Student Number Theory Seminar

Nir Elber

Spring 2024

Contents

1 January 25: Sean Gonzales

We're going to talk about the Ekedahl–Oort stratification.

1.1 Dieudonné Modules

We begin with some motivation. Fix a perfect field k of positive characteristic $p := \operatorname{char} k$. There are three possibilities for an elliptic curve E/k.

- Ordinary: $E[p]\left(\overline{k}\right) \cong \mathbb{Z}/p\mathbb{Z}$.
- Supersingular: $E[p]\left(\overline{k}\right) = 0$.

Notably, $E[p]$ should still have rank p^2 (as a finite flat group scheme). It turns out to be productive to use the theory of Dieudonné modules, which is somehow a linearization of the problem (analogous to how Lie algebras linearizes Lie groups).

Definition 1 (Dieudonné ring)**.** Fix a perfect field k of positive characteristic, and let $W(k)$ denote the ring of Witt vectors. Then the *Dieudonné ring* D_k is the non-commutative $W(k)$-algebra generated by F and V satisfying the relations

$$FV = VF = p \qquad \text{and} \qquad Fw = w^\sigma \qquad \text{and} \qquad wV = Vw^\sigma,$$

where $(-)^\sigma$ is the Frobenius. A *Dieudonné module* is a D_k-module.

Here is why we care.

Theorem 2. Fix a perfect field k of positive characteristic. There is an additive anti-equivalence of categories from finite commutative p-group schemes over k and D_k-modules of finite $W(k)$-length. Given such a group scheme G, we will let $\mathbb{D}G$ denote the D_k-module.

Here are some examples.

Example 3. One has $\mathbb{D}(\underline{\mathbb{Z}/p\mathbb{Z}}) \cong k$ with F being the Frobenius and $V = 0$.

Example 4. One has $\mathbb{D}(\mu_{p,k}) \cong k$ with $F = 0$ and V being the inverse Frobenius.

Example 5. Let α_p denote the kernel of the pth-power map $\mathbb{G}_a \to \mathbb{G}_a$. Then $\mathbb{D}(\alpha_p) \cong k$ with $F = V = 0$.

Example 6. Fix a perfect field k of positive characteristic, and let A be an abelian k-variety. Then we have $\mathbb{D}(A[p]) \cong H^1_{\mathrm{dR}}(A)$. (This isomorphism goes through the crystalline site.) In fact, there is an isomorphism of short exact sequences as follows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(A, \Omega_{A/k}) & \longrightarrow & H^1_{\mathrm{dR}}(A) & \longrightarrow & H^1(A, \mathcal{O}_A) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & (k, \sigma^{-1}) \otimes_k \mathbb{D}(A[F]) & \longrightarrow & \mathbb{D}(A[p]) & \longrightarrow & \mathbb{D}(A[V]) & \longrightarrow & 0 \end{array}$$

Here, (k, σ^{-1}) denotes

So here is another characterization of an elliptic curve E being supersingular.

- Ordinary: $F^* \colon H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E)$ is nonzero; equivalently, $V^* \colon H^0(E, \Omega_{E/k}) \to H^0(E, \Omega_{E/k})$ is nonzero.
- Supersingular: otherwise.

For example, suppose E/k is ordinary. Note that V vanishes on $\mathbb{D}(E[V])$, so we get $\mathbb{D}(E[V]) = \mathbb{D}(\underline{\mathbb{Z}/p\mathbb{Z}})$. Similarly, F vanishes on $\mathbb{D}(A[F])$, so we get $\mathbb{D}(\mu_p)$. Thus, we get a short exact sequence

$$0 \to \mathbb{D}(\mu_p) \to \mathbb{D}(E[p]) \to \mathbb{D}(\underline{\mathbb{Z}/p\mathbb{Z}}) \to 0,$$

which upon reversing $\mathbb{D}$ produces

$$0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \to \mu_p \to 0.$$

This splits at $\mathbb{Z}/p\mathbb{Z} \to E[p]$ by the Frobenius, so $E[p] \cong \mu_p \oplus \mathbb{Z}/p\mathbb{Z}$.

On the other hand, the supersingular case will end up producing a short exact sequence

$$0 \to \alpha_p \to E[p] \to \alpha_p \to 0,$$

which now need not split.

1.2 F-zips

Let X/k be a smooth proper k-scheme. As a technical hypothesis, we want the Hodge to de Rham spectral sequence degenerates at E_1, though I'm not totally sure what that means. In this situation, we get two filtration.

- Hodge filtration: $H^1_{\mathrm{dR}}(X) \supseteq \mathrm{Fil}^1_H \supseteq \mathrm{Fil}^2_H \cdots \supseteq 0$. Set $C_i \coloneqq \mathrm{Fil}^i_H$ for brevity.

- Conjugate filtration: there is an analogous filtration $H^1_{\mathrm{dR}}(X) \supseteq \overline{\mathrm{Fil}^1_H} \supseteq \overline{\mathrm{Fil}^2_H} \cdots \supseteq 0$. Set $D_i \coloneqq \overline{\mathrm{Fil}}_H^{n-i}$ for brevity.

In this situation, we will get a Cartier isomorphism $\sigma^*(C^i/C^{i+1}) \to (D_i/D_{i-1})$.

Example 7. Let A/k be an abelian variety.

- We have $\mathbb{D}(A[p]) = H^1_{\mathrm{dR}}(A)$.
- The first filtration: $H^1_{\mathrm{dR}}(A) \supseteq \ker F \supseteq 0$.
- The second filtration: $0 \subseteq \ker V \subseteq H^1_{\mathrm{dR}}(A)$.
- The Cartier isomorphism: $\operatorname{im} F = \ker V$ and $\ker F = \operatorname{im} V$.

We now package all this data into an F-zip.

Definition 8 (F-zip)**.** Fix an $\mathbb{F}_q$-scheme S. Then an *F-zip* over S is a tuple $(M, C^\bullet, D_\bullet, \varphi_\bullet)$ satisfying some coherence conditions. We define its *type* as the map $\tau\colon \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ by $\tau(i) \coloneqq \dim_k \left(C^i/C^{i+1}\right)$.

We now want to understand F-zips. Continue with A/k as an abelian variety. Then a polarization on A induces a symplectic form on $H^1_{\mathrm{dR}}(A)$. So actually we want to understand F-zips with this extra symplectic structure.

Definition 9 (symplectic F-zip)**.** Fix everything as above. A *symplectic F-zip* is an F-zip $(M, C^\bullet, D_\bullet, \varphi_\bullet)$ such that there is a symplectic form ψ on M, with some coherence conditions. For example, we want $C^\bullet$ and $D_\bullet$ to be symplectic flags (i.e., the symplectic dual spaces of an element of $C^\bullet$ lives in $C^\bullet$, and similar for $D_\bullet$).

So here is a classification result.

Theorem 10. Let k be algebraically closed, and let (V, ψ) be a symplectic k-vector space and let $G = \mathrm{Sp}(V, \psi)$ with Weyl group (W, I). Let τ be an "admissible type" (namely, on the type of our F-zips). Then there is a bijection between isomorphism classes of symplectic F-zips of type τ and $W_j \backslash W$.

The point is that F-zips can be understood from "combinatorial data" from the Weyl group, which are what produce the Ekedahl–Oort stratification.

2 January 31st: Sean Gonzales

Today we're going to define a Shimura datum. To review, let's do an example using Theorem 10.

Example 11. As usual, fix a perfect field k of positive characteristic p, and let E be an elliptic k-curve. Then $W = \mathrm{GSp}_2 = \mathrm{GL}_2$, where our vector space is $H^1_{\mathrm{dR}}(E) \cong k^2$. Fixing a basis $\{e_1, e_2\}$ corresponding to the action, our F-zip can come in two forms.

- Ordinary: $C^\bullet\colon 0 \subseteq ke_1 \subseteq k^2$ and $D_\bullet\colon 0 \subseteq ke_2 \subseteq k^2$.
- Supersingular: $C^\bullet\colon 0 \subseteq ke_1 \subseteq k^2$ and $D_\bullet\colon 0 \subseteq ke_1 \subseteq k^2$.

Notably, ordinary is $(1, 2) \in W$, and supersingular is id.

2.1 Shimura Datum Examples

A Shimura datum will consist of a pair (G, X). Instead of giving a precise definition now, we write out some examples.

Example 12. Elliptic curves over $\mathbb{C}$ can be written as $\mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$ is a lattice, where $\tau \in \mathbb{H}$. Equivalently, we can imagine fixing $\Lambda \coloneqq \mathbb{Z}^2$ and choose an embedding $j \colon \mathbb{R}^2 \to \mathbb{C}$. The point is that choice of $\tau \in \mathbb{H}$ then defines the map $\mathbb{R}^2 \to \mathbb{C}$ given by $(0,1) \mapsto \tau$, which is equivalently defining a map $\mathbb{C}^\times \to \mathrm{GL}_2(\mathbb{R})$.

The point of thinking this way is that the map $\mathbb{C}^\times \to \mathrm{GL}_2(\mathbb{R})$ is really a map $h \colon \mathbb{S} \to \mathrm{GL}_{2,\mathbb{R}}$ where $\mathbb{S} \coloneqq \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_{m,\mathbb{C}})$ is the Deligne torus. With this viewpoint, (Λ, h) is a $\mathbb{Z}$-Hodge structure: $\Lambda \otimes_{\mathbb{C}}$ has basis given by τ and something else, where the point is that h acts by conjugation on one basis vector and identity on the other one.

Anyway, taking X to be the conjugacy class of a particular h (namely, $i \mapsto \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$) has $\mathrm{Sh}(\mathrm{GL}_2, X)$ being the needed modular curve. This Shimura datum "explains" how 2-dimensional $\mathbb{Z}$-Hodge structures correspond to elliptic curves.

Example 13. Abelian varieties over $\mathbb{C}$ can be written as $\mathbb{C}^g/\Lambda$ with a Riemann form $\psi \colon \Lambda \times \Lambda \to \mathbb{Z}$. Again, we can imagine this as fixing $\Lambda \coloneqq \mathbb{Z}^{2g}$ and then choosing an embedding $\mathbb{R}^{2g} \cong \mathbb{C}^g$, but this is equivalent to choosing a map $h \colon \mathbb{C}^\times \to \mathrm{GSp}_{2g}(\psi)$. Then one can tell much the same story, producing a Shimura datum $\mathrm{Sh}(\mathrm{GSp}_{2g}(\psi), X)$.

Example 14. Let's try to parameterize elliptic curves E over $\mathbb{C}$ with an embedding $i \colon \mathbb{Z}[i] \to \mathrm{End}_{\mathbb{C}}(E)$. The elliptic curve itself becomes 2-dimensional Hodge structure, but we should now have some additional $\mathbb{Z}[i]$-module structure. Notably, it's not even clear what our group is.

Well, set $\Lambda \coloneqq \mathbb{Z}^2$ as usual, and provide it with $\mathbb{Z}[i]$-action in the usual way by $i \mapsto \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$. So our group G should have $G(R)$ be the automorphisms of $\Lambda \otimes_{\mathbb{Z}} R$ commuting with the given action of $\mathbb{Z}[i] \otimes_{\mathbb{Z}} R$, which is approximately $R[i]^\times$. So our group ought to be $\mathrm{Res}_{\mathbb{Q}(i)/\mathbb{Q}}(\mathbb{G}_{m,\mathbb{Q}(i)})$. Notably, this group isn't even split!

We are approaching the end of the talk, so we may as well define something.

Definition 15 (reflex field)**.** Fix (G, X). Then the *reflex field* E of (G, X) is the fixed field of the subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which fixes the conjugacy class of the map $z \mapsto h_{\mathbb{C}}(z, 1)$. (This is algebraic over $\mathbb{Q}$ for reasons we will not explain.)

For good enough primes p (for example, we want G to be unramified at p, i.e. split over $\mathbb{Q}_p$), one can reduce $\mathrm{Sh}(G, X)$ modulo $\mathfrak{p} \mid p\mathcal{O}_E$, where $\mathfrak{p} \in V(E)$.

Example 16. We continue Example 14. Odd primes p are good enough. Quickly, note that we have a reductive model of G over $\mathbb{Z}_p$ given by

$$G(R) \coloneqq \mathrm{GL}_{\mathbb{Z}_p[i] \otimes R}\left(\mathbb{Z}_p^2 \otimes R\right).$$

Thus, for example if $p \equiv 1 \pmod 4$, then $\mathbb{Z}_p[i]$ splits into $\mathbb{Z}_p \times \mathbb{Z}_p$, so we are looking at $\mathrm{GL}_{R^2}\left(R^2\right)$, which is $R^\times \times R^\times$. This is $\mathbb{G}_m \times \mathbb{G}_m$, which reduces $\pmod p$ just fine. Going back to the moduli problem, one can track back through to see that we are looking for elliptic $\mathbb{F}_p$-curves E equipped with a map $\mathbb{Z}[i] \to \mathrm{End}(E)$, which is equivalent to being ordinary!

3 February 7th: Sean Gonzales

Today we will talk about Hasse invariants and their generalizations. Throughout today, k is a field of positive characteristic $p \coloneqq \mathrm{char}\, k > 0$.

3.1 Hasse Invariant

Here is a definition, which is perhaps not so helpful.

Definition 17 (Hasse invariant)**.** Fix an elliptic curve E over k. Then the *Hasse invariant* h_E of E is 0 if E is supersingular and is 1 if E is ordinary.

Here is a more advanced definition, which is the same upon defining supersingular and ordinary.

Definition 18 (Hasse invariant)**.** Fix an elliptic curve E over k. Let $F\colon E \to E$ denote the absolute Frobenius. Then the *Hasse invariant* h_E of E is 0 if $F^*\colon H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E)$ is the zero map and 1 if F^* is nonzero (i.e., an isomorphism because $H^1(E, \mathcal{O}_E) \cong k$).

So we've introduced some cohomology. In fact, by using Serre duality, we can move everything into cohomology.

Definition 19 (Hasse invariant)**.** Fix an elliptic curve E over k, and let ω be a basis of $H^0(E, \Omega_E)$, which corresponds canonically to a basis element $\eta \in H^1(E, \mathcal{O}_E)^\vee$ by Serre duality. Letting $F\colon E \to E$ be the absolute Frobenius, then the *Hasse invariant* is the unique $h_{E,\omega} \in k$ such that

$$F^*\eta = h_{E,\omega}\eta.$$

Remark 20. Adjusting $\omega \mapsto \lambda\omega$ makes $\eta \mapsto \lambda^{-1}\eta$, so $h_{E,\lambda\omega} = \lambda^{1-p}h_{E,\omega}$. Thus, one can view $h_{E,\omega}$ has a level 1, weight $p-1$ modular form $\pmod p$.

Remark 21. Locally, we can think about $h_{E,\omega}$ as an element of $H^0\left(E, \underline{\omega}_E^{\otimes(p-1)}\right)$.

We would like to understand these "modular forms" as sections of some line bundles. I need to focus on the exposition, so I am going to stop taking notes.

4 February 14th: Connor James Halleck-Dube

Today we're talking about trace formulae and orbital integrals.

4.1 The Trace Formula

Fix locally compact topological group G. Representation theory might be interested in the decomposition of $L^2(G)$. It turns out $L^2(G)$ is pretty big, so perhaps we might have access to a discrete subgroup $\Gamma \subseteq G$, and we'll ask for representations living $L^2(\Gamma\backslash G)$. If $\Gamma\backslash G$ is in fact compact, then $L^2(\Gamma\backslash G)$ will decompose as a Hilbert space into a sum of irreducible representations, as one expects from representation theory of finite groups.

Example 22. The representations of $\mathbb{R}$ living in $L^2(\mathbb{Z}\backslash\mathbb{R})$ is really asking for representations to S^1, which is basically Fourier analysis. Explicitly, one can argue that

$$L^2(\mathbb{Z}\backslash\mathbb{R}) \cong L^2(\mathbb{Z}) = \widehat{\bigoplus_{n\in\mathbb{Z}}} \mathbb{R}_n,$$

where $\mathbb{R}$ acts on $\mathbb{R}_n$ via the character $r \mapsto \exp(2\pi i n r)$. As a remark, one can even decompose $L^2(\mathbb{R})$, but the decomposition is more complicated because it is no longer "discrete."

Example 23. Fix a finite group G and $\Gamma \subseteq G$ to be any subgroup. Then we are asking for irreducible representations of G when $\Gamma = 1$, and in general we are asking to decompose $\operatorname{Ind}_\Gamma^G 1$.

Example 24. Fix a global field F, and let $\mathbb{A}_F$ be the adéle ring. Given a reductive F-group G, one has a discrete inclusion $G(F) \to G(\mathbb{A}_F)$. The representation theory here is related to the story of modular forms, where G is a real reductive Lie group and $\Gamma \subseteq G$ an arithmetic subgroup.

In our representation theory, one often wants to pick up some tools to do functional analysis.

- One can upgrade the G-action on $L^2(\Gamma\backslash G)$ to a map $R\colon C_c(G) \to \operatorname{End} L^2(\Gamma\backslash G)$ in a way that agrees with the earlier G-action if we view G in $C_c(G)$ as Dirac δs. Explicitly, given $f \in C_c(G)$, we have

$$(Rf)(\varphi)(g) \coloneqq \int_G f(h)\varphi(gh)\,dh.$$

  The point is that if we imagine f as an indicator for some $g \in G$, then we are looking at the desired right translation. Notably, our Haar measure permits

$$(Rf)(\varphi)(g) = \int_G f\left(g^{-1}h\right)\varphi(h)\,dh.$$

  Now, φ is really a function on $\Gamma\backslash G$, so we can first integrate over the quotient as

$$(Rf)(\varphi)(g) = \int_{\Gamma\backslash G}\left(\sum_{\gamma\in\Gamma} f\left(g^{-1}\gamma h\right)\right)\varphi(h)\,dh.$$

  So we are looking at an integral operator via the kernel $K_f(g,h) \coloneqq \sum_{\gamma\in\Gamma} f\left(g^{-1}\gamma h\right)$. Note that this is in fact a finite sum because $\operatorname{supp} f$ is compact and Γ is discrete.

- Now that we have some ring homomorphism, we can define some traces. For some reason, the kernel $K(g,h)$ is approximately analogous to some matrix entries, so we attempt to define

$$\operatorname{tr} Rf \coloneqq \int_{\Gamma\backslash G} K_f(h,h)\,dh.$$

  When $\Gamma \subseteq G$ is cocompact, this integral will always exist, but in general it is a hypothesis on the function that we can take its trace as above.

  Expanding, we can do the same sort of conjugacy class dependence of f to see

$$\operatorname{tr} Rf = \int_{\Gamma\backslash G}\left(\sum_{\gamma\in\Gamma} f\left(h^{-1}\gamma h\right)\right)dh = \sum_{\text{class }[\gamma]} \operatorname{vol}(\Gamma_\gamma\backslash G_\gamma)\int_{G_\gamma\backslash G} f\left(h^{-1}\gamma h\right)\,dh.$$

  Here G_γ and Γ_γ are stabilizers. This is called the "geometric expansion" of the trace formula, and the integrals are "orbital integrals" because we are integrating over orbits.

- On the other side, under the hypothesis that $\Gamma \subseteq G$ is cocompact, we decompose

$$L^2(\Gamma\backslash G) = \widehat{\bigoplus_{\alpha\in\kappa}} \pi_\alpha^{m_\alpha},$$

  so by decomposing the action of some Rf here, we receive

$$\operatorname{tr} Rf = \sum_{\alpha\in\kappa} m_\alpha \operatorname{tr} R(f)|_{\pi_\alpha}.$$

  This is called the "spectral side."

So we have proven the following.

Theorem 25 (Trace formula)**.** Fix a cocompact discrete subgroup Γ of a locally compact topological group G. Given $f \in C_c(G)$, one has

$$\sum_{\text{class } [\gamma]} \operatorname{vol}(\Gamma_\gamma \backslash G_\gamma) \int_{G_\gamma \backslash G} f\left(h^{-1}\gamma h\right)\, dh = \sum_{\alpha \in \kappa} m_\alpha \operatorname{tr} R(f)|_{\pi_\alpha}.$$

Proof. Both sides equal $\operatorname{tr} R(f)$. ∎

The point is that we can try to relate some "geometric" orbital integrals with "spectral" information on irreducible representations.

Example 26. Continue from Example 22. For some $f \in C_c(\mathbb{Z}\backslash\mathbb{R})$, computing Theorem 25 produces

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \widehat{f}(n).$$

The geometric side is direct, and the spectral side depends on the Fourier expansion of f.

Example 27. Continue from Example 23. Then one recovers Burnside's lemma or Frobenius reciprocity.

Example 28. Selberg was able to make Theorem 25 work in the case where $\mathrm{SL}_2(\mathbb{Z}) \subseteq \mathrm{SL}_2(\mathbb{R})$. Selberg then used this along with the fact that geodesics of quotients $\Gamma\backslash\mathbb{H}$ with conjugacy classes in Γ, where (say) Γ is an arithmetic subgroup; comparing this with Theorem 25 allows one to count geodesics by understanding the relevant representation theory.

From here, Arthur extended Theorem 25 to allow $G(F) \subseteq G(\mathbb{A}_F)$ where G is reductive. For example, if G has any parabolic subgroup or any split torus, we are horribly not compact, so the geometric side of Theorem 25 can become infinite. The idea was to modify Theorem 25 via adding in some alternating sum of parabolic subgroups in order to cancel out some infinities.

4.2 Orbital Integrals

Let's examine our orbital integrals

$$O_\gamma(f) \coloneqq \int_{G_\gamma(\mathbb{A}_F)\backslash G(F)} f\left(g^{-1}\gamma g\right)\, dg,$$

where $\gamma \in \Gamma$ and $f \in C_c^\infty(G(\mathbb{A}_F))$ (where the ∞ means some smoothness that we will not be precise about). Here, F is a global field, so working over $\mathbb{A}_F$ allows us to perhaps decompose the integral into a product of local orbital integrals.

Example 29. Take $G \coloneqq \mathrm{GL}_2$ and $F_v \coloneqq \mathbb{Q}_p$ and $\gamma \coloneqq \left[\begin{smallmatrix} a & \\ & b \end{smallmatrix}\right]$ for $a - b \in \mathcal{O}_v^\times$. Then we can ask for the integral

$$O_\gamma = \int_{G_\gamma(F_v)\backslash G(F_v)} 1_{g^{-1}\gamma g \in G(\mathcal{O}_v)}\, dg,$$

which we can compute via some explicit combinatorics. For example, it turns out to be a rational function in p.