Elementary Projective Geometry and the structure of the Geometric Group on an Elliptic Curve

Jonathan Keogh

Trinity College Dublin

Introduction

We are mainly interested in the *projective plane* $\mathbb{P}^2(k)$ and curves therein. It is instructive to think of the projective plane as the regular affine plane with the added property that that all parallel lines intersect exactly once "at infinity". How we transfer our investigation of the usual curves we know and love into the projective plane is to represent them as images of homogeneous polynomials of the form

$$P = \sum_{n+m+l=d} a_{n,m,l} x^n y^m z^l,$$

where d is the degree.

We may first investigate how we may study intersections of algebraic curves. We axiomatically define *intersection multiplicity* $I_p(C, D)$ at a point $p \in \mathbb{P}^2(k)$ as a quantity that satisfies the following axioms:

1. $I_p(C, D) =$
$$\begin{cases} \infty, & p \text{ is not an intersection point} \\ \in \mathbb{Z}_{>0}, & p \in C \cap D, \text{ not in a common component} \\ 0, & p \notin C \cap D. \end{cases}$$
2. $I_p(C, D) = I_p(D, C)$
3. If C and D are lines and $C \cap D = \{p\}$ then $I_p(C, D) = 1$
4. $I_p(C_1 C_2, D) = I_p(C_1, D) + I_p(C_2, D)$
5. $I_p(C, D) = I_p(C, D + CR)$ if deg $R =$ deg $D -$ deg C (for homogeneity).

where C and D are curves. This quantity can be shown to be unique, and from that follows *Bézout's Theorem*:

Theorem

Suppose C and D are projective curves, with no common component, of degree n and m respectively; then they have exactly nm points of intersection, counting multiplicities; or, more succintly,

$$\sum_{q \in C \cap D} I_q(C, D) = nm. \tag{1}$$

This is a very powerful theorem. Corollaries include:

1. Every nonsingular projective curve is irreducible
2. If a projective curve is irreducible then it has finitely many singular points
3. Every nonsingular cubic is equivalent in the affine plane to the depressed cubic

$$y^2 = x^3 + \alpha x + \beta.$$

A curve that can be represented by an equation of the form in the last corollary is called an *elliptic curve*.

The Geometric Group on an Elliptic Curve

Elliptic curves are rich in structure and are very important. They are the source of a great amount of ongoing research throughout the mathematical community. This is largely because of the following theorem:

Theorem

Given two points P, Q on an elliptic curve E, construct the unique line l going through them. By Bézout's Theorem the line must meet the cubic in a third point, counting multiplicity (ie. this third point may be P or Q). Reflect this third point about the x-axis and define this point to be the formal sum $P + Q$. This definition is well-defined and defines an abelian group on our elliptic curve E we denote by $E(\mathbb{C})$.

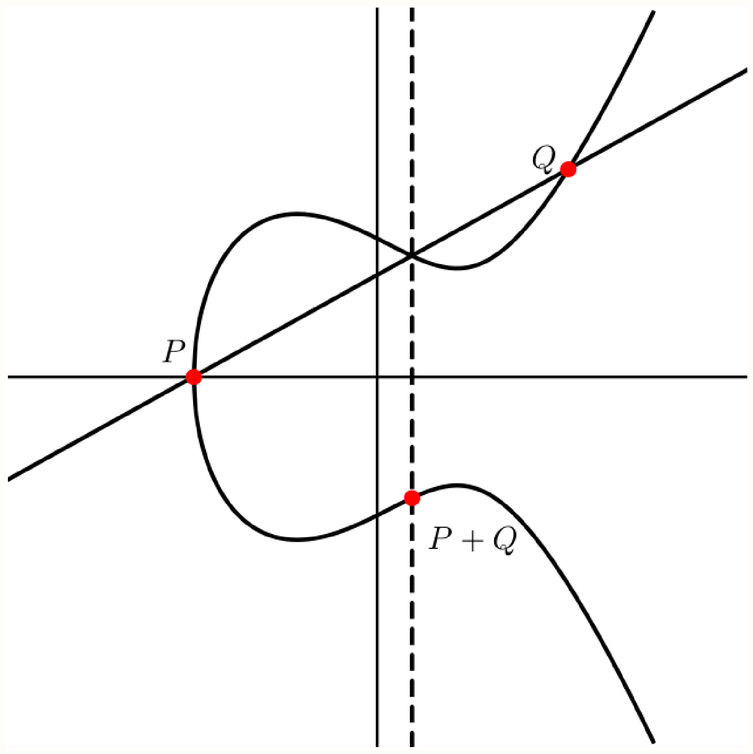

Figure 1: Addition law on $E(\mathbb{C})$

The only point that is gained by embedding into the projective plane is the identity element. Let us denote this by O, then we may write

$$E(\mathbb{C}) = \{(x, y) \in \mathbb{C} \mid y^2 = x^3 - \alpha x - \beta\} \cup \{O\}.$$

Given two points

$$P = (x_p, y_p), \; Q = (x_q, y_q)$$

addition is calculated as

$$P + Q = (x_s, -y_s) = (\lambda - x_p - x_q, \lambda(x_p - x_r) - y_p).$$

where $\lambda = \frac{y_p - y_q}{x_p - x_q}$. So addition is done by rational combinations of the coordinates; which immediately gives us two subgroups

$$E(\mathbb{R}) := \{(x, y) \in E(\mathbb{C}) \; : \; x, y \in \mathbb{R}\} \cup \{O\}$$

$$E(\mathbb{Q}) := \{(x, y) \in E(\mathbb{C}) \; : \; x, y \in \mathbb{Q}\} \cup \{O\},$$

when α and β are real or rational numbers respectively.

Elliptic Functions and Complex Tori

A lattice is a set $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$ where $w_1, w_2 \in \mathbb{C}$ are $\mathbb{R}$-independent. We make it into a group through component-wise addition. Given a lattice Λ over $\mathbb{C}$ we define a torus as the quotient group $\mathbb{C}/\Lambda$. Through the use of the Weierstrass function

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

which is invariant under the action of Λ, we have the differential equation

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3,$$

where g_2 and g_3 are certain constants.

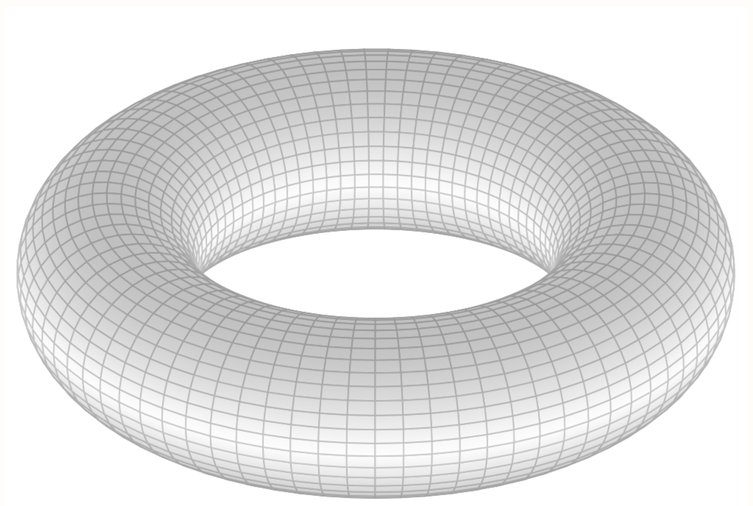

Figure 2: A complex torus $\mathbb{C}/\Lambda$ is topologically a donut

Since $y^2 = 4x^3 - g_2x - g_3$ is in fact a non-singular cubic, this illuminates a tantalizing link between elliptic curves and complex tori. In fact, we have the following theorem:

.

Theorem

Let $E(\mathbb{C})$ be the elliptic curve $y^2 = 4x^3 - g_2x - g_3$; then the map $\phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ given by $z \mapsto (\wp(z), \wp'(z))$ is a group isomorphism.

For every elliptic curve, we can find certain g_2, g_3 so that it may be put in this form; and so every elliptic curve over $\mathbb{C}$ is isomorphic as groups to the complex torus.

Properties of $E(\mathbb{C})$

From our knowledge of complex tori, we may derive many results of a geometric flavour about elliptic curves that would previously be entirely out of reach:

1. For any integer $m \geq 1$ let $E(\mathbb{C})[m]$ be the m-torsion subgroup of $E(\mathbb{C})$; then
$$E(\mathbb{C})[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$
2. The group law on a elliptic curve $E(\mathbb{C})$ is divisible: given $p \in E(\mathbb{C})$ and any integer $n \geq 1$ there exists $q \in E(\mathbb{C})$ such that
$$nq := \underbrace{q + \ldots + q}_{n \text{ times}} = p.$$
In fact, there are n^2 such points.
3. A point $P \in E(\mathbb{C})$ has $3P = O$ if and only if P is an inflection point on the elliptic curve $y^2 = x^3 - \alpha x - \beta$.
4. Every torsion point of
$$E: \; y^2 = x^3 - \alpha x - \beta$$
where $\alpha, \beta \in \mathbb{Q}$ has coordinates that are algebraic over $\mathbb{Q}$.

We can get a better view of this by considering the subgroup $E(\mathbb{R})$ in the case that α and β are real. By above, $E(\mathbb{R})[m] \subset E(\mathbb{C})[m]$ is always finite. The group of 2-torsion points in this case are easily discernible. If $P = (x_p, y_p)$ then $2P = O$ implies that the tangent line to P is parallel to the y-axis; and since $y^2 = x^3 - \alpha x - \beta$ is symmetric about the y-axis, the 2-torsion points are exactly the points at which $y_p = 0$, or $x_p^3 - \alpha x_p - \beta = 0$. There are three such points (not counting the identity element) when $\Delta = (4\alpha^3 - 27\beta^2) < 0$ and only one when $\Delta > 0$.

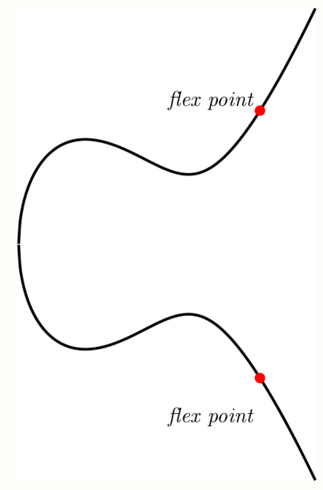

Figure 3: The points of order three

[1] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 2009.

[2] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. Springer International Publishing, Switzerland, 2015.

[3] Frances Kirwan. *Complex Algebraic Curves*. Cambridge University Press, Cambridge, 1992.

[4] Dale Husemöller. *Elliptic Curves*. Springer-Verlag, New York, 1987.

[5] M. F. Atiyah and I. G. MacDonald. *Introduction To Commutative Algebra*. Avalon Publishing, 1994.

[6] Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*. Springer-Verlag, New York, 1990.