# The Elliptic Curve Group Law

**Preliminaries:** A *general elliptic curve* is a nonsingular projective curve which is the solution set to a degree 3 cubic polynomial. A *Weierstrass elliptic curve* is the solution set to a degree 3 polynomial of the form

$$Y^2Z - (X^3 + AXZ^2 + BZ^3).$$

Here $A, B$ are constants from the field of definition. The nonsingularity condition comes down to the statement that the polynomial $x^3 + ax + b$ does not have multiple roots. It turns out that this is equivalent to the condition that $4b^3 + 27c^2 \neq 0$.

We will focus on Weierstrass elliptic curves but the preliminary lemmas work in the general case. Let $\boldsymbol{E}$ be a general elliptic curve and let $L$ be a line. If you are keen to see the main definition, you might want to just read the statements of the lemmas here on the first pass.

**Lemma 0.1** *Let $L$ be a line in the projective lane. Then $L \cap \boldsymbol{E}$ consists of at most 3 points.*

**Proof:** Let $P$ be be the homogeneous degree 3 polynomial defining $\boldsymbol{E}$. Without loss of generality, we can move the picture by a projective transformation so that $L$ is the line defined by $Z = 0$, and so that $[1 : 0 : 0] \notin L \cap \boldsymbol{E}$. Plugging this in to $P$, we see that the points of intersection are all of the form $[X : 1 : 0]$. But $P(X, 1, 0) = p(x)$ is just an ordinary cubic polynomial. We have already seen that such a cubic can have at most 3 roots. ♠

**Definition:** Let $\boldsymbol{E}$ be an elliptic curve and let $L$ be a line. We define the *multiplicity* of an intersection point $v \in L \cap E$ as follows: We move the picture by a projective transformation so that $L$ is the line $Z = 0$ and $v = [0 : 1 : 0]$. We then look at the multiplicity of 0 as a root of $p(x) = P(X, 1, 0)$.

**Lemma 0.2** *A point $v \in L \cap E$ has multiplicity greater than 1 if and only if $L$ is tangent to $\boldsymbol{E}$ at $v$. In other words, the $\nabla P(v)$ is the defining function for $L$.*

**Proof:** Let $P$ be the defining function for $L$. We write

$$L = Ax^3 + By^3 + Cz^3 + Dx^2y + Exy^2 + Fx^2z + Gxz^2 + Hy^2z + Iyz^2 + Jxyz.$$

We move by a projective transformation so that $L$ is the line $Z = 0$. Since $P(0,1,0) = 0$ we have $B = 0$. We compute

$$\nabla P(0,1,0) = (E, 3B, H) = (E, 0, H).$$

At the same time, we have

$$p(x) = Ax^3 + Dx^2 + Ex.$$

Suppose that $P$ has a double root at 0. Then $E = 0$. But then $\nabla P(0,1,0) = (0,0,H)$. Since $\boldsymbol{E}$ is nonsingular, this means that $H \neq 0$. Hence $\nabla P$ is the defining function for $L$. That is, $L$ is the tangent line to $\boldsymbol{E}$ at $v$. Conversely, if $L$ is tangent to $\boldsymbol{E}$ at $[0 : 1 : 0]$ then $\nabla P(0,1,0)$ is proportional to $(0,0,1)$. This means that $E = 0$. Hence $p$ has a double root at 0. ♠

**Lemma 0.3** *Let $L$ be a line in the projective plane. If $L \cap \boldsymbol{E}$ consists of exactly 2 points then $L$ is tangent to $E$ at one of the points of intersection.*

**Proof:** Let $\boldsymbol{F}$ be the underlying field. We normalize as in the previous lemma. The points in $L \cap \boldsymbol{E}$ are the points $[X : 1 : 0]$ where $p(X) = 0$. The hypotheses say that $p(X) \in \boldsymbol{F}[X]$ has exactly 2 distinct roots. But then $P(X)$ has two linear factors, and so the third factor must also be linear. This means that $P(X) = (X - r_1)^2(X - r_2)$. But then $\boldsymbol{E}$ and $L$ are tangent at $[r_1 : 1 : 0]$ by the previous result. ♠

**Definition of the Group Law:** We'll first consider the case of Weierstrass elliptic curves. Let $L$ be some line. We make the following rules.

1. The identity element is $0 = [0 : 1 : 0]$.
2. If $A, B, C$ are 3 distinct points of $L \cap \boldsymbol{E}$ then $A + B + C = 0$.
3. If $L \cap \boldsymbol{E}$ consists of exactly 2 points $A$ and $B$, and $L$ is tangent to $\boldsymbol{E}$ at $A$, then $A + A + B = 0$.
4. If $L \cap \boldsymbol{E}$ is just a single point $A$ and $L$ is tangent to $\boldsymbol{E}$ at $A$, then we have $A + A + A = 0$.

Figure 1 illustrates some of these rules and their consequences.

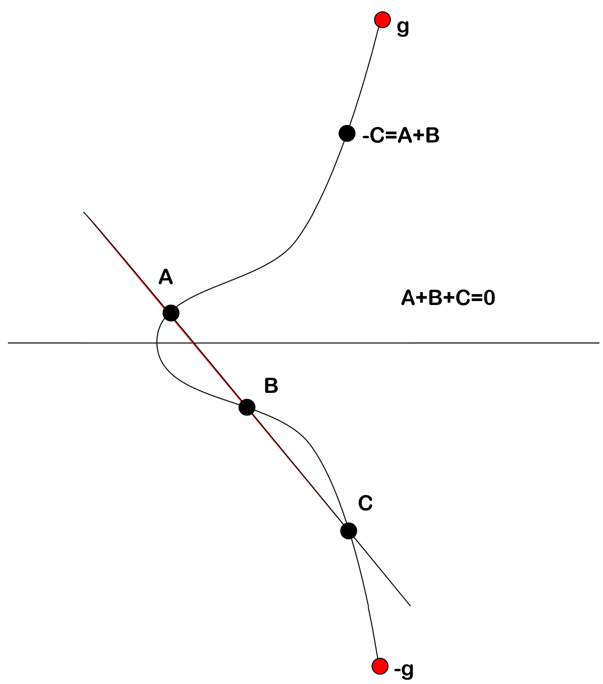


**Figure 1:** The Group Law on a Weierstrass Elliptic Curve

Here are some comments on this law:

- Note that the tangent line to $\boldsymbol{E}$ at $e$ is the line at infinity, and this line intersects $\boldsymbol{E}$ only at $e$. In fact $e$ is a triple root of the polynomial corresponding to this intersection. Thus, the Rule 4 above gives us the fact that $0 + 0 + 0 = 0$.

- By symmetry and Rule 1, the points $C$ and $-C$ are images of each other with respect to reflection in the $x$-axis.

- If we work over $\boldsymbol{R}$ or $\boldsymbol{C}$, then Rule 1 applies to almost every line that intersects $E$ in more than one point, and the remaining rules are just limiting cases. The main idea is that if two points on $\boldsymbol{E}$ are very close together then the line through them approximates the tangent line to $\boldsymbol{E}$ at nearby points.

- The rules imply that $A + B$ is computed as follows: Take the line $AB$ and let $C$ be the third point where this line intersects $\boldsymbol{E}$. Then get $-C = A + B$ by reflecting $C$ in the $x$-axis.

**Verifying the Axioms:** Now let's check that $\boldsymbol{E}$ is a group with respect to the law given above. The most interesting property is associativity. We'll get to that last.

**Definedness:** Suppose that $A$ and $B$ are arbitrary points in $\boldsymbol{E}$. If $A \neq B$ then there is a unique line $L = \overline{AB}$. By the preliminary results, $L \cap \boldsymbol{E}$ either consists of 3 distinct points $A, B, C$, or else $L \cap \boldsymbol{E}$ consists of 2 points and $L$ is tangent to $\boldsymbol{E}$ at (say) $A$. In the first case the rules tell us to define $A + B$ as the reflection of the third point $C$ in the $x$-axis. In the second case, the rules tell us that $A + B$ is the reflection of $A$ in the $x$-axis. This makes sense even if the point in question is 0; the reflection of 0 in the $x$-axis is defined to be 0. In short, the group law is defined for every pair of distinct points $A, B$.

In case $A = B$, the fact that our elliptic curve is nonsingular tells us that there is a well-defined tangent line $L$ at $A$. Either $L \cap \boldsymbol{E}$ consists of two distinct points $A, C$ or else $L \cap \boldsymbol{E}$ consists of the single point $A$. We now proceed just as in the case of distinct points. So, the group law is defined even when $A = B$.

**Abelian Property:** The rules tell us that $A + B = B + A$ for any two points $A, B \in \boldsymbol{E}$. So, if $\boldsymbol{E}$ is a group, it is an Abelian group.

**Existence of Identity:** As the notation suggests, 0 is supposed to be the identity element. We'll work in the ordinary plane, as shown in Figure 1. Given any other point $A \in \boldsymbol{E}$, the line $L = \overline{0A}$ is a vertical line, because $0 = [0:1:0]$. But then, by symmetry the third point of $L \cap \boldsymbol{E}$ is $C$, when we reflect $C$ in the $x$-axis we get back to the point $A$. Hence $0 + A = A$. Since the law is abelian we also have $A + 0 = A$.

**Existence of Inverses:** 0 is its own inverse. Any other point $C$ is such that the reflection of $C$ in the $x$-axis is the inverse. So, for any $A \in \boldsymbol{E}$ there is some $(-A) \in \boldsymbol{C}$ such that $A + (-A) = 0$.

**The Associative Law: Continuous Case:** First I will give a proof when the defining field is $\boldsymbol{C}$. We are trying to establish the relation that $(A + B) + C = A + (B + C)$ for all $A, B, C$. When we are working over $\boldsymbol{C}$ it suffices to prove this relation for a dense set of points. For a dense set of choices of $A, B, C$, the 8 points in Figure 2 are all distinct.

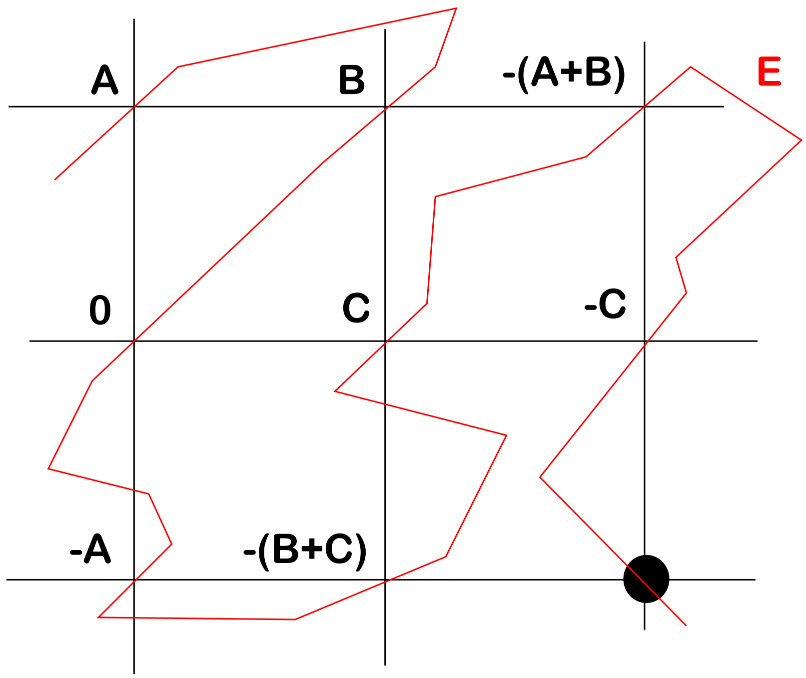


**Figure 2:** Applying the Grid Theorem

The 8 points in Figure 2 are all on $\boldsymbol{E}$, though Figure 2 is just a schematic picture. The points on a single line are meant to be on a single line in the projective plane, though perhaps not the line that is drawn. By the Grid Theorem, $\boldsymbol{E}$ contains the bottom right marked point. If we go along the bottom horizontal line, the rules tell us that this point is $A+(B+C)$. If we go along the right vertical line, the rules tell us that this point is $(A+B)+C$. Since this is the same point, we have $(A+B)+C = A+(B+C)$.

**The Associative Law: Subfield Case:** Let $\boldsymbol{F}$ be a subfield of $\boldsymbol{C}$. This case includes $\boldsymbol{Q}$ and all finite extensions of $\boldsymbol{Q}$ – i.e. the bulk of the fields we considered while doing Galois Theory. Let $\boldsymbol{E}$ be a Weierstrass elliptic curve whose coefficients $(a, b)$ lie in $\boldsymbol{F}$. We really have 2 elliptic curves to consider. Let $\boldsymbol{E}(\boldsymbol{C})$ be the elliptic curve defined over $\boldsymbol{C}$. Let $\boldsymbol{E}(\boldsymbol{F})$ be the elliptic curve defined over $\boldsymbol{F}$. The curve $\boldsymbol{E}(\boldsymbol{F})$ consists of all triples $[x : y : z] \in \boldsymbol{P}^2(\boldsymbol{F})$ satisfying the equation. In particular, $\boldsymbol{E}(\boldsymbol{F}) \subset \boldsymbol{E}(\boldsymbol{C})$ and the two group laws agree whenever both are defined. Since the group law is associative on $\boldsymbol{E}(\boldsymbol{C})$ it is also associative on $\boldsymbol{E}(\boldsymbol{F})$. This proves that the law on any Weierstrass elliptic curve over a subfield of $\boldsymbol{C}$ is associative. In particular, this is true for an elliptic curve over $\boldsymbol{Q}$.

**The Associative Law: General Case** Our proof in the previous cases used continuity properties of $\boldsymbol{C}$ to set up a situation in which we didn't have to prove the result for every given triple $(A, B, C)$, just a dense set. In particular, we could ignore the case when $A = B$. When we are working over a general field, say $\boldsymbol{Z}/5$, the kind of continuity arguments we used don't work. There are two approaches to fixing this problem.

One approach involves observing that there are algebraic formulas for $A + B$ and for $A + A$ in terms of $a$ and $b$ and the coordinates of $A$ and $B$. These functions are ratios of integer polynomials in the relevant variables. (We think of $a$ and $b$ as variables.) The associative law thus reduces to the the statement that certain polynomials $\phi_1$ and $\phi_2$ are identically zero. These polynomials involve 8 variables, namely $a$ and $b$ and the 6 coordinates of $A, B, C$. The formulas are the same in any field of characteristic 0, and in a field of charactaristic $p$ they are obtained by reducing the formulas mod $p$. The fact that $\phi_1$ and $\phi_2$ vanish when we plug in variables in $\boldsymbol{C}$ means that they are simply the 0 polynomials. Hence they vanish over any field.

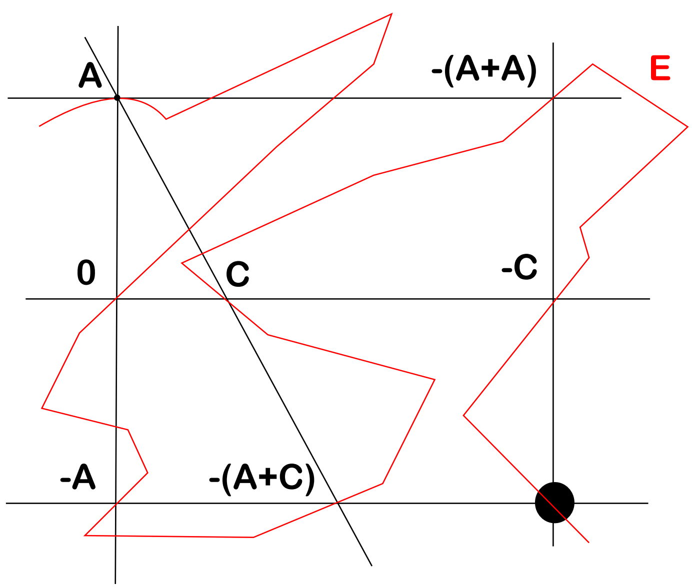


**Figure 3:** Applying the Degenerate Grid Theorem

A second approach is more concrete, and we will illustrate it by way of an example. imagine that we have the case $A = B$, but that the remaining 7 points are distinct. We then have a grid like the one shown in Figure 3.

We only have 7 (labeled) points in this case, but we have an 8th constraing coming from the fact that (by our preliminary Lemmas) the curve $\boldsymbol{C}$ must be tangent to the top horizontal line at $A$. An argument similar to what we did for the Grid Theorem shows that this 8th constraint is independent from the other 7 constraints, and this forces $\boldsymbol{E}$ to contain the marked point. The same argument as in the case over $\boldsymbol{C}$ now says that $A + (A + C) = (A + A) + C$. In other words, by enhancing the Grid Theorem so that it deals with a tangency instead of an intersection point, we can handle a degenerate case. The remaining degenerate cases are handled in a similar way. So, the general case boils down to a routine but pretty tedious case by case analysis.

**General Elliptic Curves:** I want to say a few words about the group law in the general case. In the Weierstrass case, the point $[0 : 1 : 0]$ is called an *inflection point*. The line tangent to $\boldsymbol{E}$ at this point only intersects $\boldsymbol{E}$ at this point. In this case, $[0 : 1 : 0]$ corresponds to a triple root of the associated single variable polynomial (that we get by plugging the equation for the line into the equation for $\boldsymbol{E}$ and dehomogenizing).

Here is how we define the group law at least for elliptic curves with an inflection point. (A general elliptic curve over $\boldsymbol{C}$ has 9 inflection points, so this will always work for elliptic curves over $\boldsymbol{C}$.) We define 0 to be one of the inflection points and then define the rest of the group law as above. The reason we want to define 0 as an inflection point is that we want $0+0+0 = 0$.

At least in the typical case, to find $A + B$ we proceed as follows: We compute the third point $C \in \overline{AB} \cap \boldsymbol{E}$. Then $A + B$ is the third point of $\overline{0C} \cap \boldsymbol{E}$. Again, the complete description of $A+B$ involves various tangencies and degeneracies. Once the law is defined, the same argument as above shows that it is a group.