LECTURE 11: ELLIPTIC CURVES AND PERIOD INTEGRALS

STEPHEN MCKEAN

1. What is an elliptic curve?

Last time, we gave two definitions of elliptic curves over $\mathbb{C}$. I'll recall them here after reminding you of the motivation.

Our first encounter with these was as the complex tori $\mathbb{C}/\Lambda$. As a manifold, this is smooth, compact, and has genus 1. But we can also think about this as an abelian group, where the group operation comes from addition in $\mathbb{C}$, and the identity is the image of Λ. This leads to two plausible definitions of an elliptic curve over $\mathbb{C}$.

Definition 1.1. An *elliptic curve* over $\mathbb{C}$ is a smooth, projective algebraic curve of genus 1.

Definition 1.2. An *elliptic curve* over $\mathbb{C}$ is an abelian variety of dimension 1.

I need to tell you what an abelian variety is. First, I have to tell you what an algebraic group is.

Definition 1.3. An *algebraic group* over a field k is an algebraic variety G with a distinguished element $e \in G(k)$ and regular maps $\mu : G \times G \to G$ (the group operation) and $i : G \to G$ (the inversion) that satisfy the group axioms. So for example, $\mu(x, i(x)) = \mu(i(x), x) = e$ for all $x \in G$.

Exercise 1.4. Let $\mathbb{G}_m := \operatorname{Spec}(k[x, y]/(xy - 1))$. Find $\mu : \mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m$ and $i : \mathbb{G}_m \to \mathbb{G}_m$ that endow $\mathbb{G}_m$ with the structure of an algebraic group.

Lemma 1.5. *Any (geometrically reduced, locally finite type) algebraic group G over a field k is smooth.*

Proof. Recall that $G \to \operatorname{Spec} k$ is smooth if and only if $G_{\overline{k}} \to \operatorname{Spec} \overline{k}$ is smooth, which holds if each $\overline{k}$-point of $G_{\overline{k}}$ is smooth. If G is geometrically reduced, then $G_{\overline{k}}$ is reduced and thus contains a smooth point. Now $G_{\overline{k}}(\overline{k})$ acts transitively on itself (by translations), so every other point of $G_{\overline{k}}(\overline{k})$ must be smooth. □

The following definition is slightly different from what I said last time, and it may surprise you at first.

Definition 1.6. An *abelian variety* is a proper (geometrically reduced, locally finite type) algebraic group over a field.

Why is this surprising? The only condition we've really added is properness — we said nothing about the group law being commutative! It turns out that properness will imply commutativity.

Lemma 1.7. *The group structure on any abelian variety is commutative.*

Proof. If K/k is a field extension and G is an algebraic group over k, then G_K is an algebraic group over K. (This boils down to checking that the group axioms still hold after base changing the morphisms μ and i.) Properness is also stable under base change, so it follows that if A is an abelian variety over k, then $A_{\overline{k}}$ is an abelian variety over $\overline{k}$. If the group law on $A_{\overline{k}}$ is commutative, then so is the group law on A. To save on notation, we'll just assume $k = \overline{k}$.

Since A is proper (and reduced and locally finite type), any morphism $A \to A$ is finite in an open neighborhood of any chosen point. In particular, for each $x \in A(k)$, the morphism

$$\begin{aligned} \phi : A \times A &\to A \times A \\ (x, y) &\mapsto (x, xyx^{-1}y^{-1}) \end{aligned}$$

is finite in an open neighborhood of x. Here, $xyx^{-1}y^{-1} = \mu(\mu(x, y), \mu(i(x), i(y))$. For $x = e$, we see that $\phi(x, y) = (x, e)$ in this neighborhood. In particular, $(x, y) \mapsto xyx^{-1}y^{-1}$ is the constant function e in a neighborhood of the identity. By translating by k-points, we find that $(x, y) \mapsto xyx^{-1}y^{-1}$ is the constant function e on all of $A \times A$, so the group operation on A is commutative. □

Remark 1.8. Sometimes you'll see projective instead of proper in the definition of an abelian variety. Projectivity is a stronger condition in general, although proper and projective coincide for smooth curves and surfaces.

Now we can show that the two definitions of elliptic curves over $\mathbb{C}$ coincide.

Exercise 1.9. Prove that every abelian variety of dimension 1 has genus 1.

Hint: use the group structure to show that every abelian variety has trivial tangent bundle. For curves, the tangent bundle is dual to the canonical bundle. Use the adjunction formula to compute the canonical bundle of a smooth, projective curve of genus g.

Lemma 1.10. *A smooth, projective curve of genus 1 is an abelian variety.*

Proof. Let E be a smooth, projecitve curve of genus 1. Recall that a *divisor* on a curve is a formal sum

$$D = \sum_{P \in E} n_P [P],$$

where P ranges over the closed points of E and $n_P \in \mathbb{Z}$ are zero for all but finitely many P. The set of divisors of E, together with formal addition of divisors, forms the *Picard group* $\mathrm{Pic}(E)$. The *degree* of a divisor gives us a homomorphism (of abelian groups)

$$\begin{aligned} \deg : \mathrm{Pic}(E) &\to \mathbb{Z} \\ \sum_{P \in E} n_P[P] &\mapsto \sum_{P \in E} n_P \cdot [k(P) : k]. \end{aligned}$$

Here, $k(P)$ is the residue field of P, which is a finite extension of k (since P is a closed point).

A *principal divisor* is a divisor of the form

$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f)[P],$$

where f is some rational function on E and $\mathrm{ord}_P(f)$ is the order of vanishing of f at P. Every principal divisor on a projective curve has degree 0: this is the sum of orders of zeros minus the sum of orders of poles. You can cleverly set up some contour integrals to check that the roots and poles must cancel each other out.

Now we come to a special group, $\mathrm{Pic}^0(E) := \{\text{degree 0 divisors}\}/\{\text{principal divisors}\}$. This definition works for any curve, and there's a better definition for more general varieties. For curves, the choice of a k-rational point $O \in E(k)$ gives us a map

$$\begin{aligned} J : E &\to \mathrm{Pic}^0(E) \\ P &\mapsto [P] - \deg P[O] + \{\text{principal divisors}\}. \end{aligned}$$

To see that this map is injective, we need to see that $[P] - \deg P[O]$ is not principal unless $P = O$. If this divisor were principal, then $[P]$ and $[O]$ would be linearly equivalent, which means that there would be a rational curve (i.e. a $\mathbb{P}^1$) through both P and O. But smooth, proper curves of genus at least 1 do not contain any copies of $\mathbb{P}^1$ (see Exercise 1.11).

So once we see that J is surjective, the abelian group structure on $\mathrm{Pic}^0(E)$ will determine an abelian group structure on E. The key here is Riemann–Roch. I'll go quickly at this point, since defining everything carefully will take us down too many rabbit holes.

Given $D \in \mathrm{Pic}^0(E)$, Riemann–Roch for elliptic curves implies $h^0(D + [O]) = 1$. Thus if $f \in H^0(E, D + [O])$ is not constant, there must be some $[P]$ such that $\mathrm{div}(f) = [P] - [O] - D$. Now $\deg D = \deg(\mathrm{div}(f)) = 0$, we find that $\deg[P] = \deg[O] = 1$, so $[P] - [O] \sim D$. □

Exercise 1.11. Prove that if X is a smooth, proper curve of genus $g \geq 1$, then there is no non-trivial rational map $\mathbb{P}^1 \to X$.

We can also derive the group law geometrically using the motto, "Three colinear points sum to 0." More concretely, given $A, B \in E$, we draw the line through A and B, calculate the third point of intersection $C \in E$ (which we have by Bézout's theorem), and then we reflect across $y = 0$.

Exercise 1.12. Derive the geometric description of the group law from the group law on $\mathrm{Pic}^0(E)$.

Exercise 1.13. Given an elliptic curve $E = \mathbb{V}(y^2 - x^3 - ax - b)$, write code that implements the geometric description of the group law on E. You'll need to calculate the line through two points, find the third intersection point, and reflect $y \mapsto -y$.

1.1. **Elliptic curves over other fields.**

Remark 1.14. We defined elliptic curves over other fields as well. Do the two definitions coincide in these cases? Well, abelian varieties always come equipped with a k-rational point (that plays the role of the base point), whereas genus 1 curves need not have any k-rational points at all. So in general, we need to include the data of a k-rational point in our definition of an elliptic curve.

Exercise 1.15. Show that a smooth, proper curve E over a field k with a k-rational point is an abelian variety if and only if E has genus 1.

Remark 1.16. Given an algebraic group G over a field k, we get a group structure on $G(k)$. In particular, the k-rational points of an elliptic curve form an abelian group. If $k = \mathbb{C}$, then $E(\mathbb{C})$ will not be a finitely generated abelian group, since $E(\mathbb{C})$ will be uncountable.[1] Mordell's theorem tells us that $E(\mathbb{Q})$ is always finitely generated.

So when $k = \mathbb{Q}$, we get two new invariants of an elliptic curve: the rank and torsion of $E(\mathbb{Q})$. We know a lot about the torsion, thanks to Barry Mazur:

Theorem 1.17 (Mazur)**.** *The torsion subgroup of $E(\mathbb{Q})$ is $\mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 10$ or $n = 12$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ for $1 \leq m \leq 4$. Moreover, each of these cases is known to occur.*

The rank of $E(\mathbb{Q})$ is much harder to get a handle on. The elliptic curve with largest confirmed rank has rank 20, due to Noam Elkies and Zev Klagsbrun. There are also examples whose rank is between 21 and 28, although it is not known exactly which of these integers actually gives the rank. The general conjecture is that there should be elliptic curves with arbitrarily large rank, although a fairly recent heuristic of Park–Poonen–Voight–Matchett Wood suggests that there are only finitely many elliptic curves of rank greater than 20. It's safe to say that Boston is the place to be if you want to learn about $E(\mathbb{Q})$.

[1] A finitely generated abelian group is a finite union of countable sets, which cannot be uncountable.

2. Recovering the lattice from an elliptic curve

Recall that we have a biholomorphism

$$\begin{aligned}\Phi : \mathbb{C}/\Lambda &\to \mathbb{V}(y^2z - 4x^3 + g_2xz^2 + g_3z^3)\\ 0 &\mapsto [0:1:0]\\ z &\mapsto [\wp(z) : \wp'(z) : 1]\end{aligned}$$

for any non-degenerate lattice Λ (so $g_2^3 - 27g_3^2 \neq 0$). Now suppose I hand you an equation $y^2 = 4x^3 - ax - b$ with $a^3 - 27b^2 \neq 0$. How do I recover Λ?

Well, let E be your complex elliptic curve. Let $\alpha, \beta \subset E$ be closed paths giving a basis of $H_1(E;\mathbb{Z})$. (Remember that E is a torus – try drawing a basis of H_1.) It follows that $\Phi^{-1} \circ \alpha$ and $\Phi^{-1} \circ \beta$ will give a basis of $H_1(\mathbb{C}/\Lambda;\mathbb{Z})$. We have a natural isomorphism

$$\begin{aligned}H_1(\mathbb{C}/\Lambda;\mathbb{Z}) &\to \Lambda\\ \gamma &\mapsto \int_\gamma \mathrm{d}z,\end{aligned}$$

so two generators of Λ can be calculated as $\omega_1 := \int_{\Phi^{-1}\circ\alpha} \mathrm{d}z$ and $\omega_2 := \int_{\Phi^{-1}\circ\beta} \mathrm{d}z$. All that remains is to express these as integrals on E. The chain rule says $\mathrm{d}\wp(z) = \wp'(z)\mathrm{d}z$, so

$$\begin{aligned}\mathrm{d}z &= \frac{\mathrm{d}\wp(z)}{\wp'(z)}\\ &= \Phi^*\left(\frac{\mathrm{d}x}{y}\right).\end{aligned}$$

Now we can compute

$$\begin{aligned}\omega_1 &= \int_{\Phi^{-1}\circ\alpha} \mathrm{d}z\\ &= \int_{\Phi^{-1}\circ\alpha} \Phi^*\left(\frac{\mathrm{d}x}{y}\right)\\ &= \int_\alpha \frac{\mathrm{d}x}{y},\end{aligned}$$

and similarly for ω_2. If you want to write this as an integral involving just one variable, we get

$$\omega_1 = \int_\alpha \frac{\mathrm{d}x}{\sqrt{4x^3 - ax - b}}.$$

Remark 2.1. Elliptic integrals strike again! These elliptic integrals are often called *period* integrals, since they calculate the periods of $\wp$ (which in turn give us the generators of Λ). Inspired by these definitions, you can define a *period* to be any number that you obtain by integrating a differential form over an algebraic variety.

It turns out that essentially every number we know about is a period. Just like algebraic numbers are more complicated than rational numbers but are still accessible to the

human mind, so too are periods more complicated than algebraic numbers but still familiar to us.

If you want to learn more about periods, go read the amazing notes of Kontsevich and Zagier [KZ01]. There you will learn that every algebraic number is a period, that periods form a ring that is conjectured (but not known) to not be a field, and that the only examples of known non-periods are bizarre (e.g. [Yos08]). Some well-known numbers like e and

$$\gamma = \int_1^\infty \left(-\frac{1}{x} + \frac{1}{\lfloor x \rfloor} \right) \mathrm{d}x$$

are conjecturally non-periods. It is a straightforward exercise to show that the ring of periods is a countable set (once you have a definition given), and yet this countable set accounts for basically any complex number you can think of.

Exercise 2.2. If I were mean, I might hand you an equation of the form $y^2 = x^3 + ax + b$. This should still define an elliptic curve, but I've changed the variables to obfuscate the connection to $\wp$. Your exercise is to undo my meanness.

Compute the lattice associated to the elliptic curve defined by the vanishing of $y^2 = x^3 + ax + b$. It's okay if you leave your answer in terms of elliptic integrals.

Exercise 2.3. If you actually want to get numbers for ω_1 and ω_2, you better have equations for the paths α and β. Find such equations for the elliptic curve defined by $y^2 = x^3 + ax + b$.

Next time: moduli of elliptic curves.

References

[KZ01] Maxim Kontsevich and Don Zagier. "Periods". In: *Mathematics unlimited—2001 and beyond*. Springer, Berlin, 2001, pp. 771–808. URL: https://www.ihes.fr/~maxim/TEXTS/Periods.pdf.

[Yos08] Masahiko Yoshinaga. *Periods and elementary real numbers*. 2008. arXiv: 0805.0349 [math.AG].

Department of Mathematics, Harvard University

Email address: smckean@math.harvard.edu

URL: shmckean.github.io