Algebraic Curves/Fall 2015

Aaron Bertram

2. Elliptic Curves. Let $\Lambda \subset \mathbb{C}$ be a lattice.

That is, Λ is a free abelian group of rank 2, embedded in $\mathbb{C}$ via:

$$\iota : \mathbb{Z}^2 \to \mathbb{C}; \quad \iota(1,0) = \omega_1,\ \iota(0,1) = \omega_2$$

for complex numbers ω_1, ω_2 that are not real multiples of each other.

The choice of generators for Λ is arbitrary, and will be taken up later. The quotient:

$$E_\Lambda = \mathbb{C}/\Lambda$$

is a Riemann surface of genus one (a torus!) with an origin and the (additive) structure of a group. This is an **elliptic curve**.

We can embed E_Λ in the complex plane $\mathbb{CP}^2$ via the doubly periodic meromorphic **Weierstrass function**:

$$\mathcal{P}(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

(where $\Lambda^* = \Lambda - \{(0,0)\}$), and its derivative:

$$\mathcal{P}'(z) = -\frac{1}{2} \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}$$

Remark. The "correction terms" in the sum for $\mathcal{P}$ are necessary for convergence of the sum, but they create another issue, addressed in:

Exercise 2.1. Show that $\mathcal{P}(z)$ is a meromorphic function on E_Λ, i.e. that the sum converges to a meromorphic function on $\mathbb{C}$ satisfying:

$$\mathcal{P}(z+\omega) = \mathcal{P}(z) \text{ for all } \omega \in \Lambda$$

and that $\mathcal{P}(z)$ is even, with power series expansion:

$$\mathcal{P}(z) = z^{-2} + az^2 + bz^4 + \cdots$$

for some uniquely determined constants $a, b \in \mathbb{C}$.

Thus in particular, $\mathcal{P}$ determines a map:

$$\mathcal{P} : E_\Lambda \to \mathbb{CP}^1$$

that is 2:1 (because of the double pole) at all but finitely many points, at which it is 1:1 (with multiplicity two). One of these "branch" points is the point at infinity, and it follows from topological considerations that there are three others (because E_Λ is a torus), but we may also see this by analyzing power series expansions.

Namely,

$$\mathcal{P}'(z) = -2z^{-3} + 2az + 4bz^3 + ...$$
$$\mathcal{P}'(z)^2 = 4z^{-6} - 8az^{-2} - 16b + ...$$
$$\mathcal{P}(z)^3 = z^{-6} + 3az^{-2} + 3b + ...$$

from which it follows (matching coefficients) that:

$$\mathcal{P}'(z)^2 = 4\mathcal{P}(z)^3 - 20a\mathcal{P}(z) - 28b + f(z)$$

where $f(z)$ is a holomorphic, doubly periodic function with $f(0) = 0$. But this implies that $f(z) = 0$, by the maximum principle.

In other words, the image of:

$$(\mathcal{P}, \mathcal{P}') : E_\Lambda^* \to \mathbb{C}^2$$

satisfies the polynomial relation:

$$y_2^2 = 4y_1 - 20ay_1 - 28 = 4(y_1 - \lambda_1)(y_1 - \lambda_2)(y_1 - \lambda_3)$$

where $\lambda_1 + \lambda_2 + \lambda_3 = 0, \lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_1\lambda_3 = -5a$ and $\lambda_1\lambda_2\lambda_3 = 7b$. But we can say more. Since $\mathcal{P}'(z)$ is odd and periodic, it follows that:

$$\mathcal{P}'(z) = 0 \text{ for all two-torsion elements of } E_\Lambda$$

There are three of these (up to translation by Λ), namely,

$$\frac{\omega_1}{2}, \ \frac{\omega_2}{2}, \ \frac{\omega_1 + \omega_2}{2}$$

and it follows that:

$$\{\lambda_1, \lambda_2, \lambda_3\} = \left\{\mathcal{P}\left(\frac{\omega_1}{2}\right), \mathcal{P}\left(\frac{\omega_2}{2}\right), \mathcal{P}\left(\frac{\omega_1 + \omega_2}{2}\right)\right\}$$

and that the two-torsion elements are the three other branch points of:

$$\mathcal{P} : E_\Lambda \to \mathbb{CP}^1$$

We can extend the map $(\mathcal{P}, \mathcal{P}')$ to a map to $\mathbb{CP}^2$:

$$\Phi = (1 : \mathcal{P}(z) : \mathcal{P}'(z)) = (z^3 : z^3\mathcal{P}(z) : z^3\mathcal{P}'(z)) : E_\Lambda \to \mathbb{CP}^2$$

which is an embedding, with image cut out by the single cubic equation:

$$x_0x_2^2 - 4(x_1 - \lambda_1x_0)(x_1 - \lambda_2x_0)(x_1 - \lambda_3x_0) = 0$$

and $\Phi(0) = (0 : 0 : -2) = (0 : 0 : 1)$ for the "missing" origin.

Exercise 2.2. Consider the second derivative $\mathcal{P}''(z)$.

(a) Find a quadratic relation among $\mathcal{P}'', \mathcal{P}$ and 1.

(b) Find a second quadratic relation among $\mathcal{P}'', \mathcal{P}', \mathcal{P}$ and 1.

(c) Show that $(1 : \mathcal{P} : \mathcal{P}' : \mathcal{P}'')$ embeds E_Λ in $\mathbb{CP}^3$ as the set of zeroes of two homogeneous quadratic polynomials in x_0, x_1, x_2, x_3.

Suppose $\phi(z)$ is a meromorphic function on E_Λ, i.e. a meromorphic function on $\mathbb{C}$ that is doubly periodic with respect to Λ. Then:

(i) The divisor $\mathrm{div}(\phi)$ on E_Λ has degree zero.

(ii) The *point* of E_Λ obtained by evaluating the divisor:

$$\mathrm{div}(\phi) = \sum d_i p_i$$

in the abelian group E_Λ is the origin.

Condition (ii) may be viewed as an obstruction to solving:

$$\mathrm{div}(\phi) = D - D'$$

for effective divisors D, D' of the same degree on E_Λ. If $D - D' \neq 0 \in E_\Lambda$ when evaluated in the abelian group E_Λ, then D and D' are not linearly equivalent divisors. The converse is true, and will be discussed later.

To see how (i) and (ii) may be proved analytically, given ϕ, then a fundamental (parallelogram) domain for the action of Λ on $\mathbb{C}$ may be chosen whose (oriented) boundary Γ meets no zeroes of poles of ϕ or ϕ'. Then (i) and (ii) follow from the contour integrals (see, e.g. Ahlfors):

$$\frac{1}{2\pi i}\int_\Gamma \frac{\phi'(\zeta)}{\phi(\zeta)} d\zeta = \deg(\mathrm{div}(\phi)), \quad \frac{1}{2\pi i}\int_\Gamma \zeta \frac{\phi'(\zeta)}{\phi(\zeta)} d\zeta = \mathrm{div}(\phi)$$

where the latter is evaluated on the elliptic curve. By periodicity, it follows that the first integral is zero and that the second evaluates to a point of Λ, hence to the origin in E_Λ.

Property (i) is, as mentioned in §1, a general property of the degrees of "principal" divisors, but property (ii) is particular to elliptic curves (which are the only curves that are simultaneously groups). If we apply it to rational functions of the form:

$$\phi(z) = A\mathcal{P}'(z) + B\mathcal{P}(z) + C$$

then we see that *three points on the curve*

$$y_2^2 = 4(y_1 - \lambda_1)(y_1 - \lambda_2)(y_1 - \lambda_3)$$

sum to zero if and only if they are collinear! This is nearly enough to completely determine the group law (only an origin is lacking). We will see later how an arbitrary "irreducible" plane curve of degree three is an abelian group with this collinearity property and a choice of an inflection point for the origin.

Turning to an aribtrary (smooth, projective) algebraic curve C:

Definition 2.1. To each effective divisor D on C, we associate:

$$L(D) := \{\phi \in K(C) \mid \mathrm{div}(\phi) + D \geq 0\} \cup \{0\} \subseteq K(C)$$

which is a vector space with $l(d) := \dim_{\mathbb{C}} L(D)$

Remark. $L(D)$ is a vector space because the order of zero of:

$$\phi + \psi$$

is bounded below by the minimum of the orders of zeroes of ϕ and ψ. For now we will see this using the analytic viewpoint, in which near each point $z_0 \in C$, there is an analytic local coordinate z and then:

$$\phi(z) = c_d(z - z_0)^d + ..., \quad \psi(z) = c'_e(z - z_0)^e + ...$$

and if we assume that $d < e$, then:

$$(\phi + \psi)(z) = c_d(z - z_0)^d + ...$$

has order of vanishing d while if $d = e$, then:

$$(\phi + \psi)(z) = (c_d + c'_e)(z - z_0)^d + ...$$

vanishes to order d when $c_d \neq -c'_e$ greater than d when $c_d = -c'_e$.

Proposition 2.1. For all effective divisors D on C:

$$l(D + p) \leq l(D) + 1$$

Proof. Suppose $\phi, \psi \in L(D+p) - L(D)$ and $D = \sum d_i p_i + dp$. Then $\phi(z) = c_{-d-1}(z - z_0)^{-d-1} + ...$ and $\psi(z) = c'_{-d-1}(z - z_0)^{-d-1} + ...$, where z is a local coordinate on C with $z(p) = z_0$, and $c_{-d-1}, c'_{-d-1} \neq 0$. Then: $(\phi - \left(c_{-d-1}/c'_{-d-1}\right)\psi)(z) = a_{-d}(z - z_0)^{-d} + ... \in L(D)$. Since all pairs of vectors $\phi, \psi \in L(D+p) - L(D)$ have the property that $\phi - \lambda\psi \in L(D)$ for some scalar λ, it follows that $\dim(L(D + p)/L(D)) \leq 1$. □

Corollary 2.2. $l(D) \leq \deg(D) + 1$ with equality if and only if either:

(i) $D = 0$, or else (ii) $C = \mathbb{CP}^1$.

Proof. Exercise 2.3.

Definition 2.2 The *linear series* of an effective divisor D' on C is the projective space:

$$|D'| = \{\text{effective divisors } D \text{ on } C \mid D \sim D'\}$$

and $r(D') = l(D') - 1$ is the dimension of the projective space $|D'|$.

Remark. If $\phi \in L(D')^*$, then $\mathrm{div}(\phi) = D - D'$ defines a divisor $D \in |D'|$, and conversely, given $D \in D'$, then the rational function $\phi \in L(D)$ satisfying $\mathrm{div}(\phi) = D - D'$ is determined by D up to a scalar multiple. Thus $|D'|$ is the space of lines through the origin in $L(D')$, which is the projective space $\mathbb{CP}^{r(D')}$ (after a choice of basis of $L(D')$ is chosen).

Example 2.1. One "seed" function determines all the vector spaces:

$$L(p) \subset L(2p) \subset L(3p) \subset .....$$

on the Riemann sphere $\mathbb{CP}^1$ and elliptic curves E_Λ

In the case of $\mathbb{CP}^1$, we may assume $p = 0 = (0 : 1)$, and then:

$$\langle 1, z^{-1}, z^{-2}, \ldots, z^{-n} \rangle = L(np)$$

and stringing them together gives the map to the rational normal curve:

$$\phi_n = (1 : z^{-1} : ... : z^{-n}) = (z^n : z^{n-1} : ... : 1) : \mathbb{CP}^1 \to \mathbb{CP}^n$$

while in the case of E_Λ, if we assume $p = 0$ is the origin, then:

$$\langle 1, \mathcal{P}, \mathcal{P}', \ldots, \mathcal{P}^{(n-2)} \rangle = L(np)$$

with a "gap" at $n = 1$, so that $l(np) = n$ for all $n \geq 1$.

Remark. We could have used a sequence of derivatives of z^{-1} instead of powers. This would have only changed the functions by constant multiples. The comparison between derivatives of $\mathcal{P}$ and powers of $\mathcal{P}$ is the source of the polynomial relations defining the image of E_Λ.

Definition 2.3. A curve C of genus $g \geq 2$ is *hyperelliptic* if there is a point $p \in C$ and a non-constant function $\phi \in L(2p)$.

Remarks. We will see that there are hyperelliptic curves of all genera, and that there are **non**-hyperelliptic curves of every genus $g \geq 3$. We will also see that

$$\phi : C \to \mathbb{CP}^1 \quad \text{has } 2g + 2 \text{ branch points}$$

if C has genus g and that

$$\langle 1, \phi, \phi^2, ..., \phi^n \rangle = L(2np) \text{ for all } n \leq g$$

so there are "gaps" where the vector spaces $L(0) \subseteq L(p) \subseteq \cdots \subseteq L(mp)$ don't jump at odd values of m but there will be an extra rational function $\psi \in L((2g + 1)p$ so that:

$$\langle 1, \phi, \phi^2, ..., \phi^g, \psi \rangle = L((2g + 1)p)$$

and the dimensions of $L(mp)$ thereafter are strictly increasing, so there are no subsequent gaps in the sequence.

Finally, consider the *moduli* of elliptic curves. It is immediate that:

$$E_\Lambda \cong E_{\lambda\Lambda} \text{ for } \lambda \in \mathbb{C}^*$$

as Riemann surfaces and so restricting to pairs (ω_1, ω_2) so that:

$$\omega_1 = 1 \quad \text{and} \quad \text{Im}(\omega_2) > 0$$

produces every elliptic curve (up to isomorphism). Let $\tau := \omega_2$.

The change of basis action of $\mathrm{SL}(2,\mathbb{Z})$ on $\langle \omega_1, \omega_2 \rangle$ converts into an action on bases $\langle 1, \tau = \omega_1/\omega_2 \rangle$ by linear fraction transformations:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} (\tau) = \frac{a\tau + b}{c\tau + d}$$

that preserve the property that $\mathrm{Im}(\tau) > 0$, since:

$$\mathrm{Im}\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{\mathrm{Im}(\tau)}{||c\tau + d||^2}$$

Notice that $-1 \in SL(2,\mathbb{Z})$ has no effect, and it is the quotient of the τ-upper-half plane by this action of $\mathrm{PSL}(2,\mathbb{Z}) = SL(2,\mathbb{Z})/\pm 1$ that is the moduli space of elliptic curves. Since the action of $\mathrm{PSL}(2,\mathbb{Z})$ preserves the natural hyperbolic metric on the upper-half-plane, it follows that the moduli space inherits the hyperbolic metric.

Moreover, the group $\mathrm{PSL}(2,\mathbb{Z})$ is generated by the two elements:

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

that act on τ via:

$$A(\tau) = -\frac{1}{\tau} \text{ and } B(\tau) = \tau + 1$$

yielding the familiar *fundamental domain* consisting of:

$$U = \left\{ z \mid |z| > 1,\ -\frac{1}{2} < \mathrm{Re}(z) \leq \frac{1}{2} \right\} \cup \left\{ z \mid |z| = 1, 0 \leq \mathrm{Re}(z) \leq \frac{1}{2} \right\}$$

Exercise 2.4. (a) Show that the stabilizer subgroups of $\mathrm{PSL}(2,\mathbb{Z})$ are trivial for all points of the fundamental domain **except for**

$$\tau = i \ \text{ and } \ \tau = \omega = \frac{1}{2} + \frac{\sqrt{3}}{2} i$$

and determine the stabilizer subgroups for $\tau = i$ and $\tau = \omega$.

(b) Visualize the moduli space of elliptic curves with $\tau \neq i, \omega$. Show that it is homeomorphic to the Riemann sphere minus three points.