MOVING FROM ABELIAN VARIETIES OVER $\mathbb{C}$ TO ABELIAN VARIETIES TO $\mathbb{F}_p$

JOEL SPECTER

Let X be a curve. If X is over $\mathbb{C}$, there is an alternating bilinear form on the homology lattice, given by the cup product:

$$H^1(X;\mathbb{Z}) \times H^1(X;\mathbb{Z}) \to \mathbb{Z}.$$

We saw that $H^1(X;\mathcal{O}_X)/H^1(X;\mathbb{Z})$ has the structure of an abelian variety.

More generally, for any curve X, we can define its **Jacobian** as the functor $\mathrm{Jac}(X)$ that sends a scheme T to the set of line bundles on $A \times T$ that are degree zero over each fiber $X \times \{t\}$ and trivial over each fiber $\{x\} \times T$. In the above case, this is just the kernel of $c_1 : H^1(X, \mathcal{O}_X^\times) \to \mathbb{Z}$, which is $H^1(X;\mathcal{O}_X)/H^1(X;\mathbb{Z})$.

As it turns out, this is actually projective, and you can write it as a quotient of some $\mathrm{Sym}^k(X)$. This is what motivated Weil to give the abstract definition of an abelian variety. That's great, but doesn't help us get our hands on these things. Over $\mathbb{C}$, the data of a complex torus is just given by a lattice $\pi_1(T) \cong H_1(T;\mathbb{Z}) \hookrightarrow \mathbb{C}^d$. One way to algebraize this is to replace the topological $\pi_1(T)$ by the algebraic fundamental group,

$$\pi_1^{et}(T) = \varprojlim_{Y \twoheadrightarrow T} \mathrm{Aut}(Y)$$

where Y ranges over finite étale covers of T. In particular, a map $\pi_1^{et}(T) \to \mathbb{Z}/N$ corresponds to a cover $Y \to T$ with $\mathbb{Z}/N$ as its deck transformation group.

Let Λ be a lattice in $H_1(T;\mathbb{Z})$. There's some N such that

$$NH_1(T;\mathbb{Z}) \subseteq \Lambda \subseteq H_1(T;\mathbb{Z}),$$

and this gives a chain of covers of tori

$$\mathbb{C}^d/NH_1(T;\mathbb{Z}) \twoheadrightarrow \mathbb{C}^d/\Lambda \twoheadrightarrow \mathbb{C}^d/H_1(T;\mathbb{Z}),$$

where the first and last tori are isomorphic. So we get a duality between the category of covers of T and the category of tori covered by T. But a cover $T \twoheadrightarrow Y$ of degree N is equivalent to an N-torsion point of T. Thus we get

$$\pi_1^{et}(T) \cong \varprojlim_{N \in \mathbb{N}} T[N] \cong \prod_p \varprojlim_{k \in \mathbb{N}} T[p^k].$$

Definition 1. The **ℓ-adic Tate module** of an abelian variety A over a field K is $T_\ell A = \varprojlim A[\ell^n](\overline{K})$.

If ℓ is not equal to the characteristic prime p, then $T_\ell A$ is a good stand-in for the first homology group of A. This is a $\mathbb{Z}_\ell$-module and has commuting actions by $\mathrm{Gal}(\overline{K}/K)$ and $\mathbb{Z}_\ell \otimes \mathrm{End}_K(A)$. As a $\mathbb{Z}_\ell$-module, it's isomorphic to $\mathbb{Z}_\ell^{2d}$.

Let A be an abelian scheme over $\mathbb{Z}_p$. This means that it's projective and each of its fibers are abelian varieties – in this case, that means that $A_{\mathbb{F}_p}$ and $A_{\mathbb{Q}_p}$ are abelian varieties. For example, A could be the elliptic curve defined by the projective equation

$$x^3 + z^3 = y^2 z,$$

Typed by Paul VanKoughnett.

for $p \neq 2, 3$. We can go from $\mathbb{Q}_p$ points to $\mathbb{F}_p$ points: any $\mathbb{Q}_p$ point can be represented as $[\alpha_1, \alpha_2, \alpha_3]$ where α_i all lie in $\mathbb{Z}_p$ but do not all lie in $p\mathbb{Z}_p$, and we can then reduce this mod p to get $[\overline{\alpha_1}, \overline{\alpha_2}, \overline{\alpha_3}] \in A_{\mathbb{F}_p}(\mathbb{F}_p)$. The kernel of this map corresponds to deformations

$$\begin{tikzcd} \operatorname{Spec}(\mathbb{Z}/p^N) \arrow[r] \arrow[d] & A_{\mathbb{Z}_p} \arrow[d] \\ \operatorname{Spec}(\mathbb{F}_p) \arrow[r, "e"'] & A_{\mathbb{F}_p}, \end{tikzcd}$$

or rather the inverse limit of these as N goes to ∞. One can check that this is just the formal group of A, that is, its formal completion at the identity. On the other hand, we can also pass to $A_{\mathbb{Q}_p}$, and thence to $A_{\overline{\mathbb{Q}_p}}$. But $\overline{\mathbb{Q}_p}$ is isomorphic to $\mathbb{C}$! Moreover, we have

$$\operatorname{End}(A_{\overline{\mathbb{Q}_p}}) \cong \operatorname{End}(A_{\overline{\mathbb{Z}_p}}) \hookrightarrow \operatorname{End}(A_{\overline{\mathbb{F}_p}}).$$

One consequence of this is that the complex result that the Tate module is free of rank $2d$ is also true over a finite field.

Here's an example. Let X_5 be defined by the projective equation $x^5 + y^5 = z^5$ over $\mathbb{F}_2$. This is a smooth curve of degree 5 in $\mathbb{P}^2$. Its genus is

$$\binom{d-1}{n} = \binom{4}{2} = 6.$$

Thus, its Jacobian is a 6-dimensional abelian variety. The ℓ-adic Tate module, for any $\ell \neq 2$, this is a $\mathbb{Z}_\ell$-module of rank 12. So

$$V_\ell(\operatorname{Jac} X_5) := T_\ell(\operatorname{Jac} X_5) \otimes \mathbb{Q}_\ell$$

is a 12-dimensional vector space, and Tate showed that this abelian variety is classified by the characteristic polynomial of the Frobenius endomorphism acting on this vector space. (For any $\ell \neq 2$!)

But we still don't know what $\operatorname{Jac} X_5$ is. One approach to finding its π_1 is to find covers of X_5 and use the functoriality of Jac. Another approach is the fact that

$$V_\ell^\vee = H^1_{et}((\operatorname{Jac} X_5)_{\overline{\mathbb{F}_2}}; \mathbb{Q}_\ell),$$

the first étale cohomology group; and as it turns out, this is isomorphic to $H^1_{et}((X_5)_{\overline{\mathbb{F}_2}}; \mathbb{Q}_\ell)$. There's also a comparison theorem which tells us that this étale cohomology with $\mathbb{Z}_\ell$ coefficients is isomorphic to the *singular* cohomology of $(X_5)_\mathbb{C}$ with $\mathbb{Z}_\ell$ coefficients. Finally, the Frobenius action acts on $H^2_{sing}((X_5)_\mathbb{C}; \mathbb{Z}_\ell) \cong \pi_1(\mathbb{C}^\times) \otimes \mathbb{Z}_\ell \cong \mathbb{Z}_\ell$ by multiplying by p, and on $H^0_{sing}((X_5)_\mathbb{C}; \mathbb{Z}_\ell) \cong \mathbb{Z}_\ell$ trivially. We thus obtain the Lefschetz theorem:

$$|X_5(\mathbb{F}_q)| = 1 - \operatorname{Tr} \operatorname{Frob}_p^N + p^N,$$

where $q = p^N$.

Joel then drew a table with these point counts for X_5, and used them to show that in this case, the Jacobian is just a product of elliptic curves, and has no rational points – thus proving Fermat's Last Theorem when $n = 5$!