The group structure of elliptic curves

We begin by defining elliptic curves and their group law in affine space.

Definition (Elliptic curves in affine space)**.** An elliptic curve $E \subset \mathbb{A}^2_{\mathbb{C}}$ is the set of points (x, y) satisfying

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

for some $a, b \in \mathbb{C}$, and

$$\Delta = -16(4a^3 + 27b^2) \neq 0$$

where Δ is the discriminant.[1]

For the discussion that follows, we will use the elliptic curve given by

$$y^2 = x^3 - x + 1$$

Given such a curve E, and a point $\mathcal{O}$ lying on it, we can define a group structure. For any pair of points P, Q in E, draw the line that joins them and find the third point of intersection of this line with E (which exists since we can substitute $y = ax + b$ into the defining equation for E and then invoke the fundamental theorem of algebra for the resulting univariate cubic). Call this point $P \star Q$.

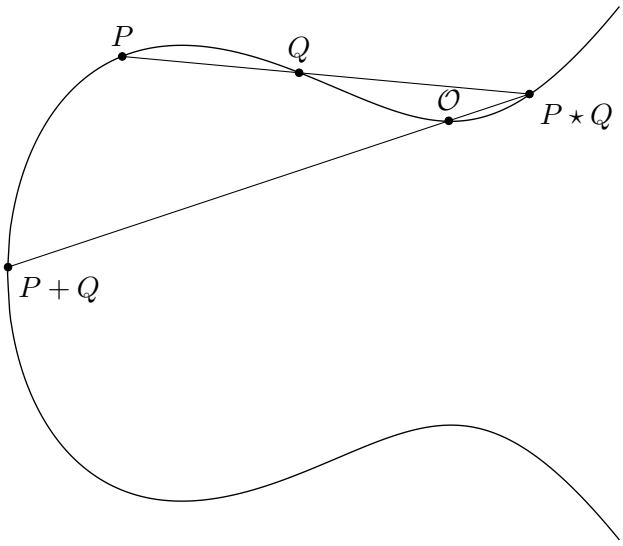

Figure 1: The group structure on elliptic curves in affine space

The operation $\star$ clearly does not give a group structure on E, as there is no identity element, but we can then form the line between $P \star Q$ and $\mathcal{O}$ as seen in Figure 1, and the point of intersection of that line we will call $P + Q$.

[1] There are of course more general ways to define elliptic curves, beginning with a general smooth genus 1 curve, and picking coordinates and applying rational transformations until the defining equation is in the above form.

This operation gives E the structure of an abelian group: $\mathcal{O}$ is the identity element, commutativity inherits from commutativity of $\star$, and associativity can be verified through laborious calculations or by Bézout's Theorem. To find inverses, let $S = \mathcal{O} \star \mathcal{O}$. Then $P \star S = -P$ for any $P \in E$.

One issue with this construction is the slightly ugly fact that a distinguished point $\mathcal{O}$ must be given in order to define the group structure, though all such groups are equivalent: if $G_{\mathcal{O}}$ and $G_{\mathcal{O}'}$ are two group structures on E, then an isomorphism between them is given by $P \mapsto P + (\mathcal{O}' - \mathcal{O})$. Moreover, the intersection multiplicity of a line and our curve is nonconstant; take any vertical line, for example, which has two intersections. To resolve this, and other issues, we may homogenize the curve and view it as a subset of $\mathbb{P}^2_{\mathbb{C}}$.

Definition (Elliptic curves in projective space)**.** An elliptic curve $E \subset \mathbb{P}^2_{\mathbb{C}}$ is the set of points $[x, y, z]$ satisfying

$$zy^2 = x^3 + axz^2 + bz^3$$

for some $a, b \in \mathbb{C}$, and

$$\Delta = -16(4a^3 + 27b^2) \neq 0$$

One advantage of this formulation is that every projective elliptic curve contains the point $[0, 1, 0]$, so we can take this to be $\mathcal{O}$ for all curves, and the group law simplifies to the following:

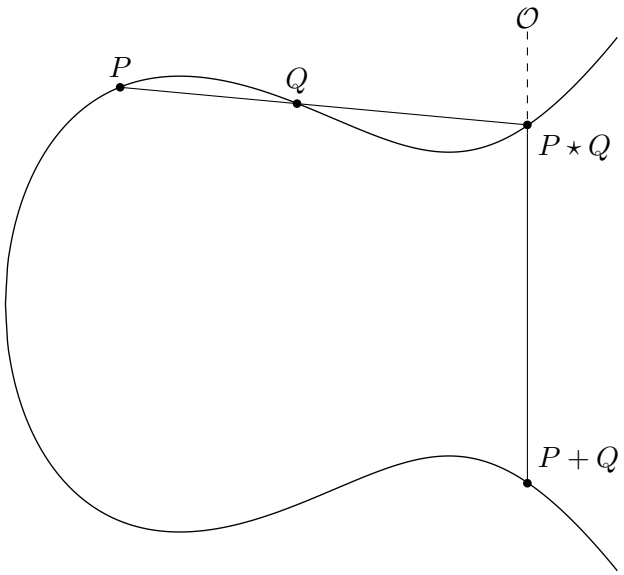

Figure 2: The group structure on elliptic curves in projective space

Since the point $\mathcal{O}$ is "at ∞," to go from $P \star Q$ to $P + Q$ we reflect about the x-axis. Similarly, since $\mathcal{O}$ is a multiplicity 3 point of this curve, $\mathcal{O} \star \mathcal{O} = \mathcal{O}$, so $-P = P \star \mathcal{O}$ for any

point P, that is, the inverse of a point is its reflection about the x-axis, which is also a cleaner situation than in the affine case. Additionally, we can now apply Bézout's Theorem in generality and not worry about missing intersections as in the affine case; moreover, nothing is lost by passing to the projective plane, as we only gain one extra point along the curve, so we can "forget" this point at infinity to recover the affine points.

By abuse of notation, we will henceforth refer to both the curve and its group structure of $\mathbb{C}$-points as E. We will not show, but will give some informal discussion of the fact that $E \cong \mathbb{C}/\Lambda$ where $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ is a lattice in $\mathbb{C}$, and ω_1, ω_2 form an $\mathbb{R}$-basis of $\mathbb{C}$. There is a straightforward way to view $\mathbb{C}/\Lambda$ as a torus; the generators ω_1, ω_2 give us a parallelogram in $\mathbb{C}$ with vertices $0, \omega_1, \omega_2, \omega_1 + \omega_2$ which we can regard as a fundamental domain of $\mathbb{C}/\Lambda$. This region has a natural interpretation as a torus in the sense of gluing edges of a square: a point leaving the right edge enters at the same height on the left edge, and a point leaving the top edge enters at the same x-coordinate from the bottom edge. If one begins with the construction of an elliptic curve as an embedding of a torus into $\mathbb{P}^2$, this is a more natural way to view the group structure.

The Picard group of an elliptic curve

Definition (Picard group)**.** Let X be a scheme, then $\mathrm{Pic}(X)$ is the abelian group of line bundles up to isomorphism on X under $\otimes$.

Definition (Divisors)**.** Let X be a smooth projective curve, then a **Weil divisor** D of X is given by

$$D = \sum_{\substack{\text{closed points} \\ x \in X}} n_x(x)$$

with $n_x \in \mathbb{Z}$ and where all but finitely many of the n_x are 0. The divisors form the group $\mathrm{Div}(X)$ under addition. The subgroup of **principal divisors** $\mathrm{PrDiv}(X)$ is given by divisors D of the form

$$D = \operatorname{div} f = \sum_{\substack{\text{closed points} \\ x \in X}} \operatorname{ord}_x(f)(x)$$

where f is a rational section and $\operatorname{ord}_x(f)$ is the (possibly negative) order of vanishing of f at x.

Note that $\mathrm{PrDiv}(X)$ is in fact a subgroup since $\operatorname{div} f + \operatorname{div} g = \operatorname{div} fg$, and $-\operatorname{div} f = \operatorname{div} \frac{1}{f}$.

Definition (Degree of a divisor)**.** Let D be a divisor on a smooth projective curve X, then

$$\deg D = \sum_{\substack{\text{closed points} \\ x \in X}} n_x$$

It is easy to see that deg induces a homomorphism $\mathrm{Div}(X) \to \mathbb{Z}$.

Theorem 1. *Let X be a smooth projective curve. Then $\mathrm{Pic}(X) \cong \mathrm{Div}(X)/\mathrm{PrDiv}(X)$, with the isomorphism originating from the natural map $\mathcal{O}_X(D) \hookleftarrow D = \sum n_x x$, where $\mathcal{O}(D)$ is the locally free rank 1 quasicoherent sheaf of rational sections f such that*

$$\operatorname{ord}_x(f) + n_x \geq 0$$

for all closed points $x \in X$ (we will sometimes write the above condition compactly as $\operatorname{div} f + D \geq 0$).

Note that there exists a subgroup $\mathrm{Div}^0(X) \subseteq \mathrm{Div}(X)$ of degree 0 divisors, and under this isomorphism, there exists a subgroup $\mathrm{Pic}^0(X) \subseteq \mathrm{Pic}(X)$ of degree 0 line bundles (Pic^0 is well-defined as $\mathrm{PrDiv}(X)$ is a subgroup of $\mathrm{Div}^0(X)$, $\deg \operatorname{div} f = 0$ for all rational sections f; for this claim to hold, the projective hypothesis on X is key). Note that $\mathrm{Pic}^0(\mathbb{P}^1)$ is trivial: if $D = \sum_{P \in \mathbb{P}^1} n_P P$ is a degree 0 divisor of $\mathbb{P}^1$, writing $P = [x_p, y_p]$, the function

$$f(x, y) = \prod_{P \in \mathbb{P}^1} (x_p y - y_p x)^{n_P}$$

is a rational function such that $\operatorname{div} f = D$. However, Pic^0 is not trivial in general; in fact, we will show that $E \cong \mathrm{Pic}^0(E)$ for any elliptic curve E.

Theorem 2 (Riemann-Roch and Serre Duality)**.** *Let X be a smooth projective curve, $L \to X$ a line bundle. Then*

$$h^0(X, L) - h^1(X, L) = 1 - g + \deg L = h^0(X, L) - h^0(X, L^* \otimes \kappa_X)$$

where $\kappa_X = \det T^*X$ is the canonical line bundle and in the second equality above we have invoked Serre duality, that

$$H^1(X, L) \cong H^0(X, L^*, \otimes \kappa_X)^*$$

First note that there is a natural map $E \to \mathrm{Pic}(E)$ given by

$$P \mapsto \mathcal{O}_E(P - \mathcal{O})$$

where $\mathcal{O}$ is the identity of the group structure on E. This is a homomorphism, since $\mathcal{O} \mapsto \mathcal{O}_E(0)$ which is the trivial line bundle, the identity of $\mathrm{Pic}(E)$. Note that we can restrict the codomain to $\mathrm{Pic}^0(E)$ since the degree of the image is 0.

- $\varphi : E \to \mathrm{Pic}^0(E)$ is surjective: for any degree 0 divisor

D, there exists a unique point $P \in E$ such that $D = (P) - (\mathcal{O})$ up to a principal divisor. To see that this holds, note that by Riemann-Roch, $\dim \mathcal{O}_E(D+\mathcal{O}) = \deg(D + \mathcal{O}) = 1$, so let f be a nonzero element (and therefore a basis) of $\mathcal{O}_E(D+\mathcal{O})$. Since $\operatorname{div} f \geq -(D)-(\mathcal{O})$, $\deg \operatorname{div} f = 0$, and $\deg(-D-\mathcal{O}) = -1$, it follows that there exists a point P such that $\operatorname{div} f = -D-(\mathcal{O})+(P)$, so, up to a principal divisor, $D = (P)-(\mathcal{O})$. Surjectivity follows immediately from this result.

- φ is a homomorphism: note that

$$\varphi(P) + \varphi(Q) \neq \varphi(P+Q)$$

if and only if the divisor $(P)+(Q)-(P+Q)-(\mathcal{O})$ is non principal; let $f(x,y,z) = 0$ be the line through P and Q, $f'(x,y,z)$ the line through $P \star Q$ and $\mathcal{O}$. Then

$$\operatorname{div}(f/z) = (P) + (Q) + (P \star Q) - 3(\mathcal{O})$$

and

$$\operatorname{div}(f'/z) = (P \star Q) + (P+Q) - 2(\mathcal{O})$$

Therefore,

$$\operatorname{div}(f/f') = (P) + (Q) - (P+Q) - (\mathcal{O})$$

which is principal as desired, so φ is a homomorphism.

- φ is injective: suppose that $\mathcal{O}_E(P - \mathcal{O}) = \mathcal{O}_E(0)$. This can hold iff there exists a rational section f such that $\operatorname{div} f = (P) - (\mathcal{O})$. Then $f \in \mathcal{O}_E(\mathcal{O})$ where $\mathcal{O}$ is regarded as a divisor, and by Riemann-Roch, $\dim \mathcal{O}_E(\mathcal{O}) = 1$, and $\mathcal{O}_E(\mathcal{O}) \supseteq \mathbb{C}$ so f must in fact be a constant function, and $P = \mathcal{O}$.

Thus, without any drawings or visualizations, one can see that the points of an elliptic curve have a group structure using the Riemann-Roch Theorem alone.

Singular elliptic curves

If we drop the restriction that $\Delta \neq 0$, we introduce the possibility of nodal or cuspidal cubics:

When the discriminant is 0, our curve E will contain singularities (in fact, precisely 1 singularity), e.g points (x, y) such that

$$f(x,y) = \frac{\partial f}{\partial x}(x,y) = \frac{\partial f}{\partial y}(x,y) = 0$$

where $f = 0$ defines E. To see that an elliptic curve has at most one singularity, it suffices to write the defining equation as

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

and note that singularities occur precisely when $y = 0$ and $e_i = e_j$ for some $i \neq j$. For there to be more than one singularity, the univariate cubic on the right hand side above would need to have at least four zeros.

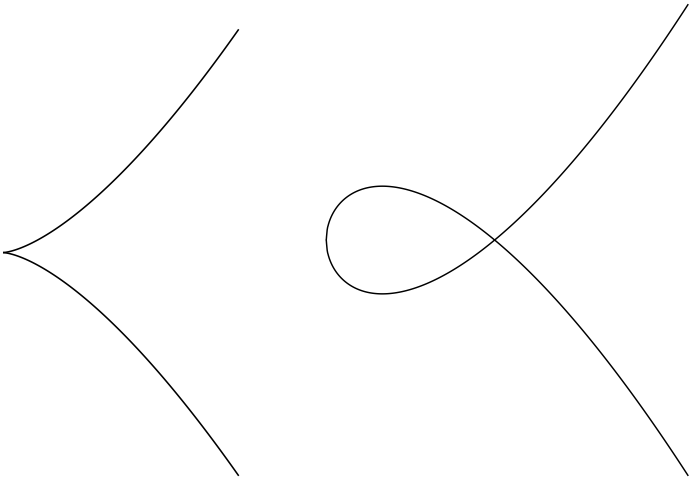

Figure 3: The curves $y^2 = x^3$ (left) and $y^2 = x^3 - 3x + 2$ (right), examples of cuspidal and nodal elliptic curves respectively

Our geometric understanding of the group structure breaks near singularities, as a line through a singularity and any other point of the elliptic curve will have no third intersection, since singularities are multiplicity 2 points of the curve. Moreover, for nodal curves, there are two tangent lines at the node rather than one. However, away from such singularities, the group structure is still well-defined as in the non-singular case (since we cannot reach a singularity S by adding nonsingular points P, Q, as the line from $P \star Q$ through $\mathcal{O}$ and S would intersect E with multiplicity 4 in violation of Bézout's Theorem). It is in fact easier to describe explicitly the group structure on the nonsingular points of a singular elliptic curve E than in the nonsingular case.

First, note that if E is singular, we can assume without loss of generality that the singularity is at $(0, 0)$ by choice of coordinates, and it turns out that the equation for such a curve takes the form

$$y^2 z + axyz - x^3 = 0$$

with a node when $a \neq 0$, and a cusp when $a = 0$.

- Let E be a nodal elliptic curve, with singularity S, E_{ns} the group of nonsingular points. Let $y = a_1 x + b_1$ and $y = a_2 x + b_2$ be the two tangent lines at S, then

the map

$$(x, y) \mapsto \frac{y - a_1 x - b_1}{y - a_2 x - b_2}$$

is an isomorphism from E_{ns} to $\mathbb{C}^*$.

- Let E be a cuspidal elliptic curve, with singularity $S = (x_0, y_0)$, E_{ns} the group of nonsingular points. Let $y = ax + b$ be the tangent line at S, then the map

$$(x, y) \mapsto \frac{x - x_0}{y - ax - b}$$

is an isomorphism from E_{ns} to $\mathbb{C}$

So, for example, by the above simplification, all cuspidal elliptic curves can be written as $y^2 z = x^3$, which has tangent line $y = 0$ at its singularity, so we have the map

$$[x, y, z] \mapsto \frac{x}{y}$$

Since $y = 0$ only at the singularity, we can dehomogenize by setting $y = 1$ and get the map

$$(x, z) \mapsto x$$

with inverse map $t \mapsto (t, t^3)$ which gives an isomorphism $E_{\text{ns}} \cong \mathbb{C}$.

As in our discussion of non-singular elliptic curves, $E_{\text{ns}} \cong \text{Pic}^0(E)$ by the same map, and for the same reasons; the version of Riemann-Roch we used holds on singular curves provided that the support of the given divisor is on the nonsingular points of the given curve. Since Riemann-Roch is the only place where we required smoothness, the result follows.

To see that $\chi(D) = \deg D + 1 - g$ for divisors supported on non-singular points, note that the result holds trivially when $D = 0$ is the trivial divisor, and then induct by adding a point to a given divisor D.

Higher genus curves

In general, a smooth projective curve X of genus $g > 1$ will not itself be a group; to see this, suppose X is a group variety. Then we know that TX is trivial, since we can construct global sections by picking basis elements at the identity element and move them around via the group structure. But

$$\deg TX = -\deg \kappa_X = 2 - 2g < 0$$

for curves with $g > 1$ so nonconstant rational sections cannot be well-defined everywhere, hence X cannot be a group variety.

An intuitive (but possibly false) reason for this failure is due to Bézout's Theorem, that the line through two points of a genus $g = \frac{(d-1)(d-2)}{2}$ irreducible curve will intersect the curve at d points, and for $g > 1$, $d > 3$ so there is no general recipe for picking a unique point from a pair of points as there is with elliptic curves, where pairs P, Q gave rise to the point $P \star Q$.

However, for a curve X of genus g there is an abelian variety $J(X)$ of dimension g with the property that $J(X) \cong \text{Pic}^0(X)$ called the Jacobian of the curve. As above, given a point $\mathcal{O} \in X$, there is an embedding $X \to J(X)$ given by $P \mapsto (P) - (\mathcal{O})$ (by the arguments made above, this is an embedding of varieties, and not of groups).