathbb{Q}_\ell)^\vee$ and its Frobenius action.

**Theorem 4.6** (Smooth and proper base change). Suppose we have a proper smooth morphism of finite type schemes $f : Y \to S$ with $S$ connected. Then for any pair of algebraically closed fields $t_i$, with $s_i = \text{Spec}(t_i)$ and any map $s_i \to S$, we have an isomorphism $H^i(Y_{s_1}, \mathbb{Q}_\ell) \cong H^i(Y_{s_2}, \mathbb{Q}_\ell)$.

In the case of $X/k$ a smooth proper geometrically integral curve, there exists a smooth proper model $X/W(k)$ of $X$ over the ring of Witt vectors of $k$. Then we can calculate $H^i(X, \mathbb{Q}_\ell)$ by passing to the generic fiber of $X$, embedding $W(k)[1/p] \to \mathbb{C}$ and using the comparison theorem to identify étale and singular cohomology of this generic fiber. Plugging this into the trace formula gives

$$ \# X(k) = \text{Tr}(\phi | H^0) - \text{Tr}(\phi | H^1) + \text{Tr}(\phi | H^2) = 1 - (\text{sum of } 2g \text{ Weil } q\text{-numbers}) + q $$

so $\# X(k) - (q + 1) \leq sg \cdot q^{1/2}$.


**Main goal:** For a fixed finite group $G$, construct a parameter space for Galois $G$ covers of $\mathbb{P}^1$, and give it the structure of a scheme over $\mathbb{Z}$. This will allow us to count $G$-covers of $\mathbb{P}^1_{\overline{\mathbb{F}_q}}$ by counting the $\mathbb{P}^1_{\overline{\mathbb{F}_q}}$-points of this parameter space. In this lecture, we won’t get to describing the scheme structure; that will be postponed to the next talk. Today, we’ll be satisfied with giving it a complex analytic structure. That is, we will describe the Hurwitz space as a set, and describe the open neighborhoods of each point in it.

5.1 Notation

Everything in this lecture is happening over $\mathbb{C}$. The following notation will be in force throughout.

- $G$ is a finite group.
- $U \leq G$ is a subgroup with no nontrivial normal subgroup. (The condition on having no nontrivial normal subgroup will be important because we’ll consider the conjugacy class of $U$; the simplest example of such a $U$ is the trivial subgroup.)
- $\text{Aut}(G, U)$ are the automorphisms of $G$ preserving the conjugacy class of $U$.
- $\text{Inn}(G)$ is the group of inner automorphisms of $G$. 

• For $r > 1$, $E_r = \{ (\sigma_1, \ldots, \sigma_r) : \sigma_i \in G, (\sigma_1, \ldots, \sigma_r) = G, \sigma_1 \cdots \sigma_r = 1 \}$. In words: $\{ \sigma_1 \}$ is an $r$-tuple of elements of $G$, such that the $\sigma_i$ together generate $G$ and such that their product is $1$. At the moment, this is just a set; later on we will endow it with a complex analytic structure.

• $E_r^{ob} = E_r / \text{Aut}(G, U)$.

• $E_r^{in} = E_r / \text{Inn}(G)$.

### 5.2 Covers of $\mathbb{P}^1$ via fundamental groups

Let $C$ be a conjugacy class of $G$. Let $C^m$ denote the conjugacy class of the set $\{ g^m : g \in C \}$. Let $\overrightarrow{C} = (C_1, \ldots, C_r)$ be an $r$-tuple of conjugacy classes.

**Definition 2.** $\overrightarrow{C}$ is said to be rational if, for all $m$ prime to $\#G$, one has $(C_1^m, \ldots, C_r^m) = (C_{\pi(1)}, \ldots, C_{\pi(r)})$ for some $\pi \in S_r$. That is, $\overrightarrow{C}$ is rational if every prime-to-$\#G$ power of it can be obtained by permuting the original $C_1, \ldots, C_r$.

Fix an embedding $\mathbb{A}^r \hookrightarrow \mathbb{P}^r$. Recall that the points of $\mathbb{A}^r$, as a set, can be identified with the set of polynomials of degree at most $r$, and the points of $\mathbb{P}^r$, as a set, can be identified with the set of polynomials of degree exactly $r$. With this in mind, define $D_r$ to be the discriminant locus for degree $r$ polynomials; that is, $D_r$ is the Zariski closure in $\mathbb{P}^r$ of the locus of all polynomials with repeated roots. Set $U_r = \mathbb{P}^r \setminus D_r$, so that $U_r$ is the open set in $\mathbb{P}^r$ corresponding to polynomials with distinct roots. Note that

$$ U_r \iff \{ \text{sets of } r \text{ distinct points in } \mathbb{C} \} $$

by sending a polynomial in $U_r$ to its set of roots.

Fix a rational base point $b = \{ b_1, \ldots, b_r \}$ in $U_r$. Define the Hurwitz monodromy group to be the fundamental group

$$ H_r = \pi_1(U_r, b) = \pi_1(\mathbb{A}^r \setminus D_r, b)/\mathbb{A}^r \hookrightarrow \mathbb{P}^r. $$

**Remark 4.** One has that $\pi_1(\mathbb{A}^r \setminus D_r, b) \cong B_r$, the Artin braid group.

We would like to define an equivalence relation on covers of $\mathbb{P}^1$. To this end, we say that 2 branched covers $\phi : X \to \mathbb{P}^1$ and $\phi' : X' \to \mathbb{P}^1$ are equivalent if there exists a morphism $\delta : X \to X'$ such that $\phi' \circ \delta = \phi$. For $X \to \mathbb{P}^1$ an equivalence class of covers, consider $\text{Aut}(X/\mathbb{P}^1)$ the automorphism group of this cover. We say that $\phi$ is Galois if $\text{Aut}(X/\mathbb{P}^1)$ acts transitively on the fibers of $\phi$. In this case, $\text{Aut}(X/\mathbb{P}^1)$ is the Galois group of $\phi$.

Let $a_1, \ldots, a_r$ be the branch points of the cover $\phi$, and for ease of notation, set $a := \{ a_1, \ldots, a_r \}$ to be the $r$-tuple of ramification points. Now $\phi$ restricts to an unramified cover $\phi^0$ over $\mathbb{P}^1 \setminus a$. $\mathbb{P}^1 \setminus a$ is a punctured Riemann sphere with $r$ punctures; pick $a_0 \in \mathbb{P}^1 \setminus a$ some basepoint.

By basic covering space theory, equivalence classes of unramified $\phi^0$ correspond to conjugacy classes of subgroups $U_\phi \leq \Gamma$ where $\Gamma := \pi_1(\mathbb{P}^1 \setminus a, a_0)$. Note that the choice of basepoint $a_0$ is not canonical, so $\Gamma$ is well-defined only up to conjugacy.

Suppose we know that the ramification locus of some cover of $\mathbb{P}^1$ is contained in $a$. We would like to know when the ramification locus is actually all of $a$, rather than a proper subset; this is equivalent to asking when the cover has exactly $r$ branch points (as opposed to at most $r$ branch points). There is a group-theoretic criterion for this: Let $\Gamma_1 := \pi_1((\mathbb{P}^1 \setminus a) \cup \{ a_i \}, a_0)$ be the fundamental group of the punctured sphere obtained from $\Gamma$ by adding back in the point $a_i$. Now
a cover $\phi$ is ramified over all of the $a_i$ precisely when the corresponding conjugacy class $U_\phi$ does not contain the kernel of $\theta_i : \Gamma \to \Gamma_i$ for any $i$. This gives that

$$\text{Aut}(X/\mathbb{P}^1) \cong N_\Gamma(U_\phi)/U_\phi.$$ 

Define $H^{ab} := H_p^{ab}(G, U)$ to be the set of equivalence classes of cover $\phi$ of $\mathbb{P}^1$ with $r$ branch points, such that there exists a surjection $f : \Gamma \to G$ with $f^{-1}(U)$ conjugate to $U_\phi$. This set is in bijection with restrictions $\phi^0$ described earlier, so we can think of $H^{ab}$ as being represented by unramified covers $\phi^0$ of a Riemann sphere punctured at $r$ points.

**Remark 5.** There is a bit of ambiguity here about whether the data of the $f$ is included in the set $H^{ab}$. In this setting, it is not; in more modern treatments, the data being parameterized would be pairs $(\phi, f)$, rather than just $\phi$ such that there exists an $f$.

**Remark 6.** The ab subscript here does not stand for “abelian.”

Similarly, define $H^{in}(G) = H^{in}_p(G)$ to be the set of pairs $(\chi, h)$ where $\chi : \tilde{X} \to \mathbb{P}^1$ is a $G$ cover of $\mathbb{P}^1$ with $r$ branch points and $h : \text{Aut}(X/\mathbb{P}^1) \to G$ is an isomorphism. We say that $(\chi, h) \simeq (\chi', h')$ if there exists a $\delta : \tilde{X} \to \tilde{X}'$ such that $h' \circ C_\delta = h$, where $C_\delta : \text{Aut}(\tilde{X}/\mathbb{P}^1) \to \text{Aut}(\tilde{X}'/\mathbb{P}^1)$ is the map induced by $\delta$ on the automorphism groups.

Points in $H^{in}$ can be viewed either as pairs $(\chi, h)$ or as triples $(a, a_0, f)$ for $a, a_0$ as before and $f : \Gamma \to G$ a surjection not factoring through any of the $\Gamma_i$s. To express the above equivalence relation in terms of these triples, we say that $(a, a_0, f) \simeq (\tilde{a}, \tilde{a}_0, \tilde{f})$ if $a = \tilde{a}$ and there exists a path $\gamma : a_0 \to \tilde{a}_0$ that induces an isomorphism $\gamma^* : \pi_1(\mathbb{P}^1 \setminus a, a_0) \to \pi_1(\mathbb{P}^1 \setminus a, \tilde{a}_0)$ and such that $f = \tilde{f} \circ \gamma^*$.

### 5.3 Topological space structure on $H^{in}$

So far, $H^{in}$ has only been given the structure of a set. Next, we wish to endow it with a complex analytic topology. Note that this does not give an algebraic structure over $\mathbb{Z}$, as we will eventually want, but it does give a complex analytic structure to $H^{in}$.

To specify a topology on $H^{in}$, it suffices to describe the neighborhoods of any point in $H^{in}$. These points are the triples $(a, a_0, f)$. To describe a neighborhood $N$ of $(a, a_0, f)$, choose discs $D_i$ around $a_i$ and choose $a_0 \notin D_i$ for all $i$. $N$ consists of points $(\tilde{a}, \tilde{a}_0, \tilde{f})$ such that $\tilde{a}$ has exactly one point in each of the $D_i$s, and $\tilde{f}$ is a composition of $f$ with the isomorphisms

$$\pi_1(\mathbb{P}^1 \setminus \tilde{a}, a_0) \cong \pi_1(\mathbb{P}^1 \setminus (D_1 \cup \ldots D_r), a_0) \cong \pi_1(\mathbb{P}^1 \setminus a, a_0).$$

Next, want to consider the monodromy action on the fibers of $H^{in}$.

**Theorem 5.1.** With this topology, $H^{in} \xrightarrow{\psi} U_r$ is a covering space map, where $\psi(a, a_0, f) = (\text{polynomial with roots }\{a_1, \ldots, a_r\})$. And, equivalence classes of $(\chi, h)$ are in bijection with fibers $\psi^{-1}(b)$.

To prove the second statement: given $(\chi, h)$, define $f = h \circ \iota : \Gamma_0 \to G$, where $\Gamma_0 := \pi_1(\mathbb{P}^1 \setminus b, b_0)$, and associate to $f$ the class $(\sigma_1, \ldots, \sigma_r) = (f(\gamma_1, \ldots, \gamma_r))$ in $E_r^{\infty}$. This gives the desired bijection, since $f$ is determined up to composition with elements of $\text{Inn}(G)$. 

9

Main goal: Last week, we saw that the Hurwitz space of cover of $\mathbb{P}^1$ ramified over a specified number of points can be endowed with a complex-analytic structure. Today, we will upgrade that to endow Hurwitz spaces with the structure of a scheme over $\text{Spec}\mathbb{Z}$. This will allow us to count $\mathbb{F}_q$-points on the Hurwitz scheme, which is the counting problem that will give information about the distributions of class groups of global function fields.

6.1 Notation and setup

Throughout, let $\Gamma$ and $A$ be finite groups. (For the counting problems we care about, $A$ will be a class group, therefore abelian; however, today, the assumption that $A$ is abelian will never be necessary). Let $\Gamma$ act on $A$, and $G = A \rtimes \Gamma$ be the semidirect product with respect to this action. Assume that $(\#\Gamma, \#A) = 1$. We work over $\mathbb{F}_q$, where $(q, \#G) = 1$. Set $D = q^n$ for $n$ a fixed integer $\geq 1$. Let $Q := \mathbb{F}_q(t)$.

Let $N(A, \Gamma, D, Q)$ denote the number of surjections $Gal(Q/Q) \to G$ such that (1) the corresponding $G$-extension of $Q$, call it $K$, has $\text{Norm}(\text{radical}(\text{disc}(K/Q)) = D$, (2) the $A$-extension $K/K^A$ is unramified everywhere, and (3) $K/Q$ splits completely at infinity. Here, $K^A$ denotes the fixed field of the subgroup $A$ of $G$.

Note that $\text{rad}(\text{disc}(KQ))$ is the branch locus of the corresponding cover of $\mathbb{P}^1$, so specifying that the norm is equal to $D$ is equivalent to requiring that this cover be branched over precisely $n$ distinct points. To spell this out in more detail: the discriminant of $K/Q$ has as its divisors the points over which this cover ramifies. The discriminant may include some places with multiplicity. Taking the radical “forgets” the multiplicity of the ramification, but remembers the set of distinct points over which the cover is ramified. The norm of this radical, then, is $D := q^n$, so $n$ is the number of distinct ramification points.

Remark 7. $K/Q$ has tame ramification since $(q, \#G) = 1$. Furthermore, the inertia groups of the cover are all cyclic.

6.2 Constructing a moduli scheme

The motivation for constructing the Hurwitz scheme as a moduli space comes from the following lemma.

Lemma 6.1 \([lwzb]\)

$$\sum_{K \in E_r(D, Q)} |\text{surj}_\Gamma(Gal(K^\#/K)), A| = \frac{1}{[A: A^\Gamma]} N(A, \Gamma, D, Q)$$

where $K^\#$ is the maximal unramified extension of $K$ with degree prime to $\#\Gamma \cdot q \cdot (q - 1)$ and $E_r(D, Q)$ is the set of totally real $\Gamma$-extensions of $Q$ with $Nm(\text{rad}(\text{disc}(K))) = D$.

The upshot of this lemma is that to count the left hand side, which is the one we care about for determining distributions of class groups, it suffices to count the right hand side. The strategy for doing this is to construct a suitable moduli space, whose number $\mathbb{F}_q$-points correspond to totally real $G$-extensions of $Q$ ramified at precisely $n$ places.

More precisely: the goal is to construct a moduli scheme $\text{Hur}^n_{G, c}$, smooth over $\text{Spec}\mathbb{Z}[[G^{-1}]]$, called the Hurwitz scheme, such that $\#\text{Hur}^n_{G, c}(\mathbb{F}_q) = N(A, \Gamma, D, Q)$ and such that for all connected components $Y$ of $\text{Hur}^n_{G, c}$, we have the comparison theorem

$$\dim H^1(Y_{\mathbb{F}_q}, \mathbb{Q}_\ell) = \dim H^{2n-1}(Y_{\mathbb{C}}, \mathbb{Q}).$$
Furthermore, we want that $\text{Hur}_{G,c}^n$ be “close to” the complex-analytic Hurwitz space described in the last talk.

Next, we establish some notation:

- $S$ is a scheme.
- A curve over $S$ is a smooth proper morphism $X \to S$ whose geometric fibers are all connected curves.
- A Galois cover of $X$ is a commutative diagram $Y \xrightarrow{f} X \xrightarrow{p} S$ for $f$ a finite flat surjective separable morphism, such that $\text{Aut} f$ acts transitively on the fibers of $f$.
- The branch locus $D \subset X$ is the effective Cartier divisor with property that $f$ is étale over $X \setminus D$ and $X \setminus D$ is maximal with respect to this property. If $\deg D = n$, then we say that $f$ has $n$ branch points.
- A cover is said to be tame if the ramification index at any geometric point is prime to the characteristic of the residue field.
- $c \subset (G \setminus \{1\})$ is the set of nontrivial elements of $G$ which have the same order as their image in $\Gamma$ under the projection $G = A \rtimes \Gamma \to \Gamma$.

Define a functor $\text{Hur}_{G,c}^n : \text{Sch} \to \text{Set}$ such that

$$\text{Hur}_{G,c}^n(S) = \{\text{isomorphism classes of triples } (f, \iota, p)\}$$

where $f : X \to \mathbb{P}^1_S$ is a tame Galois cover; $\iota : \text{Aut} f \to G$ is a fixed isomorphism of $\text{Aut} f$ with $G$; and $p : S \to X$ is a marked point in $X(S)$ making the following diagram commute:

Here, the map $\infty$ means the map sending $S$ to the point at infinity in $\mathbb{P}^1_S$.

Now, we are set up to define/state the existence of the Hurwitz scheme:

**Theorem 6.2.** [LWZB] $\text{Hur}_{G,c}^n$ is representable by a scheme, called the Hurwitz scheme. Furthermore, $\text{Hur}_{G,c}^n \to \text{Conf}^n(\mathbb{A}^1)$ is finite étale over $\text{Conf}^n(\mathbb{A}^1)$, that is, the map is finite étale away from primes dividing the order of $G$.

As for why one might expect this theorem to hold: the triples $(f, \iota, p)$ have no nontrivial automorphisms. Typically, the obstruction to a functor’s being representable by a scheme is the existence of nontrivial automorphisms of the objects. As a general philosophy, one should expect that moduli problems whose objects have nontrivial automorphisms are representable by stacks, and those without nontrivial automorphisms are representable by schemes. Of course one has to prove this in every case, but this is an idea of the behavior one should generically expect from one’s moduli spaces.
6.3 Counting points

Next up is to count $\mathbb{F}_q$-points of this Hurwitz scheme. There exists a bijection

\[ \text{Hur}_{G,c}^n(\mathbb{F}_q) \iff \{ \varphi : \text{Gal}(\overline{\mathbb{F}_q(t)}/\mathbb{F}_q(t)) \to G \}. \]

Fix an embedding

\[ \mathbb{F}_q(t) \to \mathbb{F}_q(t)_{\infty} \]

where $\mathbb{F}_q(t)_{\infty}$ is the completion of $\mathbb{F}_q(t)$ at the place at infinity. The point $p \in X(\mathbb{F}_q)$ associated to a cover $f$ gives a unique embedding $\psi : k(X) \to \mathbb{F}_q(t)_{\infty}$. Set $M = \text{im} \psi$ to get an isomorphism $\text{Gal}(M/\mathbb{F}_q(t)) \cong \text{Gal}(k(X)/\mathbb{F}_q(t))$. Now consider the following commutative diagram:

\[
\begin{array}{ccc}
\text{Gal}(\mathbb{F}_q(t)/\mathbb{F}_q(t)) & \longrightarrow & \text{Gal}(M/\mathbb{F}_q(t)) \\
\uparrow & & \downarrow \cong \\
\varphi & \longrightarrow & \text{Gal}(k(X)/\mathbb{F}_q(t))
\end{array}
\]

The claim here is that there exists a unique vertical left arrow making the diagram commute.

To count the $\mathbb{F}_q$-points, we want to understand the Frobenius action on $\mathbb{F}_q$-points of the Hurwitz space. Then we will use the fact that $\mathbb{F}_q$-points are precisely $\mathbb{F}_q$-points fixed by the action of Frobenius.

**Lemma 6.3.** ([LWZB, Lemma 11.8] For any $q$ such that $(q, \#G) = 1$, the $\mathbb{F}_q$-points of $(\text{Hur}_{G,c}^n)_{\overline{\mathbb{F}_q}}$ correspond to triples $(f, \iota, p)$ where $f : X \to \mathbb{P}^1_{\mathbb{F}_q}$ is a cover; $p : \text{Spec} \mathbb{F}_q \to X$; and $\iota : \text{Aut} f \to \text{sim} G$. The action of Frobenius on these points takes $(f, \iota, p)$ to $(f^F, \iota^F, p^F)$ where $F : \text{Spec} \mathbb{F}_q \to \text{Spec} \mathbb{F}_q$ is induced by the map $x \mapsto x^q$ on $\mathbb{F}_q$, and $X^F, f^F, p^F$ are the base change of the original maps along Frobenius.

# 7 Algebraic lifting invariant 1: Zixin Jiang. October 16.

The purpose of this talk is to introduce a lifting invariant of curves over an algebraically closed field $k$ admitting a map to $\mathbb{P}^1_k$. This invariant was introduced by Ellenberg, Venkatesh and Westerland. This talk covers sections 2-3 of [MW]. The proofs of all the statements in this lecture are available in that paper, so they’ll be omitted here. Instead, we’ll focus on understanding the motivation for the statements and their geometric interpretation. For this week, everything will be done over an algebraically closed field; the non-algebraically-closed case will be done next week.

Here’s the main idea: given a tame map of curves $C \to \mathbb{P}^1$ with Galois group $G$, one can define an invariant of $G$ by giving the multiset of conjugacy classes of cyclic subgroups of the inertia groups of the map. Equivalently, one can think of this as the multiset of cyclic subgroups of monodromy around the ramification points. The invariant defined here will refine this multiset of conjugacy classes.

## 7.1 Components of Hurwitz schemes and the lifting invariant

First we set up some notation. Throughout, $G$ is a finite group and $c$ is a set of nontrivial elements of $G$, which is closed under conjugation by elements of $G$ and which generates $G$. The elements of $c$ should be thought of as generators for the cyclic subgroups of the monodromy around ramification points of a map from a curve to $\mathbb{P}^1$. The fact that the elements of $c$ generate $G$ indicates that the cover is connected.
7.2 More on the lifting invariant

Define the group $U(G, c)$, which is the group in which the lifting invariant is valued, by the presentation with generators $[g]$ for $g \in c$ and relations $[x][y][x^{-1}] = [xyx^{-1}]$ for $x, y \in c$. Let $V_n$ denote the set of all tuples $(g_1, \ldots, g_n)$ with $g_i \in c$. The brain group $B_n$ is the group with generators $\sigma_i$ for $1 \leq i < n$ and relations $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ for $1 \leq i < n - 2$ and $\sigma_i = \sigma_j$ for $|i - j| \geq 2$. $B_n$ acts on $V_n$ as

$$\sigma_i(g_1, \ldots, g_n) = (g_1, \ldots, g_{i-1}, g_i g_{i+1} g_i^{-1}, g_i, g_{i+2}, \ldots, g_n).$$

That is to say, $B_n$ acts on the set of ramification points of a cover by exchanging the $i$th and $(i + 1)$st ramification points.

Write $\text{Conf}^n \mathbb{C}$ for the Configuration space of $n$ points in $\mathbb{C}$, that is, the quotient of $\mathbb{C}^n$ minus the fat diagonal by the natural $S_n$ action. It is well-known that $\pi_1(\text{Conf}^n \mathbb{C}) = B_n$. Define a Hurwitz space $\text{Hur}^n_{G,c}$ to be the covering space of $\text{Conf}^n(\mathbb{C})$ whose fiber is $V_n$ with the action of $\pi_1(\text{Conf}^n(\mathbb{C}))$ given above. By definition, the components of $\text{Hur}^n_{G,c}$ correspond to $B_n$ orbits of $V_n$. We want to use the group structure of $U(G, c)$ to understand these connected components.

There is a map of sets $\Pi : V_n \to U(G, c)$ taking $(g_1, \ldots, g_n)$ to $[g_1] \ldots [g_n]$, and this map is constant on braid group orbits. Therefore it induces a map $V_n/B_n \to U(G, c)$. By composition, there is a map $V_n/B_n \to \mathbb{Z}^D$, where $D$ is the number of conjugacy classes of elements of $c$. The following theorem ([MW, Theorem 3.1]) gives that when there are enough elements of each conjugacy class, $U(G, c)$ exactly detects the braid group orbits.

**Theorem 7.1.** Let $G, c$ be as above. Then there is a constant $M$ such that $\Pi$ gives a bijection between the elements of $V_n/B_n$ and $U(G, c)$ whose coordinates in $\mathbb{Z}^D$ are all at least $M$.

Now that we know that $U(G, c)$ exactly detects braid group orbits (at least when each conjugacy class has enough elements), we know that it tells us about the components of the relevant Hurwitz scheme. Therefore we want to study some other ways of understanding this group, which will be discussed in the next section.

7.2 More on the lifting invariant

In this section, I will state a lot of things and will prove none of them. The proofs can all be found in [MW], for any reader who is interested.

Let $D$ denote the set of conjugacy classes in $c$. There is a natural map $U(G, c) \to G$ sending $[g] \to g$, and a natural map $U(G, c) \to \mathbb{Z}^D$ sending $[g]$ to a generator for the conjugacy class of $g$. There is another map $\mathbb{Z}^D \to G^{ab}$ sending a generator for the conjugacy class of $[g]$ to the image of $g$ in the abelianization of $G$. Combining these two maps gives a morphism to the fiber product:

$$U(G, c) \to G \times_{G^{ab}} \mathbb{Z}^D.$$

**Lemma 7.2.** $U(G, c) \to G$ is a central extension. Moreover, if $x \in c$ and $y \in G$, with $\tilde{y}$ a preimage of $y$ in $U(G, c)$, then $\tilde{y}[x]\tilde{y}^{-1} = [xyx^{-1}]$.

Next, we want a more explicit expression for $U(G, c)$, which will be done in terms of Schur covers. Let $A$ any finite abelian group. Central extensions of $G$ by $A$

$$1 \to A \to \tilde{G} \to G \to 1$$

are parameterized by elements of $H^2(G, A)$. Universal coefficients gives an exact sequence

$$\text{Ext}^1(G^{ab}, A) \to H^2(G, A) \xrightarrow{\phi} \text{Hom}(H_2(G, \mathbb{Z}), A).$$

13
Write \( \tilde{G} \) for the class of the extension in \( H^2(G,A) \). Recall some definitions: A stem extension is a central extension such that the induced map on abelianizations is an isomorphism. For a finite group, a Schur covering is a stem extension of maximal possible order. In general, Schur covers are not unique; so, any time one uses a Schur cover, there is an additional annoyance of having to check that the construction does not depend on the choice of Schur cover.

To any Schur cover \( S \to G \), by definition there is associated an isomorphism \( \pi(S) : H_2(G,\mathbb{Z}) \to \ker(S \to G) \). Let \( x,y \in G \) be two commuting elements. Let \( \hat{x},\hat{y} \) be lifts of \( x,y \) to \( S \). Then the commutator \( [\hat{x},\hat{y}] \) lies in \( \ker(S \to G) \) by the assumption that \( x \) and \( y \) commute. And, the image of the commutator in \( \ker(S \to G) \) is independent of the choice of lifts. One can check that \( \pi(S)^{-1}([\hat{x},\hat{y}]) \in H_2(G,\mathbb{Z}) \) is independent of the choice of Schur cover. Denote this element \( \langle x,y \rangle \in H_2(G,\mathbb{Z}) \).

**Definition 3.** Let \( H_2(G,c) \) be the quotient of \( H_2(G,\mathbb{Z}) \) by the subgroup \( Q_c \subset H_2(G,\mathbb{Z}) \) generated by all elements of the form \( (x,y) \) for \( x \) and \( y \) commuting and \( x \in c \). Given \( G \) and \( c \), define a reduced Schur cover \( S_c \to G \) as the quotient of a Schur cover \( S \to G \) by \( \pi(S)(Q_c) \). For any Schur cover \( S_c \), we have that \( \pi(S_c) : H_2(G,\mathbb{Z}) \to \ker(S_c \to G) \) is an isomorphism. A reduced Schur cover need not be unique (as for Schur covers).

Given a reduced Schur cover \( S_c \), define a new group \( \widehat{G} = S_c \times_{G^{ab}} \mathbb{Z}^D \).

**Lemma 7.3.** Let \( G,c \) as above. Let \( S_c \) be a reduced Schur cover for \( G,c \) and \( \widehat{G} \) as defined above. Then \( \widehat{G}^{ab} = \mathbb{Z}^D \).

Next, we will prove that \( \widehat{G} \) is a more explicit version of the group \( U(G,c) \):

**Theorem 7.4.** Pick lifts of the elements of \( c \) to \( S_c \). Then there is an isomorphism \( \widehat{G} \to U(G,c) \) taking \( (\hat{x},e_x) \) to \([x]\) for \( x \in c \), where \( e_x \) is a generator corresponding to the conjugacy class of \( x \) and \( \hat{x} \) is a lift of \( x \) to \( S_c \).

The upshot of this theorem is that \( \widehat{G} \) is independent of the choice of Schur cover. This allows us to use this more explicit version of \( U(G,c) \) to study the group’s behavior, which will in turn allow us to compute information about the connected components of the Hurwitz scheme \( \text{Hur}^n_{G,c} \).


Let’s first recall the setup and motivation from last lecture. Notation: \( G \) is a finite group. \( c \subset G \setminus \{1\} \) is a set of nontrivial elements of \( G \) closed under conjugation by \( G \) such that the elements of \( c \) generate \( G \). The elements of \( c \) should be thought of as generators for inertia groups of ramified \( G \)-covers of \( \mathbb{P}^1 \). (These are really conjugacy classes, and represent monodromy groups around ramification points.) \( V_n \) is the set of all \( n \)-tuples \((g_1,\ldots,g_n)\) of elements of \( c \). These represent degree \( n \) \( G \)-covers of \( \mathbb{P}^1 \) whose ramification groups are all generated by elements of \( c \). \( B_n \) denotes the braid group on \( n \) generators, where the \( i \)th generator \( \sigma_i \) acts on the set of branch points by exchanging the \( i \)th and \((i+1)\)st branch points. \( \text{Hur}^n_{G,c} \) is the covering space of \( \text{Conf}^n \mathbb{C} \) with fiber \( V_n \). \( \pi_1(\text{Conf}^n \mathbb{C}) \cong B_n \), so \( B_n \) acts on the fibers of our Hurwitz space.

Our main goal is to understand the components of this Hurwitz space \( \text{Hur}^n_{G,c} \). By definition, these components are in bijection with braid group orbits on \( V_n \). Last time, we defined a group

\[
U(G,c) := \langle [g] : g \in c \rangle / \langle [x][y][x^{-1}] = [xyx^{-1}] : x,y \in c \rangle
\]

and showed that if each conjugacy class in \( c \) contains sufficiently many elements from \( V_n \), then \( U(G,c) \) exactly detects braid group orbits.
Therefore it of interest to us to understand the group \( U(G, c) \) explicitly. In the last lecture, we did this using Schur covers and reduced Schur covers. This interpretation will be important in a technical point later on today.

The group \( U(G, c) \) will almost be the target of the lifting invariant. But, \( U(G, c) \) does not naturally come equipped with an action of the automorphism group of the base field, and we would like the lifting invariant to admit such an action. Therefore the right target of the lifting invariant will not be \( U(G, c) \) itself, but rather a certain twist of it, which will be constructed in the next section.

8.1 Defining the target of the lifting invariant

Some motivation: over \( \mathbb{C} \), one can pick explicit generators for the inertia group at any point by choosing a loop around it, and orienting that loop. This gives a distinguished generator for the monodromy around that point, or equivalently for the inertia at the point. Over other fields, though, we don’t have a way of choosing this distinguished generator: we have an entire conjugacy class of possible generators of inertia, and no way of distinguishing one of them from any of the others. All these generators will differ by some root of unity, so saying that there’s no distinguished generator for inertia is equivalent to saying that we have no way of picking out a favorite root of unity in fields other than \( \mathbb{C} \). Therefore, in the data of the lifting invariant, we want to package the data of all possible generators of inertia. That is, we want to know where one generator is, and then how all the roots of unity act on that generator, which tells us what all the other possible generators are. Most of the work today will be necessary to package all this information together, and fix the problem of not having a distinguished root of unity.

Throughout, let \( k = \overline{k} \). The lifting invariant will be valued in a twist of \( U(G, c) \) by a powering action of the pro-prime-to-char \( k \) completion of \( \mathbb{Z} \), which is set up as follows.

Define \( \hat{\mathbb{Z}}(1)_k = \varprojlim \mu_m(k) \) and \( \hat{\mathbb{Z}}_k = \varprojlim \mathbb{Z}/m\mathbb{Z} \), where \( m \) ranges over all positive integers prime to \( \text{char } k \). \( \hat{\mathbb{Z}}(1)_k^\times \) denotes the subset of topological generators for \( \hat{\mathbb{Z}}(1)_k \). It is a torsor for \( \hat{\mathbb{Z}}_k \), the units of \( \hat{\mathbb{Z}}_k \).

Remark 8. The group \( \hat{\mathbb{Z}}(1)_k^\times \) will later turn out to be the maximal prime-to-char \( k \) quotient of the étale fundamental group of a disk. Therefore locally around a ramification point in \( \mathbb{P}^1 \), the action of this group on \( U(G, c) \) will describe the monodromy action around the point, which is why we want to endow the \( U(G, c) \) with an action by \( \hat{\mathbb{Z}}_k^\times \).

Next step: endow \( U(G, c) \) with an action of \( \hat{\mathbb{Z}}_k^\times \) to get the desired twist.

We begin with some generalities on sets with an action of \( \hat{\mathbb{Z}}_k^\times \). For a set \( X \) with such an action, define

\[ X \left\langle -1 \right\rangle_k := \text{Mor}_{\hat{\mathbb{Z}}_k^\times} (\hat{\mathbb{Z}}(1)_k^\times, X) \]

which is the set of morphisms of sets \( \hat{\mathbb{Z}}(1)_k^\times \to X \) which are equivariant with respect to the \( \hat{\mathbb{Z}}_k^\times \) actions on both sides.

Let \( G \) be a finite group and let \( c \subset G \) be a subset of elements of \( G \) which is closed under conjugation by elements of \( G \) and which is closed under invertible powering (that is, if \( (m, \text{ord}(g)) = 1, \text{then } g \in c \implies g^m \in c \)). Write \( D \) for the set of conjugacy classes in \( c \). Assume that \( \text{char } k \nmid G \).

Note that \( \hat{\mathbb{Z}}_k \) acts on the underlying set of elements of \( G \), where \( \{\alpha_m\} \in \hat{\mathbb{Z}}_k \) takes \( g \to g^{\text{ord}(g)} \). This action induces an action on conjugacy classes, i.e. \( \hat{\mathbb{Z}}_k \) acts on \( D \), and therefore by composition \( \hat{\mathbb{Z}} \) acts on \( \mathbb{Z}^D \). In fact, \( \hat{\mathbb{Z}}_k \) acts in this way on any profinite group prime to \( \text{char } k \). This is called the powering action.
Let \( \hat{U}_k(G,c) \) denote the pro-prime-to-char \( k \) completion of \( U(G,c) \). There is an action of \( \hat{Z}_k^\times \) on \( \hat{U}_k(G,c) \) defined by

\[
\alpha \cdot [g] = [g^{\alpha}^{-1}]^\alpha
\]

for \( \alpha \in \hat{Z}_k^\times \). This is an action on \( \hat{U}_k(G,c) \) as a group; next, we will define a related action of \( \hat{Z}_k^\times \) on \( \hat{U}_k(G,c) \) as a set:

\[
\alpha \ast v = (\alpha^{-1} \cdot v)^\alpha
\]

for \( v \in \hat{U}_k(G,c) \) and \( \alpha \in \hat{Z}_k^\times \).

**Remark 9.** The odd-looking definition of the action above is an artifact of the proof that the lifting invariant is well-defined; that is, this is the action necessary for the lifting invariant, valued in \( U(G,c)(-1) \), associated to a cover of \( \mathbb{P}^1 \), to be independent of all the choices made (these choices will be described later on).

**Lemma 8.1.** The action of \( \hat{Z}_k^\times \) on \( \hat{U}_k(G,c) \) actually gives an action on the set \( U(G,c) \).

**Proof.** The idea is as follows. First, we will prove that \( U(G,c) \) is a subset of \( \hat{U}_k(G,c) \), and that the natural map is injective. Then it suffices to prove that the \( \hat{Z}_k^\times \) action on \( \hat{U}_k(G,c) \) to itself. We will do this by understanding the image of \( U(G,c) \) in \( \hat{U}_k(G,c) \) using the description in terms of reduced Schur covers given in the last lecture. Then we will show explicitly that the action of \( \hat{Z}_k^\times \) preserves this subset.

Recall that \( U(G,c) \cong S_c \times_{G^{ab}} \mathbb{Z}^D \) for \( S_c \) a reduced Schur cover of \( G \). Any prime not dividing \( \#G \) also does not divide \( S_c \) so any finite index normal subgroup of \( U(G,c) \) contains \( 1 \times (m\mathbb{Z})^D \) for some \( m \), and \( \hat{U}_k(G,c) \cong S_c \times_{G^{ab}} (\hat{Z}_k)^D \). Therefore we see that the natural map \( U(G,c) \to \hat{U}_k(G,c) \) is injective, and its image consists of precisely the elements of \( \hat{U}_k(G,c) \) whose image under the projection to \( \hat{Z}_k^D \) actually lies in \( \mathbb{Z}^D \).

Next, wish to show that the action of \( \hat{Z}_k^\times \) preserves this subset of \( \hat{U}_k(G,c) \).

The projection morphism \( \hat{U}_k(G,c) \to \hat{Z}_k^D \) is equivariant for the \( \hat{Z}_k^\times \) action, where \( \hat{Z}_k^\times \) acts on \( \hat{U}_k(G,c) \) via the action \( \ast \) defined above and \( \hat{Z}_k^\times \) acts on \( \hat{Z}_k^D \) by the powering action. That is, the following diagram commutes:

\[
\begin{array}{ccc}
\hat{U}_k(G,c) & \longrightarrow & (\hat{Z}_k)^D \\
\downarrow^{\alpha} & & \downarrow^{\alpha} \\
\hat{U}_k(G,c) & \longrightarrow & (\hat{Z}_k)^D
\end{array}
\]

The powering action preserves \( \mathbb{Z}^D \subset \hat{Z}_k^D \), so the action by \( \hat{Z}_k^\times \) preserves \( U(G,c) \subset \hat{U}_k(G,c) \). \qed

This action of \( \hat{Z}_k^\times \) on \( U(G,c) \) is called the discrete action. Write \( U(G,c)(-1) \) for the twisting of \( U(G,c) \) by the discrete action. This gives the desired target of the lifting invariant, whose definition will be discussed in the next section.

### 8.2 Definition of the lifting invariant

First, we make precise the objects on which the lifting invariant will be defined.

Let \( S \) any scheme. A curve over \( S \) is a smooth proper map \( X \to S \) such that all the geometric fibers are connected of dimension 1. A cover of a curve \( X \) over \( S \) is a finite flat surjective map \( Y \to X \) of \( S \)-schemes, with \( Y \) also a curve over \( S \).

A cover \( f : Y \to X \) is Galois if it is separable and \( \text{Aut} f \) acts transitively on the fibers of \( f \). Associated to \( f \) is the branch locus \( D \subset Y \), satisfying the following properties:
8.2 Definition of the lifting invariant

1. $D \to S$ is étale.
2. $f \mid_{Y \setminus D}: Y \setminus D \to X$ is étale.
3. $Y \setminus D$ is maximal with respect to the previous property.

If there exists a constant $n$ such that the degree of each geometric fiber of $D \to S$ has degree $n$ (which is automatic if $S$ is connected), then we say that $f$ has $n$ branch points. $f$ is said to be tame if the ramification index at any point is prime to the characteristic of the residue field at that point.

**Definition 4.** A marked, branched $G$-cover of $\mathbb{P}^1$ over $S$ is a tame Galois cover $X \to \mathbb{P}^1_S$ with $n$ branch points, together with an identification of $G$ with $\text{Aut}(f)$ and a section $P: S \to X$ over the standard infinity section $s_\infty: S \to \mathbb{P}^1_S$, where we also require $\text{im } s_\infty$ disjoint from the branch locus of the cover.

The requirement stated above on the sections means that there exists a section $P: S \to X$ of the structure morphism of $X$ such that the following diagram commutes:

```
S \quad P
\downarrow_{s_\infty} \quad \downarrow_{\text{structure}}
\mathbb{P}^1_S \quad \quad \quad \quad \quad \quad \quad X
```

8.2.1 Inertia groups

The completion of $k(z)$ with respect to the discrete valuation associated to $z$ is the field of Laurent series $k((z))$. The maximal prime-to-char $k$ extension of $k((z))$ is the field of Puiseaux series $k((z^{1/\infty}))$, generated by $z^{1/m}$ for $\text{char } k \nmid m$. We have

$$\text{Gal}(k((z^{1/\infty}))/k((z))) \cong \hat{\mathbb{Z}}(1)_k$$

via the map $\sigma \mapsto \{\sigma_m\}$, where $\sigma_m = \sigma(z^{1/m})/z^{1/m}$, which is an $m$th root of unity. Recall that we defined an action of $\mathbb{Z}(1)_k^\times$ on $U(G,c)$. The above isomorphism of Galois groups tells us that $\hat{\mathbb{Z}}(1)_k$ is in fact the Galois group of the maximal prime-to-char $k$ extension of the $z$-adic completion of a function field of $\mathbb{P}^1_k$.

Let $K$ be any prime-to-char $k$ extension of $k(t)$. For $t_0 \in k$, letting $z = t - t_0$ gives a $\text{Gal}(K/k(t))$-conjugacy class of homomorphisms $\text{Gal}(k((z^{1/\infty}))/k((z))) \to \text{Gal}(K/k(t))$, corresponding to the homomorphisms $K \to k((z^{1/\infty}))$ respecting $k(t)$. This gives a conjugacy class of homomorphisms

$$r_{t_0}: \hat{\mathbb{Z}}(1)_k \to \text{Gal}(K/k(t))$$

coming from $t_0$. The images of this conjugacy class of homomorphisms are the isomorphism groups of $t_0$ (where $t_0$ is viewed as a point of $\mathbb{P}^1_k$).

8.2.2 Generators for $\pi_1$

Let $U \subset \mathbb{P}^1_k$ be an open subset including $\infty$. Denote by $\pi'_1(U,\infty)$ the maximal prime-to-char quotient of $\pi_1(U)$ with basepoint at infinity. Equivalently, $\pi'_1(U,\infty)$ is the Galois group of the maximal prime-to-char extension of $k(t)$ unramified at all points of $U$.

Write $t_1, \ldots, t_n$ for the $k$-pints of $\mathbb{P}^1 \setminus U$. By Grothendieck’s comparison of étale and topological $\pi_1$, $\pi'_1(U,\infty)$ contains elements $\gamma_j$ with the property that the product $\gamma_1 \cdots \gamma_n = 1$ and the $\gamma_1, \ldots, \gamma_n$
topologically generate the inertia groups at \( t_1, \ldots, t_n \), that is, they are equal to \( r_{t_i}(\gamma_i) \) for some \( \gamma_i \in \hat{\mathbb{Z}}(1)_k \). Furthermore, \( \pi'_1(U, \infty) \) is free as a prime-to-\( k \) profinite group on the generators \( \gamma_1, \ldots, \gamma_{n-1} \).

**Remark 10.** The existence of such \( \gamma_i \) is what motivates our definition of the set \( c \) of elements of \( G \). Indeed, the stated conditions on \( c \) are precisely those given by these \( \gamma_i \)'s, which means that we can use our construction of \( U(G, c) \) to study the covers of \( \mathbb{P}^1 \) which have inertia groups generated by \( \gamma_i \) and which have exactly \( n \) ramification points.

Upshot: \( \pi'_1(U, \infty) \) can be generated by the inertia groups around the punctures in the punctured sphere \( U \). The fact that the product of the \( \gamma_i \)'s is 1 corresponds to all the corresponding covers of \( \mathbb{P}^1 \) being unramified over \( \infty \).

We now want to describe the \( \xi_i \)'s. Consider the action of the \( \xi_i \) on the extension

\[
\kappa(t, \sqrt{t-t_1}/(t-t_2), \sqrt{t-t_2}/(t-t_3), \ldots, \sqrt{t-t_n}/(t-t_1)).
\]

We find that \( \gamma_i \cdots \gamma_n = 1 \) implies that the \( \xi_i \) are all equal. To see this: note that \( \gamma_i \) sends \( \sqrt{t-t_j} \) to \( \xi_i \sqrt{t-t_j} \). This means that \( \gamma_i \cdots \gamma_n \) acts on \( \sqrt{t-t_1}/(t-t_2) \) by multiplication by \( \xi_i \xi_j^{-1} \), and on \( \sqrt{t-t_i}(t-t_{i+1}) \) by multiplication by \( \xi_i \xi_j^{-1} \). Since this product must act trivially, this means that all the \( \xi_i \) are the same. It seems surprising that the one relation \( \gamma_1 \cdots \gamma_n = 1 \) implies that *all* the \( \xi_i \)'s are the same. But, one can note that the Galois group of this field extension over \( k(t) \) is \( (\mathbb{Z}/m\mathbb{Z})^{n-1} \) by Kummer theory, and the condition on the \( \xi_i \)'s is imposing a “1-dimensional” condition on this Galois group.

Write \( \gamma \) for the tuple \( \gamma_1, \ldots, \gamma_n \) and \( I(\gamma \in \hat{\mathbb{Z}}(1)_k) \) for the common value of the \( \gamma_i \)'s.

### 8.3 Definition of the lifting invariant

Let \( X \) be a branched, marked \( G \)-cover of \( \mathbb{P}^1_k \), let \( U \subset \mathbb{P}^1 \) be the complement of the branch locus, and let \( Y \subset X \) be the preimage of \( U \) in \( X \). The marked basepoint \( P \in Y \) makes \( (Y, P) \) a pointed Galois étale map, which gives a surjection \( \pi'_1(U, \infty) \to \operatorname{Aut}(Y \to U) \). Note that since we have fixed a basepoint, this is an actual surjection, not just a conjugacy class of surjections. Note that \( \operatorname{Aut}(Y \to U) = \operatorname{Aut}(X \to \mathbb{P}^1) \), so combining we get a surjection \( \pi'_1(U, \infty) \to G \).

**Theorem 8.2.** Let \( k \) be an algebraically closed field with \( \operatorname{char}(k) \neq 1 \). Let \( X \to \mathbb{P}^1_k \) be a branched marked \( G \)-cover and let \( U \subset \mathbb{P}^1 \) be the complement of the branch locus. Let

\[
\varphi : \pi'_1(U, \infty) \to G
\]

be the homomorphism associated to the cover. Assume that all inertia groups of the cover are generated by elements of \( c \). Then there exists a unique \( \xi \in \ker(U(G, c) \to G) \langle -1 \rangle \), called the lifting invariant of the cover, such that for any choice of the branch points \( t_1, \ldots, t_n \) and any choice of \( \gamma = \gamma_1, \ldots, \gamma_n \in \pi'_1(U, \infty) \) such that \( \gamma_i \) topologically generates the inertia group at \( t_i \) and \( \gamma_1 \cdots \gamma_n = 1 \), we have that \( \xi \) sends \( I(\gamma \in \hat{\mathbb{Z}}(1)_k) \) to

\[
Z(\gamma) := [\varphi(\gamma_1)] \cdots [\varphi(\gamma_n)] \in U(G, c).
\]

The action of \( \hat{\mathbb{Z}}(1)_k \) on \( \ker(U(G, c) \to G) \) is inherited from its action on \( U(G, c) \). This is well-defined because the map \( U(G, c) \to G \) is equivariant for the respective \( \hat{\mathbb{Z}}(1)_k \) actions, which acts on \( U(G, c) \) by \( \ast \) and on \( G \) by the powering action.

The content to this theorem is that the element \( \xi \) is independent of the choices of \( t_i \) and of \( \gamma_i \), provided that the \( \gamma_i \) satisfy the stated properties.
8.4 Properties of the lifting invariant

In this section, we will state 2 nice properties of the lifting invariant.

**Slogan 1:** The lifting invariant plays nice with field extensions.

More precisely:

**Lemma 8.3.** If \( \xi \) is the lifting invariant of \( X \) over \( k \) and \( \sigma : k \hookrightarrow K \) is an extension of algebraically closed fields, then \( X_K \) has lifting invariant \( \xi \circ \sigma^{-1} \).

**Slogan 2:** The lifting invariant is constant in flat families.

More precisely:

**Theorem 8.4.** Let \( S \) a scheme over \( \text{Spec } \mathbb{Z} \) such that for any geometric points of \( S \), the inertia groups of the associated cover are generated by elements of \( \mathcal{C} \). Let \( s_1, s_2 \) be geometric points of \( S \) such that the image of \( s_2 \) is in the closure of the image of \( s_1 \), and let \( k(s_i) \) be the algebraically closed field of \( s_i \). Then there exists a map of roots of unity \( \sigma : \hat{\mathbb{Z}}(1)_{k(s_1)} \rightarrow \hat{\mathbb{Z}}(1)_{k(s_2)} \) such that \( \xi_{X_{s_2}} = \xi_{X_{s_1}} \circ \sigma \). If \( S \) is a \( k \)-scheme for some algebraically closed field \( k \), then the \( \hat{\mathbb{Z}}(1)_{k(s_i)} \) are naturally identified with \( \hat{\mathbb{Z}}(1)_k \), and \( \sigma \) respects the identification.

9 Example: the 5-part of real quadratic fields for large \( q \): Sander Mack-Crane. November 6.

Main goal: compute the average 5-part of the class group of a totally real quadratic extension of \( \mathbb{F}_q(t) \).

Let \( \Gamma \) a finite group, \( H \) a finite abelian \( \Gamma \)-group (i.e., \( H \) is equipped with an action of \( \Gamma \)), such that \((|\Gamma|, |H|) = 1 \) and \( H^\Gamma = 1 \), i.e. \( H \) has no \( \Gamma \)-invariants. Then

\[
\lim_{N \to \infty} \lim_{q \to \infty} \frac{\sum_{n \leq N} \sum_{K \in E_\Gamma(q^n, \mathbb{F}_q(t))} |\text{surj}_\Gamma(Cl(K), H)|}{\sum_{n \leq N} |E_\Gamma(q^n, \mathbb{F}_q(t))|} = \frac{1}{|H|}.
\]

**Example.** \( \Gamma = \mathbb{Z}/2, \ H = \mathbb{Z}/5 \), with \( \Gamma \) acting on \( H \) by multiplication by \(-1 \). Now \( E_\Gamma(q^n, \mathbb{F}_q(t)) = \{ \text{totally real quadratic extensions of } \mathbb{F}_q(t) \text{ of discriminant } q^n \} \). This notation in general indicates the number of \( \Gamma \)-extensions of \( \mathbb{F}_q(t) \) with discriminant \( q^n \).

Note that \( |\text{surj}(A, \mathbb{Z}/5)| = |A[5]| - 1 \). This means that the above sum is measuring the average size of 5-torsion.

To prove this: Consider \( \text{Hur}^n_{G,c} \) where \( G = H \times \Gamma = D_5 \), with \( c \) the conjugacy class of reflections, i.e. elements whose order in \( G \) is the same as their order in the projection to \( \Gamma \).

For any \( n \geq 0 \),

\[ |\text{Hur}^n_{G,c}(\mathbb{F}_q)| = |H| \sum_{K \in E_\Gamma(q^n, \mathbb{F}_q(t))} |\text{surj}_\Gamma(Cl(K), H)|. \]

In particular, for \( H = 1 \), we have \( |\text{Hur}^n_{G,c}(\mathbb{F}_q)| = \#E_\Gamma \) since \( \#\text{surj}(Cl(K), 1) = 1 \).

This means that to compute the average size of the 5-part of class groups of totally real quadratic fields, it remains to count the number of \( \mathbb{F}_q \) points on \( \text{Hur}^n_{G,c} \).
Let $Y$ a connected component of Hur$_{G,c}^n$. Then $Y$ is smooth of dimension $n$. By the comparison theorem between étale and singular cohomology,

$$dimH^i_{\text{ét}}(Y_{\overline{F_q}}, \overline{\mathbb{Q}_\ell}) = dimH^i_{\text{sing}}(Y_{\mathbb{C}}, \mathbb{Q}).$$

Recall the following facts from the Riemann hypothesis for étale cohomology:

1. $|Z(\mathbb{F}_q)| = \sum (-1)^i \text{tr}(\text{Frob}_q|H^i_{c,\text{ét}}(Z))$.

2. The eigenvalues of $\text{Frob}_q$ on $H^i$ are $q^w$ Weil numbers for $w \leq i$.

3. When $\dim Z = n$, $\text{tr}(\text{Frob}_q|H^{2n}(Z)) = q^n \cdot |\{\text{Frobenius fixed } n\text{-dimensional components of } Z\}|$.

Combining these facts gives the following estimate:

$$|\text{Hur}_{G,c}^n(\mathbb{F}_q)| = q^n \cdot |\{\text{Frobenius fixed components}\}| + O(q^{n-1/2}).$$

To count points, we use the lifting invariant and $U(G,c)$, which were covered in the last 2 lectures. Recall that $U(G,c) = S \times_{G^{ab}} \mathbb{Z}^{D}$ where $S$ is a reduced Schur cover of $G$ and $D$ is the number of conjugacy classes in $c$.

For $G = D_5$ and $\Gamma = \mathbb{Z}/2$, $S \to \sim G$ and $S \to \sim \Gamma$, i.e. $\Gamma$ and $G$ are Schur trivial. Furthermore, $D = !$, i.e. $c$ has a single conjugacy class. This implies that $U(G,c) = D_5 \times \mathbb{Z}/2 \mathbb{Z}$.

For the definition of the lifting invariant, we refer to the previous lecture. Recall that the lifting invariant keeps track of components of $\text{Hur}_{G,c}^n$. There is a map

$$U(G,c) = G \times_{\mathbb{Z}/2} \mathbb{Z} \to G$$

$$\xi(I(\gamma)) \mapsto \varphi(\gamma_1) \ldots \varphi(\gamma_n) = \varphi(\gamma_1 \ldots \gamma_n) = \varphi(id) = 1,$$

that is, the lifting invariant is always trivial on the $G$-component of $U(G,c)$. This means that the lifting invariant always has the form $(1, n)$ in the fiber product.

Furthermore, lifting invariants in $D_5 \times \mathbb{Z}/2 \mathbb{Z}$ are $(1, n)$ for $n$ even. This holds because $1 \in D_5$ maps to the trivial element in the abelianization $D_5^{ab} = \mathbb{Z}/2$, so $n \in \mathbb{Z}$ must also map to $0$ in $\mathbb{Z}/2$. Therefore the number of (Frobenius-fixed) components of $\text{Hur}_{G,c}^n$ is $1$ if $n$ even and $0$ if $n$ odd. Note that in the case $n$ odd, a component of $\text{Hur}_{G,c}^n$ would correspond to a degree $2$ cover of $\mathbb{P}^1$ with an odd number of branch points, which does not exist.

By a previous theorem,

$$|\text{Hur}_{G,c}^n(\mathbb{F}_q)| = q^n + O(q^{n-1/2}).$$

Therefore, the average 5-part of a real quadratic extension of $\mathbb{F}_q(t)$ is

$$\lim_{N \to \infty} \lim_{q \to \infty} \frac{\sum_{n \leq N} \sum_{K \in E^q(n^5,F_q(t))} \text{surj}_{\Gamma}(Cl(K), \mathbb{Z}/5)}{\sum_{n \leq N} |E_{\Gamma}(q^n, F_q(t))|}$$

$$= \frac{1}{5} \sum_{n \leq N} |\text{Hur}_{G,c}^n(\mathbb{F}_q)|$$

$$= \lim_{N \to \infty} \sum_{n \leq N} \left|\text{Hur}_{\Gamma,\Gamma \setminus 0(\overline{\mathbb{F}_q})}\right|$$

$$= \lim_{N \to \infty} \frac{1}{5} q^N + O(q^{N-1/2}) = \frac{1}{5}.$$
There is a problem with the previous lecture: computing dimensions of these cohomology groups exactly is hard. What we’ll try to do instead is work to get bounds on how fast these dimensions can grow. The main tool for obtaining such bounds comes from homological stability, and the source of all the results stated is [EVW]. Our main goal is to understand the following theorem:

[EVW, Thm 1.2] Let \( \ell > 2 \) be a prime, \( A \) a finite abelian \( \ell \)-group, and \( E_n \) be the set of imaginary quadratic extensions of \( \mathbb{F}_q(t) \) is discriminant degree \( n + 1 \). Then

\[
\lim_{q \to \infty} \lim_{N \to \infty} \sup_{n \leq N} \frac{\sum \{ L \in E_n : Cl(L)_\ell \cong A \}}{\sum_{n \leq N} \#E_n}
= \lim_{q \to \infty} \lim_{N \to \infty} \inf_{n \leq N} \frac{\sum \{ L \in E_n : Cl(L)_\ell \cong A \}}{\sum_{n \leq N} \#E_n}
= \prod_{i \geq 1} (1 - \ell^{-i}) \left| \text{Aut} A \right|.
\]

The upshot of this theorem is that we want to be able to reverse the order of limiting \( q \) and \( N \). We can’t reverse the orders with impunity, but this theorem gives us a version that is close enough. The one difference in this and Sander’s lecture on the 5-part of real quadratic fields is that in this theorem, the cover is assumed imaginary, i.e. ramified over \( \infty \).

We will show that \( E_N \) grows exponentially in \( N \), so that we can replace \( \sum_{n \leq N} \) with \( n = N \). Fix \( q, \ell \) with \( \ell \) a prime not dividing \( q \), and \( A \) a finite abelian \( \ell \)-group. Set \( G = A \rtimes \mathbb{Z}/2 \) where the nontrivial element of \( \mathbb{Z}/2 \) acts as \( -1 \). Let \( c \) denote the set of reflections, so \( c = \{(a, 1) : a \in A\} \subset G \).

**Proposition 10.1.** [EVW, Prop 2.5] \( \text{Hur}^{\ell}_G,c(C) \) is homeomorphic to a CW complex with \( (2|G|)^n \) cells.

This gives a crude bound on the dimension of homology groups. It is obviously a better bound when \( n \) is small, so our goal will be to use this bound for small \( n \) (with an appropriate definition of “small”), then use homological stability to get a similar bound for large \( n \).

**Theorem 10.2.** Let \( k \) a field such that \( |G|^{-1} \in k \). Then there exist constants \( a, b, D \) such that there is a map

\[
U : H_i(\text{Hur}^{\ell}_G,c(C),k) \to H_i(\text{Hur}^{\ell+D}_G,c(C),k)
\]

which is an isomorphism for all \( n, i \) such that \( n > ai + b \).

This theorem is the desired homological stability result for large \( n \). (The construction of the morphism \( U \) is part of the content of the theorem; the structure of the map is not a priori obvious.) This homological stability theorem will be used to bound the Betti numbers, i.e. \( \dim H_i(\text{Hur}^{\ell}_G,c) \) for large \( n \) as a function of \( i \), i.e. independent of \( n \).

**Proposition 10.3.** There exists a constant \( G(G,c) \) such that

\[
\dim H^{i \text{\acute{e}t}}_i(\text{Hur}^{\ell}_G,c,\mathbb{Q}_p) \leq C(G,c)^{i+1}
\]

for all \( n, i \) and \( p > \max\{|G|, n, q\} \). In particular, this bound is exponential in \( i \) but independent of \( n \).
Proof. For all \( n \), there exists an \( n' < ai + b \) such that

\[
H_i(Hur^n_{G,c}(\mathbb{C}), \mathbb{Z}/p) \cong H_i(Hur^n'_{G,c}(\mathbb{C}), \mathbb{Z}/p) \leq (2|G|)^{n'}
\]

where the last inequality is from Prop 2.5. Consider the following commutative diagram, where the middle column is an \( S_n \) cover of the left hand column, and the rightmost column is a projectivization of the center one:

\[
\begin{array}{ccc}
\text{Hur}_n^{G,c} & \xrightarrow{S_n} & \text{Hur}_n^{G,c} \\
\downarrow G & & \downarrow \\
\text{Conf}_n & \xrightarrow{S_n} & \text{Conf}_n
\end{array}
\]

The middle term represents the ordered configuration space and ordered Hurwitz space.

We can compare cohomologies of the compactified spaces. Want that

\[
H^i_\text{ét}(\text{Hur}_n^{G,c}, \mathbb{Z}/p) \cong H^i_\text{ét}(\text{Hur}_n^{G,c}(\mathbb{C}), \mathbb{Z}/p).
\]

One has \( \text{Conf}_n \subset \text{Conf}_n^\text{P} \) a subvariety whose complement is a divisor with simple normal crossings. This implies that the same comparison holds in the middle, rather than just over the compactifications.

To get the same comparison on the leftmost column, take invariants under the \( S_n \) action, to go from ordered to unordered spaces. This gives

\[
\dim H^i_\text{ét}(\mathbb{Q}_p) \leq \dim H^i_\text{ét}(\mathbb{Z}_p) \leq \dim H^i_\text{ét}(\mathbb{Z}/p)
\]

where the dimension of cohomology with coefficients in \( \mathbb{Z}_p \) is defined as the minimal number of generators for the cohomology group as a \( \mathbb{Z}_p \)-module.

We now tie this back to Cohen-Lenstra heuristics for function fields:

**Theorem 10.4.**

\[
\left| \sum_{L \in E_n} \frac{|\text{Surj}(\text{Cl}(L), A)|}{\#E_n} - 1 \right| \leq \frac{c(A)}{\sqrt{q}}
\]

for \( \ell \nmid q \), \( \ell \nmid q - 1 \), \( \sqrt{q} > c(A) \), ad \( n > c(A) \), where \( c(A) \) is a constant depending only on \( A \).

**Proof.** Points in \( Hur^n_{G,c}(\mathbb{F}_q) \) classify surjections \( \text{Cl}(L) \to A \), and \( E_n \) is classified by monic squarefree polynomial of degree \( n \). A simple combinatorial argument shows that \( |E_n| = q^n - q^{n-1} \). We have

\[
|\text{Hur}_n^{G,c}(\mathbb{F}_q)| = \sum_{i=0}^{2n-1} \text{tr}(\text{Frob}_q|H^i(\text{Hur}_n^{G,c}, \mathbb{Q}_p)) + \text{tr}(\text{Frob}_q|H^{2n}(\text{Hur}_n^{G,c}, \mathbb{Q}_p))
\]

where the second term is \( q^n - 1 \) since this is the number of components, as in the previous talk. Using the fact that the eigenvalues of Frobenius on \( H^i \) are all Weil integers of size \( q^{i/2} \), we get

\[
\left| \sum_{i=0}^{2n-1} \text{tr}(\text{Frob}_q|H^i(\mathbb{Q}_p)) \right| \leq \sum_{i=0}^{2n-1} \sqrt{q}^i \dim H^i(\mathbb{Q}_p).
\]
Poincare duality implies that this is bounded by
\[
\sum_{i=0}^{2n-1} \sqrt{q} \dim H^{2n-i}(\mathbb{Q}_p) \leq q^n \sum_{i=0}^{2n-1} \sqrt{q}^{-2n} C(G,c)^{2n-i+1} \frac{c(A)}{\sqrt{q}}^k \leq q^n \frac{2c(A)}{\sqrt{q}}
\]
for $\sqrt{q} > 2c(A)$.


Let $G$ a finite group, $C$ a conjugacy class in $G$, and $D$ a closed disk with a marked point. Recall that $\text{Hur}_{G,n}$ is the moduli space of ramified $G$-covers of $D$. That is, the points of $\text{Hur}_{G,n}$ are covers $p : Y \to D \setminus S$, where the marked point of $Y$ is sent to the marked point of $D$, $S \subset D$ is the ramification divisor and has degree $n$, and we have fixed an isomorphism $\alpha : G \to \text{Aut}(p)$. Recall also that $\text{Hur}^c_{G,n}$ is the moduli space of covers of $D$ such that $f(\gamma_i) \in C$ for all $i$.

There is a product structure on these Hurwitz spaces, given by taking disjoint union of covers:

$$\text{Hur}^c_{G,n_1} \times \text{Hur}^c_{G,n_2} \to \text{Hur}^c_{G,n_1+n_2}$$

defined up to homotopy.

Fix $i \geq 0$ and fix a field $k$ with $\text{char } k \nmid \#G$.

Claim: $h_i(\text{Hur}^c_{G,n}, k)$ is periodic for $n >> 0$.

The rest of today will be dedicated to outlining the idea of the proof of this theorem.

Let $M_i = \bigoplus_n H_i(\text{Hur}^c_{G,n}, k)$. If we have a map $U : M_i \to M_j$ of some fixed positive degree that is eventually an isomorphism, then we win.

For the degree-0 case: set $i = 0$, and $R = M_0$. We'll see that $R \cong k[S]$ as graded $k$-algebras, where $S = \bigsqcup S_n$, where $S_n := C^n / B_n$, where $B_n$ is the braid group acting on $C^n$ in the obvious way.

Recall that the components of $\text{Hur}^c_{G,n}$ are the orbits of $B_n$ acting on $C^n$, at least when $n >> 0$. This holds from the description of $\text{Hur}^c_{G,n}$ as a cover of $\text{Conf}^n$. Therefore the claim is true “as $k$-vector spaces”; that is, $R \cong k[S]$ as $k$-vector spaces, so it remains to upgrade this to an isomorphism as graded $k$-algebras. To consider the product structure: multiplication is given by concatenation of words in $C$. This product structure is generated in degree 1 by elements $r_g$ for $g \in C$, with relations $r_g^{-1} r_{g^{-1}} = r_g r_{g^{-1}}$. This product structure is used to get the isomorphism as $k$-algebras. One then inducts on the degree to prove the full claim.

Definition 5. $(G, c)$ is said to be non-splitting if for all sugroups $H \subset G$, $H \cap C$ is either $\emptyset$ or consists of a $c \in H$ generating $H$.

Our case of interest is that $\#G$ is twice an odd number, and $c = \{\text{elements of order 2}\}$. In this case, $(G, c)$ is non-splitting by Sylow’s theorem.

Let $(G, C)$ be non-splitting, and let $U_D := \sum_{g \in C} r_g^{D(g)} \in R$, for $D \in \mathbb{N}$. This element is central in $R$. Moreover, there exists a $D$ such that $U_D : R \to R$ is eventually an isomorphism of degree equal to $D \cdot |g|$.

Proof. We begin with a lemma:
Lemma 11.1. Let $g \in C$ and $n >> 0$. Then any $(g_1, \ldots, g_n)$ with $\langle g_i \rangle = G$ is $B_n$-equivalent to some $(g, g'_1, \ldots, g'_{n-1})$ with $\langle g'_i \rangle = G$.

Let $S_n(H) = \{n \text{-tuples that generate } H\} \subset S_n = C^n/B_n$.

Claim: for $n >> 0$, $r^{[g]}_g : S_n(H) \to S_{n+\lvert g\rvert}(H)$ is an isomorphism.

To prove the claim: use descending induction, with base case being $S_n = C^n/B_n$.

Claim: There exists a $D$ such that for $n >> 0$, $r^{[D]g}_g : S_n(H) \to S_{n+D\lvert g\rvert}(H)$ is independent of $g$.

To prove the claim: choose $g_1, g_2$ and let $A_i = r^{[g_i]}_{g_i}$. Now $A_1 \circ A_2^{-1}$ permutes $S_n(H)$. There exists a $D$ such that the order of all permutations of $S_{n+D}(H)$ divides $D$, for all $H$. Then $(A_1 \circ A_2^{-1})^D = A^D_1 \circ A^D_2$ by centrality, which is the identity.

Claim: Let $R \supset F_m R$, where $F_m R$ is the subspace generated by $S_n(H)$ with $\lvert H\rvert \geq m$. $F_1 R$ is defined to be $R$. Then $U_n : F_m R \to F_m R$ is an isomorphism for $n >> 0$.

To prove the claim: use descending induction, with base case being $m > \lvert G\rvert$.

Now we turn to the case of higher-degree homology.

Claim: $U_D : M_i \to M_i$ is an isomorphism for $n >> 0$. View $M_i$ as a $k[x]$-module, with $x$ acting as $U_D$.

Proving homological stability is equivalent to bounding $\text{Tor}^{k[x]}_{0,1}(k, M_i)$. We have $\text{Tor}_0(k, M_i) = k \otimes_{k[x]} M_i = \text{coker}(U_D)$, and $\text{Tor}_1(k, M_i) = M_i[x] = \text{ker}(U_D)$.

Let $H_j(M) := \text{Tor}^R_j(k, M)$. Note that $H_0(M) = M/R_0 M$.

Lemma 11.2. For $M$ and $N$ graded left and right $R$-modules,

$$\deg(N \otimes_R M) \leq \deg N + \deg(H_0(M)).$$

Here, the degree is defined to be the homological degree of the module.

Proof. Without loss of generality, $\deg N, \deg H_0(M) < \infty$. If $N = k$, then $\deg(N \otimes_R M) = \deg(H_0(M))$ and we win. (More generally, this is true for any $N$ with homological degree 0.)

One can check that if $0 \to N_1 \to N_2 \to N_3 \to 0$ is a short exact sequence of $R$-modules, and the lemma holds for $N_1$ and $N_3$, then the lemma holds for $N_2$. Using this fact, one inducts on $\deg N$ using the short exact sequence

$$0 \to N_{\max} \to N \to N/N_{\max} \to 0.$$

Let $\overline{R} = R/UR$ be an $R$-bimodule of finite degree.

Lemma 11.3. Let $\overline{M}$ be a graded left $\overline{R}$-module. Then

$$\deg(\text{Tor}_i^\overline{R}(k, \overline{M})) \leq \deg(\overline{R}) i + \deg(\overline{M}).$$
Proof. Form a projective resolution

\[ \cdots \to P_1 \to P_0 \to k \to 0 \]

with \( P_i \) generated in degree at most \( i \deg(\mathcal{R}) \). Namely, \( P_0 = \mathcal{R} \), and \( P_i \) is a free \( \mathcal{R} \)-module on generators of \( \ker(P_{i-1} \to P_{i-1}) \). Then:

\[
\deg \operatorname{Tor}^\mathcal{R}_i(k, M) \leq \deg R_i \otimes_\mathcal{R} \overline{M}
\]

\[
\leq \deg(H_0(P_i)) + \deg(\overline{M}) \leq \deg(\mathcal{R})_i + \deg(\overline{M}).
\]

\[ \square \]

References

