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.

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

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 $C_i := \mathrm{Fil}^i_H$ 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 $D_i := \overline{\mathrm{Fil}_H^{n-i}}$ 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 $\tau(i) := \dim_k \left(C^i/C^{i+1}\right)$.

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 $\Lambda := \mathbb{Z}^2$ 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 $\mathbb{S} := \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_{m,\mathbb{C}})$ 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 $\Lambda := \mathbb{Z}^{2g}$ 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 $\Lambda := \mathbb{Z}^2$ 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

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

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!