Fall 2023 Caltech Number Theory Learning Seminar: Introduction

September 27, 2023

1 Analytic Picture

We begin by looking at complex tori. Let $V \cong \mathbb{C}^g$ be a complex vector space of dimension $g \geq 1$, and let $\Lambda \subset V$ be a lattice of full rank. So $\Lambda \cong \mathbb{Z}^{2g}$ as a group and $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \cong V$. Then the quotient

$$X := V/\Lambda$$

is a complex manifold of dimension g called a complex torus. When $g = 1$ and $V = \mathbb{C}$, then this is an elliptic curve.

However, not all complex tori can be realized as a variety because they cannot be embedded into projective space $\mathbb{P}^N$ for some N. However, by a theorem of Lefschetz, we can classify those that do precisely by whether they have a Riemann form on them.

Theorem 1 (Lefschetz)**.** *Suppose $X = V/\Lambda$ is a complex torus. Then X can be embedded into $\mathbb{P}^N$ if and only if there exists a positive definite Hermitian form $H: V \times V \to \mathbb{C}$ (so $H(v,w) = \overline{H(w,v)}$ and $H(v,v) > 0$ for $v \neq 0$) such that $\mathrm{Im} H|_{\Lambda \times \Lambda} \in \mathbb{Z}$.*

The complex tori that do have such a Hermitian form are abelian varieties.

Example 2. Any complex torus of dimension $g = 1$ is automatically abelian varieties. That is because we scale our lattice Λ so it is generated by 1 and $\tau \in \mathbb{H}$, then take $H(v,w) = \frac{v\overline{w}}{\mathrm{Im}(\tau)}$.

This is over $\mathbb{C}$, but as number theorists, we would like to talk about abelian varieties over any (number) field. So, we have the following definition.

Definition 3. An abelian variety is a proper algebraic variety X with a group law $m: X \times X \to X$ such that m and the inverse are both algebraic morphisms.

Remark. Here, proper can be thought of as compact. Notice how the group law is also not required to be commutative, but, it turns out that it automatically is abelian.

Proposition 4. *Suppose X is a complex compact Lie group. Then the group structure on X is commutative.*

Proof. Consider the commutator function $f(x,y) = xyx^{-1}y^{-1}$ on $X \times X$. Let $U \subset X$ be an open neighborhood of the identity element $e \in X$. Then for any $x \in X$, we have $f(x,e) = e$ so continuity gives us open neighborhoods $V_x \ni x, W_x \ni e$ such that $f(V_x, W_x) \subset U$. We can find open neighborhoods for all $x \in X$. Since X is compact, there are finitely many x so that the V_x cover X and letting $W = \bigcap W_x$ for such x, we get an open neighborhood $W \ni e$ such that $f(X,W) \subset U$.

Now we use a strong property of holomorphic functions. Every holomorphic function $g: M \to \mathbb{C}$ from a compact complex manifold is constant. Since X is compact and we can embed U as an open subset in $\mathbb{C}^g$, we get that $f(X,W)$ is constant and equal to e. Then since f is constant on an open subset of the domain, it is constant everywhere so $f(X,X) = e$ and X is commutative. $\square$

However, this proof relies on looking at the analytic properties of X and of complex holomorphic functions. In order to prove that the group structure of abelian varieties are commutative, we need to look at the line bundles of X and a rigidity lemma. This is Lecture 2.

Also, we have only defined abelian varieties X to be proper (compact). Not all proper varieties are projective (see Hartshorne II.7.13). In order to show that there is a closed embedding of $X \to \mathbb{P}^N$ into projective space, we will need a theorem of the cube for abelian varieties. This is Lecture 3.

For every abelian variety A, we can also construct a dual abelian variety $A^\vee$. Over $\mathbb{C}$, if we write $A \cong V/\Lambda$, then the dual can be written as

$$A^\vee \cong V^\vee/\Lambda^\vee,$$

where the dual is taken as vector spaces. However, for general abelian varieties, we will need to define it another way using line bundles and the Picard group of A. It has nice properties such as for every isogeny $f\colon A \to B$, meaning that the map is surjective with finite kernel, there is a dual isogeny $f^\vee\colon B^\vee \to A^\vee$. Moreover, given any ample line bundle $\mathcal{L}$ on A, we get an isogeny

$$\lambda_{\mathcal{L}}\colon A \to A^\vee$$

called a polarization. This is the subject of Lecture 4.

2 CM Theory

For an abelian variety A, we can look at the endomorphism algebra $\mathrm{End}(A)$. We can add an element to itself multiple times which gives a map $\mathbb{Z} \to \mathrm{End}(A)$. But, the endomorphism ring could be bigger. If the ring is of largest size, then we say that A has complex multiplication (CM).

Definition 5. If $\mathrm{End}(A) \otimes_Z \mathbb{Q}$ has a commutative $\mathbb{Q}$-subalgebra of dimension $2g$, then A has CM.

An easy picture is when $g = 1$ and A is an elliptic curve. This is saying that the endomorphism algebra of A is an order of a quadratic field $K = \mathbb{Q}(\sqrt{D})$. An endomorphism $V/\Lambda \to V/\Lambda$ sends $\Lambda \to \Lambda$, and hence A has CM if Λ itself is an order inside K, meaning that K is an imaginary quadratic field. So, the picture is $A(\mathbb{C}) \cong \mathbb{C}/\mathcal{O}_K$. In general, we take F to be a totally real field of degree g over $\mathbb{Q}$ and K/F a totally imaginary quadratic extension. Then a CM abelian variety A will have an action by an order $\mathcal{O}_K$ of K. The fundamental theorem of complex multiplication gives a functorial map between ideals of K and abelian varieties with CM by K. By using this functoriality property, we can get results like the following.

Theorem 6. *Let A be an elliptic curve over $\mathbb{C}$ with complex multiplication by an order of a quadratic imaginary field K. Then $j(E)$ is algebraic and $K(j(E))$ is an abelian extension of K. If $\mathrm{End}(A) = \mathcal{O}_K$ is the maximal order, then $K(j(E))$ is the Hilbert class field of K.*

This and further results is the content of Lecture 5.

3 Finite Field Case Theorems

We can also consider abelian varieties defined over finite fields $\mathbb{F}_q$. There is a classical finiteness result.

Theorem 7. *Fix a dimension $g > 0$. There are only finitely many abelian varieties over $\mathbb{F}_q$ of dimension g, up to isomorphism.*

The proof of this result comes from using the Weil pairing, a map $e_m \colon A[m] \times A^\vee[m] \to \mu_m$, with $\gcd(m, q) = 1$.

In addition, let $N_m = |A(\mathbb{F}_{q^m}|$. Then one of Weil's conjectures is that

$$|N_m - q^{mg}| \leq 2gq^{m(g-1)/2} + (2^{2g} - 2g - 1)q^{m(g-1)}.$$

When $g = 1$ and A is an elliptic curve, this says that $|N_m - q^m - 1| \leq 2\sqrt{q^m}$, which is also known as the Hasse bound.

We can construct a local ζ-function for A by defining

$$\zeta(A, t) = \exp\left(\sum_{m=1}^{\infty} N_m \frac{t^m}{m}\right).$$

Then, the other part of Weil's conjectures concern an analog of the Riemann Hypothesis. It says that the zeroes of the ζ-function occur for t with $\mathrm{Re}(t) = \frac{1}{2}, \frac{3}{2}, \ldots, \frac{2g-1}{2}$, and the poles occur at $\mathrm{Re}(t) = 0, 1, 2, \ldots, g$.

Another question that we can ask is if we have an abelian variety A defined over $\mathbb{F}_p$, does it come from taking an abelian variety originally defined over $\mathbb{Z}$ or $\mathbb{Z}_p$, and taking it modulo p? And if that is the case, can we recover the original abelian variety? These lifting questions concern deformations of abelian varieties and p-divisible groups. Serre and Tate proved that there is a way to canonical choose a lifting of an abelian variety to $\mathbb{Z}_p$.

A subset of these topics will be the content of Lectures 6 and 7.

4 Mordell–Weil Theorem

Theorem 8 (Mordell Conjecture (1922))**.** *Let K be a number field and C/K be a projective smooth curve of genus $g \geq 2$. Then $|C(K)| < \infty$.*

Faltings proved this in 1983 by reducing it to a question about abelian varieties. This was proven with the following reductions. First, a trick of Parshin showed that it suffices to show that there are only finitely many curves over K of fixed genus with good reduction outside a finite set of places S. Then, by taking the Jacobian of a curve, it suffices to prove that there are finitely many abelian varieties of dimension g over K with good reduction outside S. This is done in two steps. First, by looking at the Tate module

$$T_\ell(A) := \varprojlim_n A[\ell^n](\overline{K})$$

as a Galois module, Faltings shows that there are finitely many isogeny classes of abelian varieties. Then, by looking at the moduli space of abelian varieties of dimension g $\mathcal{A}_g$ and looking at height functions on it, we get there there are finitely many abelian varieties in a single isogeny class. These two results combine to give the Mordell–Weil Theorem. An in depth dive into this proof is the content of Lectures 8 and 9.