2 Elliptic curves as abelian groups

In Lecture 1 we defined an elliptic curve as a smooth projective curve of genus 1 with a distinguished rational point. An equivalent definition is that an elliptic curve is an abelian variety of dimension one. An *abelian variety* is a smooth projective variety that is also a group, where the group operation is defined by rational functions (ratios of polynomials). Remarkably, these constraints force the group to be commutative, which is why they are called abelian varieties.

A variety is (roughly speaking) the zero locus of a set of polynomials, subject to an irreducibility condition. The precise definition won't concern us here, it is enough for us to know that a variety of dimension one is a curve, so an abelian variety of dimension one is a smooth projective curve with a group structure specified by rational functions. We will prove in this lecture that elliptic curves are abelian varieties. In fact the converse holds, every abelian variety of dimension one is an elliptic curve, but we won't prove this.

As mentioned in the first lecture, it is possible to associate an abelian variety to any smooth projective curve; this abelian variety is called the *Jacobian* of the curve. The dimension of the Jacobian is equal to the genus g of the curve, which means that in general the Jacobian is a much more complicated object than the curve itself (which always has dimension one). Writing explicit equations for the Jacobian as a projective variety is quite complicated, in general, but for elliptic curves, the curve and its Jacobian both have dimension one, and in fact the Jacobian is isomorphic to the curve itself.

2.1 The group law for Weierstrass curves

Recall from Lecture 1 that the group law for an elliptic curve defined by a Weierstrass equation $y^2 = x^3 + Ax + B$ is determined by the following rule:

Three points on a line sum to zero, which is the point at infinity.

It is then easy to determine the inverse of a point: negating the y-coordinate of a projective point $P = (x : y : z)$ yields the point $Q = (x : -y : z)$. The line between P and Q is vertical, and like all vertical lines it passes through the point O at infinity. We then have $P + Q + O = O$, which means that $P + Q = O$, so $Q = -P$ (this also works when $P = O$).

We can also check that O acts as the identity: the line between O and any point P intersects the curve at $-P$ (this is a double intersection at a tangent when $P = -P$). We then have $0 + P + (-P) = O$, and therefore $O + P = P$.

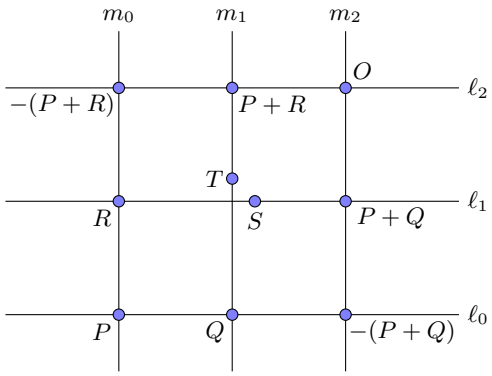
Associativity is not obvious, and while it can be rigorously proven algebraically, this is a tedious task that does not yield much insight. So we will give two proofs. The first will only apply to the generic case but it is short and provides some explanation as to *why* the group operation is associative. The second will be algebraic and fully rigorous, but we will let Sage do all the dirty work for us.

2.1.1 A geometric proof of associativity in the generic case

This is an adaptation of the proof in [2, p. 28]. Let P, Q, R be three points on an elliptic curve E over a field k that we may assume is algebraically closed. We shall also assume that

P, Q, R, and the zero point O are all in *general position* (this means that in the diagram below there are no relationships among the points other than those that necessarily exist by construction).

The line ℓ_0 through P and Q meets the curve E at a third point, $-(P+Q)$, and the line m_2 through O and $-(P+Q)$ meets E at $P+Q$. Similarly, the line m_0 through P and R meets E at $-(P+R)$, and the line ℓ_2 through O and $-(P+R)$ meets E at $P+R$. Let S be the third point where the line ℓ_1 through $Q+P$ and R meets E, and let T be the third point where the line m_1 through Q and $P+R$ meets E. See the diagram below.



We have $S = -((Q+P)+R)$ and $T = -(Q+(P+R))$. It suffices to show $S = T$. Suppose not. Let $g(x,y,z)$ be the cubic polynomial formed by the product of the lines ℓ_0, ℓ_1, ℓ_2 in homogeneous coordinates, and similarly let $h(x,y,z) = m_0 m_1 m_2$. We may assume $g(T) \neq 0$ and $h(S) \neq 0$, since the points are in general position and $S \neq T$. Thus g and h are linearly independent elements of the k-vector space V of homogeneous cubic polynomials in $k[x,y,z]$. The space V has dimension 10, thus the subspace of homogeneous cubic polynomials that vanish at the eight points O, P, Q, R, $\pm(Q+P)$, and $\pm(P+R)$ has dimension 2 and is spanned by g and h. The polynomial $f(x,y,z) = x^3 + Axz^2 + Bz^3 - zy^2$ that defines E is a nonzero element of this subspace, so we may write $f = ag + bh$ as a linear combination of g and h. Now $f(S) = f(T) = 0$, since S and T are both points on E, but $g(S) = h(T) = 0$ and $g(T), h(S) \neq 0$, which implies that both a and b are zero. This is a contradiction because f is not the zero polynomial.

2.1.2 The group law in algebraic terms

Let $P = (x_1, y_1, z_1)$ and $Q = (x_2, y_2, z_2)$ be two points on E. We will compute the sum $P + Q = R = (x_3, y_3, z_3)$ by expressing the coordinates of R as rational functions of the coordinates of P and Q. If either P or Q is the point at infinity, then R is simply the other point, so we assume that P and Q are affine points with $z_1 = z_2 = 1$. There are two cases:

Case 1. $x_1 \neq x_2$. The line $\overline{PQ}$ has slope $m = (y_2 - y_1)/(x_2 - x_1)$, which yields the equation $y - y_1 = m(x - x_1)$. The point $-R = (x_3, -y_3, 1)$ is on this line, thus $-y_3 = m(x_3 - x_1) + y_1$. Substituting for y_3 in the Weierstrass equation for E yields

$$(m(x_3 - x_1) + y_1)^2 = x_3^3 + Ax_3 + B.$$

Simplifying, we obtain $0 = x_3^3 - m^2 x_3^2 + \cdots$, where the ellipsis hides lower order terms. The values x_1 and x_2 satisfy the same cubic equation, thus its roots are x_1, x_2, and x_3,