Attribution Key

for more information see: http://open.umich.edu/wiki/AttributionPolicy

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

Public Domain – Government: Works that are produced by the U.S. Government. (17 USC § 105)

Public Domain – Expired: Works that are no longer protected due to an expired copyright term.

Public Domain – Self Dedicated: Works that a copyright holder has dedicated to the public domain.

Creative Commons – Zero Waiver

Creative Commons – Attribution License

Creative Commons – Attribution Share Alike License

Creative Commons – Attribution Noncommercial License

Creative Commons – Attribution Noncommercial Share Alike License

GNU – Free Documentation License

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

Public Domain – Ineligible: Works that are ineligible for copyright protection in the U.S. (17 USC § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

Fair Use: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (17 USC § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

Lecture 2: Elliptic curves

This lecture covers the basics of elliptic curves. I begin with a brief review of algebraic curves. I then define elliptic curves, and talk about their group structure and defining equations. Following this is the theory of isogenies, including the important fact that degree is quadratic. Next is the complex theory: elliptic curves are one-dimensional tori. Finally, I talk about the Tate module and Weil pairing.

A good reference for this lecture is Silverman's "The arithmetic of elliptic curves" (MR0817210), especially chapters II, III, and VI.

1 Review of curves

1.1 Divisors

Let k be a field. Let C/k be an algebraic curve (smooth, projective, and connected). A divisor on C is a formal sum $\sum_{x \in C} n_x[x]$, where n_x is an integer and all but finitely many of the n_x are 0. The set of divisors forms a group, $\mathrm{Div}(C)$.

We define the degree of $x \in C$ to be the the degree of the extension $k(x)/k$, where $k(x)$ is the residue field at x. The degree of a divisor $D = \sum n_x[x]$, denoted $\deg(D)$, is $\sum n_x \deg(x)$. We thus have a homomorphism $\deg\colon \mathrm{Div}(X) \to \mathbf{Z}$. We let $\mathrm{Div}^0(X)$ be its kernel.

We write $D \geq 0$ if $n_x \geq 0$ for all x; such divisors are said to be effective. We write $D \geq D'$ to mean $D - D' \geq 0$.

Let f be a non-constant function on C. We define the divisor of f, denoted $\mathrm{div}(f)$, as $\sum v_x(f)[x]$, where $v_x(f)$ denotes the valuation of f at x, i.e., the order of zero or pole of f at x. An important theorem states that $\mathrm{div}(f)$ has degree 0; in other words, the number of zeros of f is equal to the number of poles of f, when multiplicities are taken into account. A divisor of the form $\mathrm{div}(f)$ is called principal. The set of principal divisors forms a group $\mathrm{PDiv}(X)$.

The divisor class group of X, denoted $\mathrm{Cl}(X)$, is the quotient $\mathrm{Div}(X)/\mathrm{PDiv}(X)$. Since principal divisors have degree 0, it makes sense to speak of the degree of a divisor class, and we have a subgroup $\mathrm{Cl}^0(X)$.

Let $f\colon X \to Y$ be a map of curves. Given a divisor $D = \sum n_x[x]$ on X, we let $f_*(D)$ be the divisor $\sum n_x[f(x)]$ on Y. Given a divisor $D = \sum n_y[y]$ on Y, we let $f^*(D)$ be the divisor $\sum_{y \in Y} \sum_{f(x)=y} e(x|y) n_y[x]$ on X, where $e(x|y)$ is the ramification index. Both f_* and f^* are homomorphisms and preserve principal divisors. Furthermore, we have $f_*(f^*(D)) = \deg(f)D$.

1.2 Riemann–Roch

Let D be a divisor on X. Define $\mathcal{L}(D)$ to be the set of functions f on X with $\mathrm{div}(f) \geq -D$. (This includes the zero function.) For example, if $D = [x]$ then $\mathcal{L}(D)$ consists of functions which have at worst a simple pole at x and are holomorphic everywhere else. It's easy to see that $\mathcal{L}(D)$ is a k-vector space. Note that if $\deg(D) < 0$ then $\mathcal{L}(D) = 0$, since the divisor of a function has degree 0. We let $\ell(D)$ be the dimension of $\mathcal{L}(D)$.

Theorem 1 (Riemann–Roch)**.** *We have $\ell(D) - \ell(K - D) = \deg(D) - g + 1$, where g is the genus of C and K is the so-called canonical divisor, which has degree $2g - 2$.*

Corollary 2. *If $\deg(D) > 2g - 2$ then $\ell(D) = \deg(D) - g + 1$.*

These are notes for Math 679, taught in the Fall 2013 semester at the University of Michigan by Andrew Snowden.

Proof. With this hypothesis, $\deg(K - D) < 0$, and so $\ell(K - D) = 0$. □

Special case: if C has genus 1 then $\ell(D) = \deg(D)$ for $\deg(D) > 0$.

1.3 Separability

Let $f\colon X \to Y$ be a non-constant map of curves. We then have an extension of function fields $k(X)/k(Y)$. Field theory implies that there is a maximal intermeidate field K such that $k(X)/K$ is purely inseparable and $K/k(Y)$ is separable. Going back to geometry, this means that we can factor f as $X \xrightarrow{g} X' \xrightarrow{h} Y$, where g is purely inseparable and h is separable. We define the separable degree of f to be the degree of h, and the inseparable degree of f to be the degree of g.

Suppose k has characteristic p and X is given by the equation $f(x, y) = 0$. Let $f^{(p)}(x, y)$ be the polynomial obtained by raising all the coefficients of f to the pth power, and let $X^{(p)}$ be the curve defined by $f^{(p)}(x, y) = 0$. If $f(x, y) = 0$ then $f(x, y)^p = 0$. But since we're in characteristic p, raising to the pth power is a ring homomorphism, and so $f(x, y)^p = f^{(p)}(x^p, y^p)$. It follows that $(x, y) \mapsto (x^p, y^p)$ defines a map of curves $F_p\colon X \to X^{(p)}$. This map is called the Frobenius map, and is purely inseparable. We can similarly define a Frobenius map for powers of p.

The Frobenius map is essentially the only example of a purely inseparable map: a map $X \to Y$ factors as $X \to X^{(q)} \to Y$, where the first map is F_q and the second map is separable. Of course, q is in the inseparable degree of f.

In characteristic 0, all maps are separable.

2 Elliptic curves

Definition 3. An elliptic curve is a pair $(E, 0)$ where E is a genus 1 curve over k and 0 is a k-point of E. □

2.1 Group law

Proposition 4. *The map $E(k) \to \mathrm{Cl}^0(E)$ given by $x \mapsto [x] - [0]$ is an isomorphism.*

Proof. Suppose D is a degree 0 divisors on E. Then $\ell(D + [0]) = 1$ by Riemann–Roch. Let $f \in \mathcal{L}(D + [0])$ be non-constant. Then necessarily $\mathrm{div}(f) = -D - [0] + [x]$ for some $x \in E$ of degree 1, i.e., $x \in E(k)$. Thus $D = [x] - [0]$ in $\mathrm{Cl}(E)$. This proves surjectivity. Injectivity is left to the reader. □

Since $\mathrm{Cl}^0(E)$ is a group, the above isomorphism allows us to define a group structure on $E(k)$. In fact, E itself is a group variety, that is, the group law on $E(k)$ is induced from a map of varieties $E \times E \to E$.

2.2 Equations

The space $\mathcal{L}([0])$ obviously contains the constant functions. By Riemann–Roch, $\ell([0]) = 1$, and so $\mathcal{L}([0])$ consists exactly of the constant functions.

We have $\ell(2[0]) = 2$, and so $\mathcal{L}(2[0])$ contains a non-constant function; call it x.

We have $\ell(3[0]) = 3$, and so $\mathcal{L}(3[0])$ contains a function which does not belong to the span of 1 and x; call it y.

We have $\ell(4[0]) = 4$, but we know what the new function is: it's just x^2.

Similarly, we have $\ell(5[0]) = 5$, but we know what the new function is: it's xy.

Finally, we have $\ell(6[0]) = 6$. But we know two new functions: x^3 and y^2. We therefore have 7 functions in $\mathcal{L}(6[0])$, namely, 1, x, y, x^2, xy, x^3, and y^2. It follows that there is a linear dependence:

$$a_1y^2 + a_2x^3 + a_3xy + a_4x^2 + a_5y + a_6x + a_7 = 0$$

This equation defines a plane curve E', and we have a natural map $E \to E'$ taking a point $p \in E$ to $(x(p), y(p))$. One can show that this map is an isomorphism of projective curves. Thus every elliptic curve is given by an equation of the above form.

Assume now that k is not of characteristic 2 or 3. Then using a simple change of variables we can eliminate many of the above terms and reach an equation of the form

$$y^2 = x^3 + ax + b$$

Let us call this equation (or the curve it defines) $E_{a,b}$. By putting $y = u^{-3}y_1$ and $x = u^{-2}x_1$, for some non-zero $u \in k$, we see that $E_{a,b}$ is isomorphic to E_{u^4a,u^6b}. In fact, these are the only isomorphisms between these curves.

2.3 Discriminant and j-invariant

We have shown that every elliptic curve is of the form $E_{a,b}$, but are all $E_{a,b}$ elliptic curves? The answer is no: some of them are singular. In fact, $E_{a,b}$ is singular if and only if the discriminant $\Delta = -16(4a^3 + 27b^2)$ vanishes. If Δ is non-zero then $E_{a,b}$ is an elliptic curve.

We have therefore shown that the set of isomorphism classes of elliptic curves over k is naturally in bijection with the set of pairs $(a, b) \in k^2$ with $\Delta \neq 0$, modulo the equivalence $(a, b) \sim (u^4a, u^6b)$ for $u \in k^\times$.

Define $j = -1728(4a)^3/\Delta$. The constants here are not so important. It's clear that j is invariant under the equivalence relation. Thus j is an invariant of elliptic curves: it is called the j-invariant. Using what we have stated above, it is easy to see that if k is algebraically closed then two elliptic curves are isomorphic if and only if they have the same j-invariant. This is not true, in general, if k is not closed.

3 Isogenies

3.1 Definition and examples

Definition 5. An isogeny $f\colon E_1 \to E_2$ is a non-constant map of curves with $f(0) = 0$. □

One can show that any isogeny is a group homomorphism. We let $\mathrm{Hom}(E_1, E_2)$ denote the set of isogenies, together with the zero morphism. This is a group, via the group law on either E_2. In fact, it is a free abelian group of finite rank. We write $\mathrm{End}(E)$ for $\mathrm{Hom}(E, E)$. This is a ring, where multiplication is composition.

Example 6. The multiplication-by-n map, denote $[n]\colon E \to E$, is an isogeny. We regard $\mathbf{Z}$ as a subring of $\mathrm{End}(E)$ by $n \mapsto [n]$. □

Example 7. If k has characteristic p, then the Frobenius map $F_q\colon E \to E^{(q)}$ is an isogeny. □

3.2 Basic results

Proposition 8. *Let $f\colon E_1 \to E_2$ be an isogeny of separable degree n and inseparable degree m.*

- *For any $y \in E_2(\overline{k})$, the set $f^{-1}(y) \subset E_1(\overline{k})$ has n elements.*
- *For any $y \in E_2$ and any $x \in E_1$ lying over y, the ramification index $e(x|y)$ is equal to m.*
- *The map f is everywhere unramified if and only if $m = 0$; this is automatic in characteristic 0.*

Proposition 9. *Let E_1 and E_2 be elliptic curves and let ω_1 and ω_2 be non-zero global differentials on them.*

- *An isogeny f is separable if and only if $f^*(\omega_2)$ is non-zero.*
- *For an isogeny f define $\alpha(f) \in k$ by $f^*(\omega_2) = \alpha(f)\omega_1$. Then $\alpha\colon \mathrm{Hom}(E_1, E_2) \to k$ is a group homomorphism.*
- *If $E_1 = E_2$ and $\omega_1 = \omega_2$ then α is a ring homomorphism.*

Corollary 10. *The isogeny $[n]\colon E \to E$ is separable if and only if n is prime to the characteristic of k.*

3.3 Dual isogeny

Proposition 11. *Let $f\colon E_1 \to E_2$ be an isogeny. Then there exists an isogeny $f^\vee\colon E_2 \to E_1$, called the dual isogeny, such that the following diagram commutes.*

$$\begin{array}{ccc} E_2(k) & = & \mathrm{Cl}^0(E_2) \\ {\scriptstyle f^\vee}\downarrow & & \downarrow{\scriptstyle f^*} \\ E_1(k) & = & \mathrm{Cl}^0(E_1) \end{array}$$

In fact, this diagram continues to commute if we pass to extensions of k, and this uniquely specifies $f^\vee$. With a little more sophistication, one can construct $f^\vee$ using this diagram.

We have the following two important facts: (1) $f^\vee f = [\deg f]$; and (2) $(f+g)^\vee = f^\vee + g^\vee$. These can be deduced easily from the above characterization of $f^\vee$ and properties of f^*.

3.4 The quadratic nature of degree

Let E_1 and E_2 be elliptic curves and let $\Lambda = \mathrm{Hom}(E_1, E_2)$, a finite free $\mathbf{Z}$-module. For $f, g \in \Lambda$, define an element $\langle f, g\rangle$ of $\frac{1}{2}\mathbf{Z}$ by

$$2\langle f, g\rangle = \deg(f+g) - \deg(f) - \deg(g).$$

Using the identity $\deg(f) = f^\vee f$, we find

$$2\langle f, g\rangle = f^\vee g + g^\vee f.$$

It follows that $\langle , \rangle$ is bilinear. The above expression shows that $\langle f, f\rangle = \deg(f)$, which shows that $\langle , \rangle$ is positive definite. It also shows that deg is a quadratic function.

An important corollary of this discussion is that $\deg([n]) = n^2$. This follows from the quadratic nature of deg and the obvious fact that $\deg([1]) = 1$.

4 Elliptic curves over the complex numbers

4.1 Uniformization

Let E be an elliptic curve over $\mathbf{C}$, and identify E with its complex points. Then E is a genus 1 surface. Its universal cover is therefore the complex numbers, and, in fact, the covering map $\pi\colon \mathbf{C} \to E$ is a group homomorphism. The kernel of π is a lattice Λ, i.e., a subgroup of $\mathbf{C}$ such that the map $\Lambda \otimes \mathbf{R} \to \mathbf{C}$ is an isomorphism. We note that Λ is naturally identified with the homology $\mathrm{H}_1(E, \mathbf{Z})$. Note that if f is a meromorphic function on E then $f \circ \pi$ is a doubly-periodic meromorphic function on $\mathbf{C}$, that is, it is invariant by translation by any element of Λ.

Now suppose that Λ is a lattice in $\mathbf{C}$, and let $E = \mathbf{C}/\Lambda$ (and $0 = \pi(0)$). Then E is a genus 1 Riemann surface. Riemann's theory implies that E is an algebraic curve. To prove this, one must construct meromorphic functions on E, which amounts to constructing meromorphic functions on $\mathbf{C}$ with period lattice Λ. The basic example of such a function is the Weierstrass $\wp$ function, defined by

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda^*} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2},$$

where here $\Lambda^* = \Lambda \setminus \{0\}$. The derivative $\wp'(z)$ is also doubly periodic, and satisfies an equation of the form

$$\wp'(z)^2 = 4\wp(z)^3 + a\wp(z) + b.$$

Thus $z \mapsto (\wp(z), \wp'(z))$ defines an isomorphism of E with a plane algebraic curve.

4.2 Isogenies

Suppose $E_1 = \mathbf{C}/\Lambda_1$ and $E_2 = \mathbf{C}/\Lambda_2$. Then one can show that $\mathrm{Hom}(E_1, E_2)$ is naturally in bijection with the set of complex numbers $\alpha \in \mathbf{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$. The map corresponding to α is an isogeny if and only if $\alpha \neq 0$, and an isomorphism if and only if $\alpha\Lambda_1 = \Lambda_2$. We can thus say that the set of isomorphism classes of elliptic curves over $\mathbf{C}$ is naturally in bijection with the set of lattices in $\mathbf{C}$ modulo scaling (aka, homothety).

4.3 Complex multiplication

Let Λ be a lattice. Scaling Λ, we can assume it is generated by 1 and some complex number τ. Let's example $\mathrm{End}(E)$. Suppose $\alpha\Lambda \subset \Lambda$. Then $\alpha \cdot 1 \in \Lambda$, and so $\alpha = a + b\tau$ for integers a and b. Similarly, $\alpha\tau \in \Lambda$, and so $\alpha\tau = c + d\tau$ for integers c and d. If $b = 0$ then $\alpha \in \mathbf{Z}$, which is not so interesting. But if $b \neq 0$ then, combining the equations, we find

$$b\tau^2 + (a-d)\tau - c = 0,$$

which shows that τ, and thus α as well, belongs to a quadratic subfield K (necessarily imaginary) of $\mathbf{C}$. In fact, α must belong to an order of K, which shows that $\mathrm{End}(E)$ is an order in a quadratic imaginary field. We thus find that $\mathrm{End}(E)$ is either $\mathbf{Z}$ or an order in a quadratic imaginary field. In the latter case, we say that E has complex multiplication (CM).

As an example, suppose Λ is generated by 1 and i. Then multiplication by i induces an endomorphism $[i]$ of E. In fact, E is given by the equation $y^2 = x^3 + x$, and the map $[i]$ is given by $(x, y) \mapsto (-x, iy)$.

5 The Tate module and Weil pairing

5.1 The Tate module of an elliptic curve

Let E/k be an elliptic curve and let n be an integer coprime to the characteristic of k. From what we have said above, it follows that $[n]$ is a separable map of degree n^2. Thus all fibers of the map $n\colon E(\overline{k}) \to E(\overline{k})$ have cardinality n^2; in other words, $E[n](\overline{k})$ has cardinality n^2, where $E[n]$ is the kernel of the isogeny $[n]$ (regarded as a subscheme of E). If n is prime then this implies that $E[n](\overline{k}) = (\mathbf{Z}/n\mathbf{Z})^2$. The same conclusion holds for composite n using an inductive argument involving all divisors of n.

Let ℓ be a prime number different from the characteristic. The ℓ-adic Tate module of E, denoted $T_\ell(E)$, is the inverse limit of the groups $E[l^n](\overline{k})$, where the transition maps are multiplication by ℓ. Explicitly, an element of $T_\ell(E)$ is a sequence $(x_0, x_1, \ldots)$ of $\overline{k}$-points of E, where $x_0 = 0$ and $\ell x_i = x_{i-1}$ for $i > 0$. The results of the previous paragraph imply that $T_\ell(E)$ is isomorphic to $\mathbf{Z}_\ell^2$.

If $k = \mathbf{C}$ and $E = \mathbf{C}/\Lambda$ then the n-torsion of E is $\frac{1}{n}\Lambda/\Lambda$. It follows that $T_\ell(E)$ is naturally isomorphic to $\Lambda \otimes \mathbf{Z}_\ell$. Thus $T_\ell(E)$ is very close to just being Λ. Over a general field, one should think of $T_\ell(E)$ as the best possible replacement for the lattice Λ.

An extremely important property of the Tate module which cannot be seen in the complex picture is its Galois action. If k is not algebraically closed then the n-torsion of E will typically not be defined over k, and so the absolute Galois group $G_k = \mathrm{Gal}(\overline{k}/k)$ will move the n-torsion points around. This carries through the inverse limit, and so there is an action of G_k on $T_\ell(E)$. Picking a basis for $T_\ell(E)$, this action can be thought of as a homomorphism $\rho\colon G_k \to \mathrm{GL}_2(\mathbf{Z}_\ell)$, i.e., an ℓ-adic representation of the Galois group. This perspective has proved to be very useful.

5.2 The Tate module of the multiplicative group

The multiplicative group, denoted $\mathbf{G}_m$ is the algebraic group which represents the functor $R \mapsto R^\times$ (where R is a k-algebra). As a scheme, it is simply $\mathbf{A}^1 \setminus \{0\}$, i.e., $\mathrm{Spec}(k[t, t^{-1}])$.

The construction of the Tate module in the previous section can be applied equally well to $\mathbf{G}_m$. If n is prime to the characteristic then the n-torsion $\mathbf{G}_m[n]$ is just the group of nth roots of unity; its $\overline{k}$-points is isomorphic to $\mathbf{Z}/n\mathbf{Z}$. It follows that $T_\ell(\mathbf{G}_m)$ is isomorphic to $\mathbf{Z}_\ell$ as a group. Of course, it also carries a Galois action, which can be recorded as a homomorphism $\chi\colon G_k \to \mathrm{GL}_1(\mathbf{Z}_\ell) = \mathbf{Z}_\ell^\times$. This homomorphism is called the cyclotomic character, and describes how the Galois group acts on roots of unity.

A common notation, which we will use, is to write $\mathbf{Z}_\ell(1)$ for $T_\ell(\mathbf{G}_m)$. The idea is that the underlying group is $\mathbf{Z}_\ell$ and the (1) records that the Galois group is acting through the first power of the cyclotomic character.

5.3 The Weil pairing

In what follows, I'll abbreviate $E[n](\overline{k})$ to $E[n]$ and write μ_n for the nth roots of unity in $\overline{k}$.

Proposition 12. *Let E/k be an elliptic curve and let n be prime to the characteristic. Then there exists a pairing $e_n\colon E[n] \times E[n] \to \mu_n$ satisfying the following:*

- *Bilinear: $e_n(x + y, z) = e_n(x, z)e_n(y, z)$. (Note: the group law on $E[n]$ is typically written additively, while that on μ_n is written multiplicatively.)*
- *Alternating: $e_n(x, x) = 1$. This implies $e_n(x, y) = -e_n(y, x)$, but is stronger if n is even.*
- *Non-degenerate: if $e_n(x, y) = 1$ for all $y \in E[n]$ then $x = 0$.*

- *Galois equivariant:* $e_n(\sigma x, \sigma y) = \sigma e_n(x, y)$ *for* $\sigma \in G_k$.
- *Compatibility: if* $x \in E[nm]$ *and* $y \in E[n]$ *then* $e_{nm}(x, y) = e_n(mx, y)$.

The compatibility condition allows us to take the inverse limit of the e_{ℓ^n} to obtain a pairing on the Tate module

$$\langle , \rangle \colon T_\ell(E) \times T_\ell(E) \to \mathbf{Z}_\ell(1).$$

The properties of the Weil pairing imply that the above pairing induces an isomorphism $\bigwedge^2(T_\ell E) \cong \mathbf{Z}_\ell(1)$. In other words, if one regards the Tate module as a two dimensional Galois representation ρ, the Weil pairing implies that $\det(\rho) = \chi$, the cyclotomic character.

The Weil pairing has another important compatibility property:

Proposition 13. *Let* $f \colon E_1 \to E_2$ *be an isogeny, let* $x \in E_1[n]$*, and let* $y \in E_2[n]$*. Then* $e_n(f(x), y) = e_n(x, f^\vee(y))$*, where* $f^\vee$ *is the dual isogeny.*

From this, we can deduce the following useful result:

Proposition 14. *Let* $f \colon E \to E$ *be an isogeny. Then* $\deg(f) = \det(f \mid T_\ell E)$.

Proof. Suppose $x, y \in T_\ell(E)$. Then $\langle f(x), f(y) \rangle = \det(f) \langle x, y \rangle$. This is essentially the definition of the determinant! On the other hand, we have $\langle f(x), f(y) \rangle = \langle f^\vee(f(x)), y \rangle$, and $f^\vee f = [\deg f]$. This completes the proof. □