Johns Hopkins Number Theory Seminar

Nir Elber

Spring 2025

Contents

1 January 22: Friedrich Knop

This is joint work with Zhgoon. For a group G with two subgroups $P, H \subseteq G$, we may be interested in the double coset space $P\backslash G/H$. Today, G will be a connected reductive group over a field K, which may or may not be algebraically closed. Then H and P will be closed subgroups of G.

Example 1. Take $G = \mathrm{GL}_n(\mathbb{C})$ and $H \subseteq \mathrm{O}_n(\mathbb{C})$ and P to be the upper-triangular matrices. Then $P\backslash G/H$ becomes complete flags together with some data of a quadratic form; it turns out to be classified by involutions in S_n, where a σ has attached to it the quadratic form $\sum_i x_i x_{\sigma i}$. For example, the orbit corresponding to $x_1^2 + x_2^2 + x_3^2$ is open.

In general, one can see that having finitely many orbits. For example, there is the following result.

Theorem 2. Fix G a connected reductive group over an algebraically closed field K with Borel subgroup $B \subseteq G$, and let $H \subseteq G$ be a closed subgroup. Then B has an open orbit in G/H if and only if $|B\backslash G/H|$ is finite.

There are examples yielding some level of sharpness for this result. One can ask what is special about the quotient $B\backslash G$, which the following notion helps explain.

Definition 3 (complexity)**.** Fix a group H acting on a variety X over an algebraically closed field K. Then we define the *complexity* $c(X/H)$ as the transcendence degree of $K(X)^H$; note that this is the dimension of X/H if such a quotient makes sense.

Theorem 4 (Vinburg)**.** Let $Y \subseteq X$ be a subvariety with an action by G. Then $c(Y/B) \leq c(X/B)$.

The moral of the story is that we are able to bound open orbits.

We would like to have such theorems over fields K which may not be algebraically closed, but this requires some modifications. For example, one may not have a Borel subgroup B defined over K, so we must work with a minimal parabolic subgroup P. For example, we have the following.

Theorem 5. Work over the field $\mathbb{R}$. Then if P has an open orbit in G/H, then $|P(\mathbb{R})\backslash X(\mathbb{R})|$ is finite, where X refers to the quotient G/H.

However, even this result fails over (say) $\mathbb{Q}$.

Example 6. Consider $G = \mathbb{G}_{m,\mathbb{Q}}$ with $H = \mu_2$. Then $X = G/H$ becomes $\mathbb{G}_m$, but then action is given by the square, so the quotient is the infinite set $\mathbb{Q}^{\times 2}\backslash\mathbb{Q}^\times$.

Remark 7. This example suggests that we may be able to salvage the theorem over local fields of characteristic 0.

To fix the result in general, we want to try to work over the algebraic closure.

Theorem 8. Work over a perfect field K. Let $P \subseteq G$ be a minimal parabolic, and let X be a variety with a G-action. Suppose that there is $x \in X(K)$ such that the orbit $Px \subseteq X$ is open. Then the quotient $P(\overline{K})\backslash X(K)$ is finite.

Here, this quotient by $P(\overline{K})$ refers to "geometric" equivalence classes: two points x and x' are identified if and only if one has $p \in P(\overline{K})$ such that $x = px'$. We want the following notion.

Definition 9. Let G act on a variety X. Then X is K*-spherical* if and only if there is a point $x \in X(K)$ such that the orbit by the minimal parabolic is open.

For example, suitably stated (one should assume that $X(K) \subseteq X$ and $Y(K) \subseteq Y$ are dense and that X is normal), one is able to recover the result on complexity. Roughly speaking, the idea is to reduce to the case where G has rank 1. There are two cases for this reduction.

- Previous work explains how to achieve the result when $GY = Y$.
- If GY strictly contains Y, then we pass to a quotient by a parabolic subgroup corresponding to some simple root.

We are now in the rank 1 case. If $K = \overline{K}$, then it turns out that one may merely work with $G = \mathrm{SL}_2$; then one actually directly classify closed subgroups to produce the result. With $K = \mathbb{R}$, a similar idea works, but the casework at the end is harder. However, no such classification is available for general K. Instead, for general K, we develop some structure theory of these sorts of spherical varieties.

2 January 24: Milton Lin

Today, we are talking about period sheaves in mixed characteristics. The references are to relative Langlands duality and the geometrization of the local Langlands conjectures. In relative Langlands duality, they stated a duality of pairs of spaces (X, G) and $(\check{X}, \check{G})$. Today, we will be interested in the "Iwasawa–Tate" case, which is the pair $(\mathbb{A}^1, \mathbb{G}_m)$, where the dual is itself. In particular, we will study the period duality.

Today, Λ will be one of the coefficient rings $\{\mathbb{F}_\ell, \mathbb{Z}_\ell, \mathbb{Q}_\ell, \overline{\mathbb{Q}}_\ell\}$, and E is a p-adic field. Here is our main reesult.

Proposition 10. There is a map of v-stacks $\pi\colon \mathrm{Bun}_G^X \to \mathrm{Bun}_G$.

Intuitively, a v-stack is some kind of geometric object.

Definition 11. We call $\mathcal{P}_X := \pi_! \Lambda$ the *period sheaf*.

Remark 12. These objects all exist in the equal characteristic case. Roughly speaking, $\mathcal{P}_X$ categorifies period functionals.

Remark 13. Conjecturally, one can go down to local systems and define a map $\mathrm{Loc}_{\check{G}}^{\check{X}} \to \mathrm{Loc}_{\check{G}}$. This allows us to define an L-sheaf by $\mathcal{L}_{\check{X}} := \pi_* \omega_{\widehat{\check{X}}}$, which is supposed to categorify L-functions. One expects $\mathcal{L}_{\check{X}}$ and $\mathcal{P}_X$ to correspond to each other in the case of $\mathbb{G}_m$, where the result is a known case of the local geometric Langlands conjecture due to Zou.

We would like to recover the correspondence between $\mathcal{P}_X$ and $\mathcal{L}_{\check{X}}$ in our mixed characteristic setting.

Let's review some background on Bun_G before continuing. We let $\mathrm{Pftd}_{\mathbb{F}_q}$ be the category of perfectoid spaces over $\mathbb{F}_q$. These spaces are glued together from "affines" $\mathrm{Spa}(R, R^+)$ where (R, R^+) is a perfectoid ring: R is some topological ring, and $R^+ \subseteq R$ is a subring of the bounded elements (and equality will hold in our cases of interest).

Example 14. The prototypical examples in positive characteristic look like $\mathbb{F}_p((t))$ embedded in a completion of $\mathbb{F}_p((t^{1/p^\infty}))$.

Example 15. The prototypical examples in mixed characteristic look like $\mathbb{Q}_p$ embedded in a completion of $\mathbb{Q}_p(\mu_{p^\infty})$.

Definition 16 (Fague–Fontaine curve)**.** Fix a perfectoid ring (R, R^+). Set $E := \mathbb{Q}_p$ and $S := \mathrm{Spa}(R, R^+)$. Then we define

$$\mathbb{D}_S := \mathrm{Spa}\left(W(R^+) \otimes_{W(\mathbb{F}_p)} \mathcal{O}_E\right).$$

Morally, we have base-changed a disk to our desired coefficients. We also define the punctured disk $\mathbb{D}_S^\times$ as removing the vanishing set of $\pi[\varpi]$, where $\pi \in E$ is a uniformizer and ϖ is a topologically nilpotent unit. (Here, $[\varpi]$ refers to the Teichmuler lift from R to $W(R)$.) Lastly, we define the Fague–Fontaine curve

$$\Sigma_{S,E} := \mathbb{D}_S^\times / \varphi^{\mathbb{Z}},$$

where φ is the Frobenius on $W(R^+)$.

Remark 17. Morally, the point of $\mathbb{D}_S^\times$ is that we are trying to replicate some object like $\mathrm{Spec}\,\mathbb{Z} \times_{\mathbb{F}_1} \mathrm{Spec}\,\mathbb{Z}$: the point is that we want a second parameter in (R, R^+) to keep track of the distance between our points in the mixed characteristic situation.

Definition 18. We define Bun_G as the functor $\mathrm{Pftd}_{\mathbb{F}_q}$ to anima (here, anima is approximately speaking topological spaces) sending a perfectoid space S to G-torsors on $\Sigma_{S,E}$. This is a v-stack, meaning that it satisfies some kind of descent for the v-topology.

Example 19. For $G = \mathbb{G}_m$, there is an explicit description in terms of quotients $[*/E^\times]$. This allows a computation of $D(\mathrm{Bun}_{\mathbb{G}_m}, \Lambda)$.

3 January 31st: Milton Lin

Let's begin with some motivation today. Fix a reductive group G defined over a number field F. An automorphic form on G is some sort of smooth function f on the automorphic quotient $[G] = G(F)\backslash G(\mathbb{A}_F)$. Given a G-variety X, one finds many interesting period functionals Θ_X, and then the canonical pairings $\langle \Theta_X(\varphi), f\rangle$.

Let's be a bit more explicit about where this functional Θ_X arises from. Roughly speaking, one defines a Schwartz space $\mathcal{S}(X(\mathbb{A}_F))$ and then

$$\Theta_X(\varphi) \coloneqq \sum_{\gamma \in X(F)} \gamma\varphi,$$

where $\varphi \in \mathcal{S}(X(\mathbb{A}_F))$. The point is that choosing Θ_X, φ, and f carefully recovers some special values.

Let's be a bit more explicit. Throughout, $G = \mathbb{G}_m$ and $X = \mathbb{A}^1$.

Example 20. We work over a number field F. Then we know how to define $\mathcal{S}(\mathbb{A}_F)$ as

$$\mathcal{S}(\mathbb{A}_F) = \bigoplus_{v \in V(F)} (\mathcal{S}(F_v), 1_{\mathcal{O}_v}),$$

where this refers to a restricted tensor product. Our special vector $\varphi \in \mathcal{S}(\mathbb{A}_F)$ will be the self-dual one from Tate's thesis: define φ_v by

$$\varphi_v \coloneqq \begin{cases} 1_{\mathcal{O}_v} & \text{if } v < \infty, \\ e^{-\pi|x|^2} & \text{if } v \mid \infty. \end{cases}$$

Next, we note that automorphic forms on $\mathbb{G}_m$ are simply Hecke characters χ, and it turns out that $\langle \Theta_X(\varphi), \chi\rangle$ recovers the special value $L(\chi, 0)$ of the Hecke L-function $L(s, \chi)$.

Example 21. We work over a function field $F = \mathbb{F}_q(\Sigma)$, where Σ is a smooth projective curve over a finite field $\mathbb{F}_q$. Then all places $v \in V(F)$ are finite already, so we should define φ as $\prod_v 1_{X(\mathcal{O}_v)}$. But now we note that φ is notably $\mathcal{O}_v^\times$-invariant for each place v, so $\Theta_X(\varphi)$ will descend to the double quotient

$$G(F)\backslash G(\mathbb{A}_F)/G(\mathcal{O}_F),$$

which has a geometric meaning as $\mathrm{Bun}_G(\mathbb{F}_q)$. In particular, it turns out that $\Theta_X(\varphi)$ is realized as some trace of a constant sheaf on a moduli space $\mathrm{Bun}_G^X(\mathbb{F}_q)$ of G-bundles together with a section from the associated X-bundle. In fact, one can compute that this sends a G-bundle $\mathcal{L}$ (which is a line bundle!) to $\#H^0(\Sigma, \mathcal{L})$.

Let's now return to the setting from last week. Let E be a nonarchimedean local field, and let Λ be the coefficient ring $\mathbb{F}_\ell$. Last time we described a stratification

$$\mathrm{Bun}_G = \bigsqcup_{d \in \mathbb{Z}} [\mathrm{pt}/E^\times],$$

and we label each piece by Bun_G^d. It is interesting, from the perspective of these sheaves, to understand $\mathcal{P}_X := \pi_! \underline{\Lambda}_X$. For example, last time we explained

$$\mathcal{P}_{X,d} = \begin{cases} \Lambda_{\text{norm}}[-2d] & \text{if } d > 0, \\ \Lambda_c(E) & \text{if } d = 0, \\ \Lambda_{\text{triv}} & \text{if } d < 0, \end{cases}$$

where these are all elements of the derived category $D^{\text{sm}}(E^\times, \Lambda)$ of smooth representations of $E^\times$ over Λ. Remarkably, we see that $d = 0$ recovers our functions on E, which is seen in Tate's thesis.

This study of periods is all "motivic" in some sense. On the spectral/automorphic side, one has a dual version $\mathrm{Bun}_G^X \to \mathrm{Bun}_G$ named

$$\pi \colon \mathrm{Loc}_{\check{G}}^{\check{X}} \to \mathrm{Loc}_{\check{G}},$$

which are intended to categorify L-functions; however, these objects are not available in mixed characteristic.

Let's begin by discussing $\mathrm{Loc}_{\check{G}}$, which is available. Intuitively, we are looking for "local systems with G-action," which amounts to a group homomorphism from a fundamental group to G. One usually begins by defining a moduli stack of 1-cocycles named $\mathcal{Z}^1(\omega_E, \check{G})$, and then $\mathrm{Loc}_{\check{G}}$ is the quotient of this by the adjoint action from $\check{G}$. So we now want to define $\mathcal{Z}^1(\omega_E, \check{G})$, which as a functor of points takes a commutative $\mathbb{Z}_\ell$-algebra A to

$$\mathrm{Hom}_{\text{cts}}(W_E, \check{G}(A)),$$

where W_E is the Weil group. Here, W_E is to be understood as a stand-in for the fundamental group of the Fargues–Fontaine curve.

Example 22. With $G = \mathbb{G}_m$, the fact that G is abelian yields

$$\mathcal{Z}^1(W, \check{G})/\check{G} = \mathrm{Hom}_{\text{cts}}(W_E, \check{G}) \times B\check{G}.$$

We now expand our coefficients to $\Lambda = \overline{\mathbb{Q}}_\ell$. It turns out that

$$D(\mathrm{Bun}_G, \Lambda) \cong \mathrm{QCoh}(\mathrm{Loc}_{\check{G}}),$$

which is some sort of categorical version of the local Langlands correspondence. The left-hand side is understood to decompose geometrically, and the right-hand side (due to the $B\check{G}$) is seen to decompose similarly. Namely, one computes both sides as

$$\prod_{d \in \mathbb{Z}} D^{\text{sm}}(E^\times, \Lambda) \cong \prod_{d \in \mathbb{Z}} \mathrm{QCoh}(\mathrm{Hom}_{\text{cts}}(W_E, \check{G})),$$

and the two decompositions roughly align (up to a sign). In short, one uses the Hecke again to reduce to $d = 0$. Roughly speaking, this comes from class field theory, though to be formal, one should reduce everything to a "finite level" by taking quotients by a chosen compact open subgroup $K \subseteq E^\times$, which is legal because our representations are smooth.

The moral of the story is that we can move our period sheaf $\mathcal{P}_X$ from the left to the right. In particular, the proof of the previous paragraph even provides an explicit formula how to do this. For example, on the 0th component, we are interested in what quasicoherent sheaf corresponds to $\mathrm{ind}_1^{E^\times} \Lambda = \Lambda_c(E^\times)$. In particular, we find that we get

$$\varinjlim_{K \subseteq E^\times} \Lambda_c(E^\times)_K,$$

where $(-)_K$ denotes the coinvariants. Eventually one computes that we get $\Lambda[E^\times/K]$ at finite level, which becomes the structure sheaf of $\mathrm{Hom}(W_E, \check{G})$ after the colimit. In total, one finds that

$$\mathrm{Loc}_{\check{G}}^d = \begin{cases} i_{\text{cyc}*}\Lambda[2d] & \text{if } d > 0, \\ ? & \text{if } d = 0, \\ i_{\text{triv}*}\Lambda & \text{if } d < 0. \end{cases}$$

To guess the last entry $?$, one uses the short exact sequence

$$0 \to \Lambda_c(E^\times) \to \Lambda_c(E) \to \Lambda \to 0,$$

where the right-hand map is given by evaluation at 0, so one can dualize the short exact sequence.

4 February 5: Ryan Chen

Today we are talking about near-center derivatives and arithmetic 1-cycles. Recall that one can normalize the weight-2 Eisenstein series to have a Fourier expansion

$$E_2^*(z) = \frac{1}{8\pi y} + \frac{\zeta(-1)}{2} + \sum_{t>0} \sigma_1(t) q^t,$$

where $q := e^{2\pi i z}$ as usual. We claim that all terms except for the $\frac{1}{8\pi y}$ admit geometric meanings.

- The value $\zeta(-1)/2$ is the volume of the modular curve $Y(1)$, where the measure is given by the push-forward of the Hodge module Ω^1 along the universal elliptic curve $\pi\colon \mathcal{E} \twoheadrightarrow Y(1)$. Explicitly, one finds that this volume form is $-\frac{1}{4\pi^2} dx \wedge dy$.
- The values $\sigma_1(t)$ are degrees of some Hecke correspondences $\mathrm{Hk}(t)$ over $Y(1)$. Imprecisely, $\mathrm{Hk}(t)$ parameterizes degree-t isogenies.

Let's do this for other Shimura varieties. Let's define SL_2-Eisenstein series. Here, $F/\mathbb{Q}$ is an imaginary quadratic field with discriminant Δ, and we assume 2 splits for technical reasons. Then our SL_2 is given the real form $\mathrm{SU}(1,1)$, and it acts on the upper-half plane $\mathcal{H}$ as usual. Of course, there are higher-dimensional versions of this. Let $P \subseteq \mathrm{SU}(1,1)$ be the Siegel parabolic of upper-triangular matrices, and for even positive weight, we have

$$E_n(z,s) := \sum_{\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in P(\mathbb{Z}) \backslash \mathrm{SU}(1,1)(\mathbb{Z})} \frac{(\det y)^s}{\det(cz+d)^n \left|\det(cz+d)\right|^{2s}}.$$

Sometimes, one shifts s by $s_0 = \frac{1}{2}(n-m)$ to make the functional equation look nicer.

It again turns out that $E_2^*(z,s)$ can be written out as a constant plus some Fourier coefficients of the form $E_2^*(y,s)(t)q^t$. Roughly speaking, this Euler product $E_2^*(y,s)$ reaks into archimedean and nonarchimedean parts

$$W_{t,\infty}^*(y,s) \prod_p W_{t,p}^*(s).$$

The archimedean part is something coming from hypergeometric functions, and the nonarchimedean part basically multiplies to something involving divisor functions as $|t|^{s+1/2} \sigma_{-2s}(|t|)$ (after shifting s).

We are now ready to state a corollary of the main theorem.

Corollary 23. One has

$$\frac{1}{2} \frac{d}{ds}\bigg|_{s=1/2} \prod_p W_{t,p}^*(s) = \sum_{\substack{\varphi\colon E \to E_0 \\ \deg \varphi = t}} (h_{\mathrm{Fal}}(E) - h_{\mathrm{Fal}}(E_0)),$$

where E_0 is a fixed elliptic curve with CM by $\mathcal{O}_F$ for some imaginary quadratic field $F/\mathbb{Q}$ in which 2 is split, and h_{Fal} is the Faltings height.

Notably, the right-hand expression depends on F, but the left-hand side does not! We remark that one can give geometric meaning to the entire expression $E_2^*(y,s)(t)$ as coming from some cycle.

Remark 24. Let's recall something about the Faltings height. Let $\widetilde{E}$ be an elliptic scheme over $\mathcal{O}_K$; we are only interested in the CM case, so we may as well assume that $\widetilde{E}$ has good reduction everywhere. We also assume that $\Gamma(\widetilde{E}, \Omega^1)$ is free over $\mathcal{O}_K$ gnerated by some α. Then

$$h_{\mathrm{Fal}}(E) = -\frac{1}{2}\frac{1}{[K:\mathbb{Q}]}\sum_{\sigma\colon K\hookrightarrow\mathbb{C}} \log\left|\frac{1}{2\pi}\int_{E_\sigma(\mathbb{C})}\alpha\wedge\overline{\alpha}\right|.$$

Remark 25. This complex volume on the right-hand side can also be seen as a volume of the arithmetic curve $\widetilde{E}$ over $Y(1)_{\mathcal{O}_K}$. We remark that one can approximate this "arithmetic volume" by intersecting $\widetilde{E}$ with Hecke translates of a given curve. Some version of equidistribution of Hecke orbits is then able to let us compute a volume! This is a key idea in the proof.

Let's move to a higher-dimensional case. Simply upgrade the group $\mathrm{SU}(1,1)$ to $\mathrm{SU}(m,m)$ everywhere, and we are able to define our Eisenstein series. Then it turns out that one has a Fourier expansion

$$E_n(z,s) = \sum_{T\in\mathrm{Herm}_m(F)} E_n(y,s)(T)\cdot q^T,$$

where $\mathrm{Herm}_m(F)$ refers to the Hermitian $m\times m$ matrices with entries in F. We let $\widetilde{E}(z,s)$ denote some suitable normalization, mostly multiplying in some πs, a discriminant, some gamma factors, and some L-function of a quadratic character.

Our main theorem is some version of the Siegel–Weil formula. Here is the classical result, which tells us that special values of Eisenstein series know about counting lattice points.

Theorem 26 (Seigel–Weil)**.** Choose an integer n divisible by 4. Then with $m=1$,

$$\widetilde{E}(y,s)(T) = \sum_{\Lambda}\frac{\#\{x\in\Lambda : (x,x)=T\}}{\#\operatorname{Aut}\Lambda},$$

where Λ varies over Hermitian $\mathcal{O}_F$-lattices which are positive-definite, self-dual (with respect to the trace pairing over $\mathbb{Z}$), and rank n.

Remark 27. There is also a straightforwardly stated generalization to higher m. One basically replaces $x\in\Lambda$ with a tuple $\underline{x}\in\Lambda^m$ and replaces the norm condition with a condition on the Gram matrix $(\underline{x},\underline{x})$.

Remark 28. The set of vector spaces $\Lambda\otimes_{\mathbb{Z}}\mathbb{Q}$ is a Shimura variety of unitary type.

To make this result more geometric, we replace all these lattices by abelian varieties. We pick up a few definitions.

Definition 29 (Hermitian abelian scheme)**.** A *Hermitian abelian scheme* over a base S is a triple (A,ι,λ), where A is an abelian scheme over S, $\iota\colon\mathcal{O}_F\to\operatorname{End}A$ is an embedding, $\lambda\colon A\to A^\vee$ is a polarization, along with some compatibility conditions. For example, complex conjugation should correspond to the Rosati involution.

Definition 30 (Kottwitz signature)**.** Fix a Hermitian abelian scheme (A,ι,λ) over S, where S is a scheme over $\mathcal{O}_F$. Then the *Kottwitz signature* is a pair $(n-r,r)$ of integers such that any $\alpha\in\mathcal{O}_F$ has its characteristic polynomial of $\iota(\alpha)$ acting on $\operatorname{Lie}A$ taking the form

$$(X-a)^{n-r}(X-\sigma a)^r.$$

Now, to state our more geometric Siegel–Weil formula, we count points in a lattice $\mathcal{L} = \mathrm{Hom}(E_0, A)$, where E_0 is a fixed CM elliptic curve, which we go ahead and equip with its canonical principal polarization. Roughly speaking, the norm (x,x) comes from a "Rosati involution" (arising from the ambient polarizations) and is defined as $x^\intercal \circ x$. Lastly, the self-duality condition corresponds to having $\ker \lambda$ equaling the kernel of the different ideal acting on A, and it is included for some technical conditions.

At the end of this story, we have defined a subfunctor $\mathcal{Z}$ of $\mathcal{L}^m$, and it is called the Kudla–Rapoport special cycle. This is some 0-dimensional cycle.

Remark 31. Prior work computed an arithmetic degree of $\mathcal{Z}(T)$ as

$$\frac{\#\,\mathrm{Cl}\,\mathcal{O}_F}{\#\mathcal{O}_F^\times}\frac{d}{ds}\bigg|_{s=0}E(y,s)(T).$$

The main theorem roughly tells the same story for an analogously defined 1-cycle, proving a case of the Kudla's program.

5 February 19: Stefan Dawydiak

This talk was titled "Affine and asymptotic Hecke algebras." I don't expect to be able to follow much. Today, we are talking about p-adic representation theory. It is well-known that they are controlled by affine Hecke algebra, but today we would like to extend this to asymptotic Hecke algebras. Philosophically, the affine Hecke algebra is important because it has two presentations, each of which know something about one side of the local Langlands correspondence. The asymptotic Hecke algebra will have a similar role.

Let's begin with affine Hecke algebras. This requires us to define Coxeter groups, which tell the story of finite Weyl groups.

Definition 32 (Coxeter)**.** A *finite Coxeter group* W is one which is generated by some reflections $s_i \in S$ with explicit relations which look like $(s_is_j)^\bullet = 1$.

Definition 33 (affine Hecke algebra)**.** The *affine Hecke algebra* $\mathcal{H}_{\mathrm{fin}}$ is a q-deformation of $\mathbb{Z}[W]$, spanned by some letters $\{T_w : w \in W\}$ satisfying the relations

$$(T_s+1)(T_s-q)=0$$

for each $s \in S$.

Example 34. At $q = 1$, we recover $\mathbb{Z}[W]$.

Remark 35. There is a Kazhdan–Lusztig basis which provides a ring J_{fin} (over $\mathbb{Z}$) such that there is an embedding

$$\mathcal{H}_{\mathrm{fin}} \hookrightarrow J_{\mathrm{fin}}[q^{\pm 1}],$$

which is an isomorphism as soon as one localizes by some polynomial $P_W(q) = \sum_{w\in W} q^{\ell(w)}$.

Next we move to affine Weyl groups.

Definition 36 (affine Weyl)**.** An *affine Weyl group* $\widetilde{W}$ takes the form $W_{\mathrm{fin}} \ltimes X_*$ where $(X^*, X_*, R, R^\vee)$, where $(X^*, X_*, R, R^\vee)$ is the root datum of a split connected reductive group G over a p-adic field F.

Remark 37. There is a decomposition
$$G(F) = \bigsqcup_{w \in \widetilde{W}} IwI,$$
where $I \subseteq G(F)$ is the Iwahori subgroup. For example, with $G = \mathrm{GL}_2(\mathbb{Q}_p)$, we find that I consists of the matrices which are $\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right] \pmod p$.

Definition 38. Given an affine Weyl group $\widetilde{W}$, there is an *affine Hecke algebra* $\mathcal{H}_{\mathrm{aff}}$ spanned by some T_w for $w \in \widetilde{W}$ satisfying some relations.

Remark 39. It now turns out that $\mathcal{H}_{\mathrm{aff}}$ is isomorphic to $C_c(I \backslash G(F)/I)$, whose modules tell us something about smooth admissible representations of $G(F)$.

Remark 40. On the other hand, we see that $\mathcal{H}_{\mathrm{aff}}$ can be seen as some kind of equivariant K-theory over a Steinberg variety. For example, this allows us to say something about what the modules of $\mathcal{H}_{\mathrm{aff}}$ are.

Comparing the above two remarks allows us to prove some subcases of the local Langlands correspondence.

Remark 41. We note that there is once again some "Kazhdan–Lusztig" basis which produces a ring J_{aff} over $\mathbb{Z}$ such that one admits an embedding $\mathcal{H}_{\mathrm{aff}} \hookrightarrow J_{\mathrm{aff}}\left[q^{\pm 1}\right]$. This thing becomes an isomorphism after taking some completion on both sides.

Let's indicate the main theorem. As before, G is a connected split reductive group over a p-adic field F. Let $P \subseteq G$ be a varying parabolic subgroup, and let $P = MU$ be the Levi decomposition. Then we fix some square integrable representation σ of the Levi M, and we let ν vary over the unramified characters of M; note that the collection $X_{\mathrm{unr}}(M)$ of unramified characters on M forms a variety. We now note two constructions coming from $\pi = \mathrm{ind}_P^G(\sigma \otimes \nu)$.

- For $f \in C_c(I \backslash G/I)$, one can produce a function $\pi(f)$ on $X_{\mathrm{unr}}(M)$ defined by
$$\pi(f)v := \int_G f(g)\pi(g)v \, dg.$$
It turns out that this construction will produce infinite tuples η for each choice (P, σ), each η of which varies algebraically in ν.
- The same construction sends Schwartz functins in $\mathcal{C}(I \backslash G/I)$ to endomorphisms which vary smoothly in ν.

It is the proposal of Braverman–Kazhdan that one can fit the ring J_{aff} into the above picture as going to the families $\eta_{(P,\sigma)}$ where $\eta_{(P,\sigma)}$ varies rationally in ν with no poles when one has some positivity condition on ν. This last sentence is our main theorem.

6 February 26: Jeremey Taylor

Today we are talking about tame local Betti Langlands.

6.1 Springer Theory

Our story begins in springer theory, which is motivated by the following observation.

Theorem 42. Fix a nonnegative integer $n \geq 0$. Then the following are in bijection.

(i) Irreducible representations of S_n.

(ii) Partitions of n.

(iii) Conjugacy classes of nilpotent matrices in $M_n(\mathbb{C})$.

Classically, one shows that (i) and (ii) in some explicit combinatorial way, and then the bijection between (ii) and (iii) is not so hard.

Springer theory provides a geometric bijection between (i) and (iii). To explain this, let $\widetilde{\mathcal{N}}$ denote the space of pairs of a nilpotent matrix X and a complete flag of $\mathbb{C}^n$ preserved by X.

Theorem 43 (Springer)**.** There is an isomorphism of algebras

$$\mathrm{H}^{\mathrm{BM}}_{\mathrm{top}}(\widetilde{\mathcal{N}} \times_{\mathcal{N}} \widetilde{\mathcal{N}}) \cong \mathbb{C}[S_n].$$

Morally, one takes some $X \in \mathcal{N}$ on the right to homology of some Springer fiber $\widetilde{\mathcal{N}}_X$.

In positive characteristic, Kazhdan and Lusztig give the following analogue.

Definition 44 (affine Hecke algebra)**.** Let $I \subseteq \mathrm{GL}_n(\mathbb{F}_q((T)))$ be the Iwahori subgrouup, and define the *afine Hecke algebra* H_q as functions on $I \backslash \mathrm{GL}_n(\mathbb{F}_q((T)))/I$.

Remark 45. One should understand H_q as a q-deformation of the Weyl group $S_n \ltimes \mathbb{Z}^n$.

Theorem 46 (Kazhdan–Lusztig)**.** One has

$$K^{\mathrm{GL}_n \times \mathbb{C}^\times}(\widetilde{\mathcal{N}} \times_{\mathcal{N}} \widetilde{\mathcal{N}}) \otimes_{K^{\mathbb{C}^\times}(\mathrm{pt})} \mathbb{C}(q) \cong H_q.$$

From here, one can then use this isomorphism to understand representations of H_q, which has applications to the geometric local Langlands correspondence. In particular, it is produce a bijectino between irreducible representations with an Iwahori-fixed vector; irreducible representations of H_q; and a tuple (s, X) (up to conjugacy) where $s \in \mathrm{GL}_n(\mathbb{F}_q((T)))$ is semisimple, X is nilpotent, and we satisfy $sXs^{-1} = qX$.

Remark 47. There is a rather explicit way to use parabolic induction to write down this bijection when $q = 1$, which means we are looking for irreducible representations of $S_n \ltimes \mathbb{Z}^n$. Roughly speaking, the semisimple element determines the action of the $\mathbb{Z}^n$, and the nilpotent element provides a representation of S_n (given by some induction) via the Springer theory.

6.2 Categorification

We are now ready to state our main theorem, which categorifies the above theorem.

Theorem 48. Fix a complex reductive group G with maximal torus T, let $I \subseteq G(\mathbb{C}((t)))$ be the Iwahori subgroup, and let $I^\circ \subseteq I$ be its pro-unipotent subgroup. Further, set $\widetilde{\mathrm{Fl}} := G(\mathbb{C}((t)))/I^\circ$. Then the following two categories admit a monoidal equivalence.

(i) The category $\mathrm{Sh}_I(\widetilde{\mathrm{Fl}})$ of sheaves which are locally constant on I-orbits.

(ii) The category of ind-coherent sheaves on $\check{B}/\check{B} \times_{\check{G}/\check{G}} \check{B}/\check{B}$.

Remark 49. For (i), we are looking at sheaves in the analytic topology, which explains why we are restricted to $\mathbb{C}$.

Remark 50. The category in (i) is predicted by geometric local Langlands: we are supposed to look at (nilpotent) sheaves on the moduli space of G-bundles on $\mathbb{P}^1$ with "unipotent reduction" at two fixed points. (The unipotent reduction is roughly asking for a basis of the associated graded bundle at the given points.)

Remark 51. Once again, the category in (ii) is predicted by geometric local Langlands, roughly speaking looking for ind-coherent sheaves on the category of $\check{G}$-local systems on $\mathbb{P}^1 \setminus \{0, \infty\}$ with the extra data of some flags at the boundary points.

Remark 52. This can be thought of as a "family of equivalences" varying over $\check{T} \times \check{T}$: (ii) lives over this space because there is a quotient map $\check{B} \times \check{T}$, and (i) lives over this space by some kind of restriction. Taking the fiber at the identity of $\check{T} \times \check{T}$ recovers a result of Bezrukaunikov.

7 March 12: Tsao-Hsien Chen

The title of this talk is "Real groups, symmetric varieties, quantum groups, and Langlands duality." For today, we will work with real groups G (over $\mathbb{R}$), to which one can associate symmetric varieties G/K. There is now an emerging procedure, via relative Langlands duality, to produce quantum groups.

By way of motivation, choose a complex group G, and one may want to understand its real forms. Additionally, one may ask for an anti-holomorphic involution η of the complex group G. Asking for real forms is classified by some marked Dynkin diagrams, and Cartan solved the problem with the additional involution. Cartan's idea to solve the problem with the involution is to directly solve for algebraic involutions $\theta\colon G \to G$ which then give rise to certain subgroups $K = G^\theta$, which amounts to some complex linear algebra. Then there is a correspondence between the anti-holomorphic involutions and the algebraic ones.

The representation theory of Lie groups frequently has this feature, where one can find interesting equivalences between real analytic situations and algebraic "symmetric" ones. Here are some more examples.

- Cartan noticed there is an equivalence between real forms $G_\mathbb{R}$ and symmetric spaces G/K.
- Harish-Chandra showed an equivalence between real representations of G and $(\mathfrak{g}, K)$-modules.
- Matsuki noted there is some correspondence between the flag variety $G_\mathbb{R}\backslash G/B$ and the symmetric space $K\backslash G/B$. (There is a way to upgrade this to derived categories.)
- Approximately speaking, real Langlands on $\mathbb{P}^1$ over $\mathbb{R}$ becomes relative Langlands. Namely, real Langlands on $\mathbb{P}^1$ considers G-bundles on $\mathbb{P}^1_\mathbb{R}$, and relative Langlands considers the loop space L^+G acting on $LX = X(\mathbb{C}((t)))$.

It is worth remembering that the complex story is understood. For example, G-bundles on $\mathbb{P}^1_\mathbb{C}$ are understood by the action of a loop group L^+G on some Grassmannian $\mathrm{Gr}_G := LG/L^+G$. Here is another such statement.

Theorem 53 (geometric Satake)**.** Fix a complex group G. Then there is an equivalence between the following two categories.

- The category of perverse sheaves on $L^+G\backslash\mathrm{Gr}_G$.
- The category of representations of $\check{G}$.

Remark 54. Note that this provides a Tannakian description of $\check{G}$!

One can then prove geometric Langlands for $\mathbb{P}^1$ by upgrading the geometric Satake equivalence to work with derived categories.

Theorem 55. Fix a complex group G. Then there is an equivalence between the following two categories.

- The derived category on $\mathrm{Bun}_G(\mathbb{P}^1)$.
- The derived category on $L^+G\backslash \mathrm{Gr}_G$.

Remark 56. The idea is to consider the following diagram of quotients.

$$\begin{tikzcd} & G\backslash \mathrm{Gr}_G \arrow[dl] \arrow[dr] & \\ L^+G\backslash \mathrm{Gr}_G & & G\left[t^{-1}\right]\backslash \mathrm{Gr}_G \end{tikzcd}$$

The left-hand side turns out to be $\mathrm{Bun}_G(\mathbb{P}^1)$. Then one can build the functor for the above theorem by pull back and push forward.

We now return to the real situation. On the "symmetric" side one works with the category $D(L^+G\backslash LX)$. On the real side, one wants to define a suitable version of $\mathrm{Bun}_G(\mathbb{P}^1)$, which we see will now require two involutions to define: one involution for G and another involution for $\mathbb{P}^1$. However, this extra involution for $\mathbb{P}^1$ does not actually add much content because there are only two real forms up to equivalence: there is $\mathbb{P}^1_{\mathbb{R}}$ and a "twisted" version with no real points.

Remark 57. Similar to how one has a twisted $\mathbb{P}^1$, there is a twisted version of LX.

We are now ready to state a main theorem, which is joint with David Nadler.

Theorem 58. For complex Lie group G with real form $G_{\mathbb{R}}$, there is an equivalence

$$D\left(\mathrm{Bun}_{G_{\mathbb{R}}}(\mathbb{P}^1_{\mathbb{R}})\right) \to D\left(L^+G\backslash LX\right).$$

Remark 59. Once again, the functor is produced by a correspondence with some object $L^+G\backslash LG/K_{\mathbb{R}}$.

Remark 60. Here is an application going from "real" to "symmetric." By using the Hecke action, one can in fact build an equivalence

$$D\left(L^+G_{\mathbb{R}}\backslash \mathrm{Gr}_{G_{\mathbb{R}}}\right) \to D\left(\mathrm{Bun}_{G_{\mathbb{R}}}(\mathbb{P}^1_{\mathbb{R}})\right).$$

Now, the composite equivalence $D\left(L^+G\backslash LX\right) \cong D\left(L^+G_{\mathbb{R}}\backslash \mathrm{Gr}_{G_{\mathbb{R}}}\right)$ is compatible with all structures available. One can even restrict this composite to perverse sheaves and then further restrict to some understood Tannakian subcategories.

Remark 61. Conjecturally, one can understand the full category of perverse sheaves on our spaces as representations of a quantum group.

8 March 19: Chi-Hen Lo

This talk was given at MIT. It was titled "Desiderata and uniqueness of the local Langlands correspondence."

8.1 The Local Langlands Correspondence

Today, F is a p-adic field, and W_F is its Weil group. For example, class field theory provides a canonical isomorphism $W_F^{\mathrm{ab}} \cong F^\times$; by pre-composition, this provides a canonical bijection between smooth one-dimensional representations of $\mathrm{GL}_1(F) \to \mathrm{GL}_1(\mathbb{C})$ and homomorphisms $W_F \to \mathrm{GL}_1(\mathbb{C})$. We would like to go beyond GL_1; for today, we will work with connected reductive algebraic group G over F, and for simplicity we will assume that G is quasi-split. We would like to exhibit maps between the following two sets.

- $\Pi(G, F)$ is the set of smooth irreducible representations of $G(F)$. This may be abbreviated to $\Pi(G)$.
- $\Phi(G, F)$ is the set of L-parameters of maps $\varphi\colon W_F \times \mathrm{SL}_2(\mathbb{C}) \to {}^LG$. This may be abbreviated to $\Phi(G)$.

Here is the main conjecture.

Conjecture 62 (local Langlands)**.** There is a canonical surjective map $\Pi(G) \twoheadrightarrow \Phi(G)$, written $\pi \mapsto \varphi_\pi$ or $\pi \mapsto \mathrm{LLC}_M(\pi)$.

Remark 63. There is a way to enhance the target $\Phi(G)$ to some $\Phi^e(G)$ in order to have a conjectural bijection.

Remark 64. Here is a bit of what is known for fixed G.

- For tori G, this is due to Langlands.
- For GL_n, this is due to Harris–Taylor, Henniart, and Scholze.
- If G is an arbtirary classical group, this is known by many teams.

Remark 65. For some special $\pi \in \Pi(G)$, one can do a bit more. For example, Kazhdan–Lusztig can do it for unipotent representations π, and Kaletha can do it for non-singular supercuspidal representations (for p large).

8.2 Desiderata

Thus, we see that there is a lot known, so it becomes a nontrivial problem to compare the various correspondences. Here is our main result.

Theorem 66. Fix p very large. There is a unique local Langlands correspondence $\Pi(G) \to \Phi(G)$ which satisfies a long list of desiderata.

Let's list our desiredata. For example, it ought to agree with Kaletha's construction (Remark 65) in the non-singular supercuspidal case. Quickly, we note that non-singularity is not scary.

Theorem 67. Assume p is large enough. Then any generic supercuspidal representation is non-singular.

Next up, we want LLC to be compatible with the Langlands classification.

Theorem 68 (Langlands classification)**.** Fix everything as above.

- There is a bijection between $\pi \in \Phi(G)$ and triples (P, π_t, ν) of parabolic $P \subseteq G$, tempered π_t, and unramified character ν. (A triple goes to the parabolic induction twisted by ν.)
- There is a bijection between $\varphi \in \Phi(G)$ and triples (P, ϕ_t, ν) similarly.

Then Theorem 66 asks for LLC to be compatible with the Langlands classifications on both sides.

Our next desideratum has to do with infinitesimal characters.

Definition 69 (infinitesimal character)**.** Fix some $\varphi\colon W_F \times \mathrm{SL}_2(\mathbb{C}) \to {}^L G$. Then there is an *infinitesimal character* given by

$$w \mapsto \varphi\left(w, \begin{bmatrix} |w|^{1/2} & \\ & |w|^{-1/2} \end{bmatrix}\right).$$

Then Theorem 66 asks that two generic $\pi_1 \in \Pi(G)$ and $\pi_2 \in \Pi(M)$ for Levi subgroup $M \subseteq G$ (here, genericity is taken with respect to a chosen Whittaker datum of G) will have π_1 live in the parabolic induction of π_2 if and only if they share the infinitesimal character.

We would also like some control on parabolic induction, so Theorem 66 will ask for $\pi \hookrightarrow \mathrm{Ind}_P^G \sigma$ (with σ unitary tempered) to imply that φ_π is the composition of φ_σ with the induced embedding ${}^L M \to {}^L G$, where $P = MN$ is the Levi decomposition.

We are now ready to note that we have gotten somewhere.

Theorem 70. Let $\Pi^M(G)$ denote the collection of $\pi \in \Pi(G)$ whose paraboic induction has a generic quotient. For p large enough, LLC is uniquely determined on $\Pi^M(G)$ given the above desiredata.

Sketch. If π is non-tempered, then the Langlands classification allows us to induct and replace G by a smaller group. Now, if π is tempered, generic, and supercuspidal, then Kaletha's construction provides LLC. Lastly, if π is tempered, generic, but not supercuspidal, then π is an induction of some supercuspidal. After some twisting, one can use the hypothesis on parabolic induction in the tempered case. ■

Remark 71. The above proof is "almost constructive," in the sense that it can almost inductively calculate what LLC is from the supercuspidal case. Conjecturally, one can sharpen this.

Here are more desiderata.

- We would like the Shahidi conjecture: if φ is tempered, then there is a unique generic element π of the fiber Π_φ.
- We would like some stability: if φ is tempered, then there is a finite sum $\eta_\varphi^{\mathrm{st}}$ into πs with the generic member having nonzero coefficient.
- Lastly, we want "strong atomic stability," which I did not really understand.

9 April 16: Chol Park

This talk was titled "Families of strongly divisible modules of rank 2." This is joint work with Seongjae Han.

9.1 Some Galois Reprensetations

We are interested in computing $\pmod p$ reductions of semistable Galois representations. For today, K is a finite extension of $\mathbb{Q}_p$, and we let G_K denote its absolute Galois group with inertia subgroup $I_K \subseteq G_K$. We let E be another finite extension of $\mathbb{Q}_p$, which will be our coefficient field, so we also set $\mathbb{F} \coloneqq \mathcal{O}_E/\mathfrak{p}_E$.

Thus, our Galois representations will be continuous maps $G_K \to \mathrm{GL}_n(E)$. General Galois representations are a bit hard to handle, so we will restrict our attention to de Rham representations, semistable representations, or even crystalline representations. We note each of those representations admits a Hodge–Tate decomposition given by some weights $\nu \in (\mathbb{Z}^n)^{\mathrm{Hom}(K,E)}$. ALso, potentially semistable representations admit Galois types $\tau\colon I_K \to \mathrm{GL}_n(E)$ (where the target has the discrete topology) which measures how "potential" the potentially semistable reduction is; of course, by the p-adic monodromy theorem, potentially semistable is the same as de Rham.

We will not discuss the p-adic Hodge theory which gives rise to these adjectives, but let's give the key examples. For any smooth projective variety X over K, then the G_K-representation $\mathrm{H}^i_{\text{ét}}(X_{\overline{\mathbb{Q}}_p}, \overline{\mathbb{Q}}_p)$ is de Rham, and X has good (repsectively, semistable) reduction if and only if the Galois representation is crystalline (respectively, semistable).

The intended application for our results is to give a description of some Galois deformation ring, frequently used for the Breuil–Mezard conjecture. Let's give one formulation ("numerical") of this conjecture. Given $\overline{\rho}_0 \colon G_K \to \mathrm{GL}_n(\mathbb{F}_E)$ and Hodge–Tate weight ν and Galois type τ, then Kisin produces a Galois deformation ring $\mathfrak{R}^{\nu,\tau}_{\overline{\rho}_0}$ which is a complete local $\mathcal{O}_E$-algebra whose geometric points parameterize potentially semistable lifts of $\overline{\rho}_0$ with the given Hodge–Tate weight and Galois type. Additionally, τ and ν produces some representations $\sigma(\tau)$ and $\sigma(\nu)$ of $\mathrm{GL}_n(\mathcal{O}_K)$. Then the conjecture is that any irreducible representation σ of $\mathrm{GL}_n(\mathcal{O}_K)$ over $\mathbb{F}$, there is an integer $M_\sigma(\overline{\rho}_0) \in \mathbb{Z}_{\geq 0}$ such that

$$e\left(\mathfrak{R}^{\nu,\tau}_{\overline{\rho}_0}/\mathfrak{p}_E\right) = \sum_\sigma n_\sigma(\nu,\tau) M_\sigma(\overline{\rho}_0),$$

where $n_\sigma(\nu,\tau)$ is some explicit integer not depending on $\overline{\rho}_0$, given by $\overline{\sigma(\nu) \otimes_E \sigma(\tau)}^{\mathrm{ss}} = \bigoplus_\sigma \sigma^{n_\sigma(\nu,\tau)}$. (Here, e is some invariant from commutative algebra, called the Hilbert–Samuel multiplicity.)

Theorem 72 (Cariani–Emerton–Gee–Savitt)**.** When $n = 2$ and $\nu = (0,1)$, the conjecture holds.

Additionally, the proof is able to say something about the integers $M_\sigma(\overline{\rho}_0)$.

9.2 A Little Integral p-adic Hodge Theory

Let's give our review in a few steps.

1. Coleman and Fontaine provided a correspondence between semistable Galois representations of G_K over E and (weakly) admissible filtered (φ, N)-modules over $K \otimes_{\mathbb{Q}_p} E$.
2. To add integrality, we want to work with Galois stable lattices in E, which by Breuil and Lin correspond on the linear algebraic side to strongly divisible modules (which are some kind of lattice in the (φ, N)-module); however, the correspondence only works for Hodge–Tate weights between 0 and $p-2$.
3. Now that we have integrality, we can take $\pmod p$ reduction to get Galois representations of G_K over $\mathbb{F}$. This then corresponds to Breuil modules, but now the functor from Breuil modules to $\pmod p$ repreesentations is merely fully faithful only when $K/\mathbb{Q}_p$ is unramified.

So our goal is to start with the (φ, N)-module, find a strongly divisible module, map down to the Breuil module, and lastly apply the functor to compute some $\pmod p$ Galois representation.

We now focus on the case where $K/\mathbb{Q}_p$ is unramified with degree f. The (φ, N)-modules are already understood. It turns out that producing the strongly divisible module is the difficult step, and the remaining computations are pretty easy. The rest of the talk consisted of explaining how to parameterize the strongly divisible modules, which uses a lot of data and many equations.

10 April 23: Ari Shnidman

This talk was titled "Class group heuristics." This is joint work with Artane Siad.

10.1 The Question

Fix an integer $m \geq 2$, a transitive subgroup $G \subseteq S_m$, a number field K, and a prime ℓ. We are interested in the distribution of the groups $\mathrm{Cl}_F[\ell^\infty]$ as F varies over extensions F/K of degree m with (Galois closure of) Galois group G. This question is old, originating more or less with Gauss, who essentially studied the 2-torsion of the class group of imaginary quadratic fields. In particular, he found some obstructions to the size which suggest we should take $\ell \nmid m$ to get truly random groups.

Here is some of the modern history in this area.

- For $m = 2$ and $F = \mathbb{Q}$, there are the Cohen–Lenstra heuristics (1983), which claim

$$\mathbb{P}(\mathrm{Cl}_F[\ell^\infty] \cong H) \approx \frac{1}{|H|^{r_1} |\mathrm{Aut}\, H|},$$

  where (r_1, r_2) is the signature of the field F, and $\approx$ refers to an explicit constant. This was more or less observed directly from the data.

- For $m > 2$, we found that the Cohen–Lenstra heuristics are incorrect, which was attempted to be fixed by Cohen–Martinet (2008) and corrected by Malle (2008) and Achter. It was recently observed (2020) that the class group has some extra structure which explains the correction observed by Malle. The state of the art seems to be by Sawin–Wood for $\ell \nmid |G|$.

- There are many results supporting the various heuristics in the function field case. The strongest known results are known by Landesmann–Levy, who get very close: they can prove the result for a fixed function field and fixed H.

- In the number field case, there are not many results. Davenport–Heilbronn (1973) counted 3-torsion of class groups of quadratic fields. Bhargava (2005) counted 2-torsion of class groups of cubic fields with full Galois group. There are known generalizations to number fields. Recently, Lemke Oliver–Wang–Wood compute 3-torsion for some 2-groups $G \subseteq S_{2^n}$; they basically manage to inductively bootstrap the Davenport–Heilbronn result.

Here are our main results.

Theorem 73. Choose $K = \mathbb{Q}(\zeta_3)$, and we study $(\mathbb{Z}/3\mathbb{Z})$-extensions. Order extensions $F_n := K(\sqrt[3]{n})$ for $n \in \mathcal{O}_K$ by norm. Then the average of $\#\mathrm{Cl}_{F_n}[2]$ is $3/2$.

Remark 74. This confirms the Cohen–Lenstra–Martinet–Malle heuristics in this case.

We can even do this for different base fields. Of course, as number theorists, we would love to handle $K = \mathbb{Q}$. We will be able to study 2-torsion of the extensions $\mathbb{Q}(\sqrt[3]{n})$ for cube-free $n \in \mathbb{Z}$, but the answer is complicated, as one would expect because it has not been proven yet!

Definition 75. A cubic extension $\mathbb{Q}(\sqrt[3]{n})$ is *type I* if and only if $n \not\equiv \pm 1 \pmod 9$; otherwise, it is *type II*.

Remark 76. This condition $n \pmod 9$ has to do with the structure of the ring of integers.

Theorem 77. Choose $K = \mathbb{Q}$, and we study S_3-extensions.

(a) Among $F_n = \mathbb{Q}(\sqrt[3]{n})$ of type I, the average of $\#\mathrm{Cl}_F[2]$ is 2.

(b) Among $F_n = \mathbb{Q}(\sqrt[3]{n})$ of type II, the average of $\#\mathrm{Cl}_F[2]$ is $3/2$.

Remark 78. This is not predicted by Sawin–Wood's heuristics because $2 \mid \#S_3$.

Note that (b) is what is predicted among the general class of cubic extensions, but (a) is not!

10.2 Hecke Reciprocity

The main tool in the proof is a Hecke reciprocity. Fix an extension F/K of odd degree m, and we work with relative class groups $\mathrm{Cl}_{F/K} := \mathrm{Cl}_F / \mathrm{Cl}_K$. Now, class field theory explains that $\mathrm{Cl}_{K/F}[2]$ are in bijection with unramified quadratic extensions $F(\sqrt{t})/F$ of F, and we require $\mathrm{N}_{F/K}(t) \in K^{\times 2}$ in order to pick up only 2-torsion of the relative class group. For psychological reasons, we want to realize our glass group as some kind of Selmer group. As such, set

$$M := \ker\left(\operatorname{Res}_{F/K}\mu_2 \xrightarrow{\mathrm{N}} \mu_2\right),$$

which is a group of order 2^{m-1}. Now, one can compute that

$$\mathrm{H}^1(K, M) = ker\left(F^\times/F^{\times 2} \xrightarrow{\mathrm{N}} K^\times/K^{\times 2}\right),$$

which allows us to define a Selmer group $\mathrm{Sel}_2^{\mathrm{unr}}(F/K)$ as being in the pre-image in the following diagram

$$\begin{tikzcd}
\mathrm{Sel}_2^{\mathrm{unr}}(F/K) \arrow[r] \arrow[d] & \mathrm{H}^1(K, M) \arrow[r] \arrow[d] & \ker\left(F^\times/F^{\times 2} \to K^\times/K^{\times 2}\right) \arrow[d] \\
\mathrm{H}^1_{\mathrm{unr}}(K_\mathfrak{p}, M) \arrow[r] & \mathrm{H}^1(K_\mathfrak{p}, M) \arrow[r] & \ker\left(F_\mathfrak{p}^\times/F_\mathfrak{p}^{\times 2} \to K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 2}\right)
\end{tikzcd}$$

for all primes $\mathfrak{p}$. It turns out that this Selmer group is exactly $\mathrm{Cl}_{F/K}[2]$.

Definition 79 (Hecke ideal)**.** For an extension F/K, there is a *Hecke ideal* $H_{F/K} = \operatorname{Disc}_{F/K}\operatorname{Diff}_{F/K}^{-1}$.

Remark 80. It turns out that $H_{F/K}$ has square norm and is in fact a square in the class group. The proof that it is a square is a very strange theorem, and it does not seem to have an application outside this talk.

We are now ready to state Hecke reciprocity.

Definition 81 (Hecke prime)**.** Fix an extnesion F/K. A prime w of F lying over a prime v of K is *Hecke* if and only if the following hold.

- w divides $H_{F/K}$ to an odd power.
- There is a local class $t \in \mathrm{H}^1_{\mathrm{unr}}(K_\mathfrak{p}, M)$ has $t_w \notin F_w^{\times 2}$.

Theorem 82 (Hecke reciprocity)**.** For any $F(\sqrt{t}) \in \mathrm{Cl}_{F/K}[2]$, the number of Hecke primes w inert in $F(\sqrt{t})$ is even.

Proof. This follows from the fact that $H_{F/K}$ is a square in the ideal class. Let $\chi\colon \mathrm{Cl}_F \to \mathbb{Z}/2\mathbb{Z}$ be the character corresponding to $F(\sqrt{t})/F$. Now, one may expand $H_{F/K} = \prod_w w^{\nu_w}$ for some w, and we find that

$$\chi(H_{F/K}) = \sum_w h_w \chi(w)$$

receives nonzero contributions from a prime w if and only if it is Hecke and for which $F(\sqrt{t})/F$ is inert (so that $\chi(w) = 1$). ∎

Remark 83. The result explains the second condition in the definition of Hecke prime: having $t_w \notin F_w^{\times 2}$ is simply saying that the extension $F_w(\sqrt{t})/F_w$ looks inert locally.

Example 84. Fix a cubic extension F/K. Then it turns out that w is Hecke if and only if F_w/K_v is quadratic, ramified, and generated by the square root of a uniformizer.

Example 85. Fix an extension $K(\sqrt[p]{n})/K$ where p is an odd prime. Then the only possible Hecke primes will lie above p. In particular, one can compute that either $(p) = w_1 w_2^{-1}$ or $(p) = w_1^p$. For example, our main theorems take $p = 3$, and the congruence class $n \pmod 9$ correspond to either of those two classes.

Let's now say something about the proof of Theorem 77.

Proof of Theorem 77. We proceed in steps. Let $F_n = \mathbb{Q}(\sqrt[3]{n})$. Then our M_n is order-4 and self-dual.

- Because M is self-dual, there is a cup-product pairing

$$\mathrm{H}^1(\mathbb{Q}, M) \times \mathrm{H}^1(\mathbb{Q}, M) \stackrel{\cup}{\to} \operatorname{Br} \mathbb{Q}[2].$$

  It turns out that this pairing arises from a quadratic form $q\colon \mathrm{H}^1(\mathbb{Q}, M) \to \operatorname{Br} \mathbb{Q}[2]$ given by sending our t to $\frac{1}{3} \operatorname{tr}_{F_n/\mathbb{Q}} tx^2 \in \mathrm{H}^1(\mathbb{Q}, \mathrm{SO}(3))$. Let $q_p\colon \mathrm{H}^1(\mathbb{Q}_p, M) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ be the local version.

- One can compute that the nonzero class $t \in \mathrm{H}^1_{\mathrm{unr}}(\mathbb{Q}_p, M_n)$ lies in the kernel of q_p if and only if p splits as $\lambda_1^2 \lambda_2$ where λ_1 is a Hecke prime. It turns out that this computation re-proves the fact that $H_{F/K}$ is a square.

- There is some "arithmetic invariant theory" which relates the Selmer group $\mathrm{Cl}_F[2] \cong \mathrm{Sel}_2^{\mathrm{unr}}(F/\mathbb{Q})$ to some integral orbits according to some group action. (This is where Hecke reciprocity is used.) This is now something which is understood how to count. ■