LECTURE NOTES

An Introduction to Elliptic Curves

The chord-and-tangent group law

Giulio Fellin

Prerequisites. We assume familiarity with fields, polynomial algebra, elementary coordinate geometry, and the equations of tangent lines (including partial derivatives). Projective coordinates and homogenisation are recalled in Section 1. The short Weierstrass form and the addition formulas are studied over fields of characteristic different from 2 and 3; where intersection theorems are used, the field is assumed algebraically closed. The classical nine-point theorem is stated without proof, and the argument for associativity is presented as a geometric outline.

1 From affine curves to projective curves

An elliptic curve looks at first like a plane curve defined by an equation

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

The equation is familiar, but the underlying geometry is richer than that of a usual graph: for a fixed x there may be two values of y, and a line can meet the curve in three points. Moreover, one additional point "at infinity" will play the role of a neutral element for an addition law. To make these observations precise we begin with the projective plane.

Projective points and the affine chart

Definition 1.1 (Projective space)**.** Let K be a field. For nonzero vectors $\mathbf{u}, \mathbf{v} \in K^{n+1}$ define

$$\mathbf{u} \sim \mathbf{v} \quad \Longleftrightarrow \quad \mathbf{u} = \lambda \mathbf{v} \quad \text{for some } \lambda \in K^{\times}.$$

The n-dimensional projective space over K is

$$\mathbb{P}^n_K = (K^{n+1} \setminus \{\mathbf{0}\})/\sim .$$

A point of $\mathbb{P}^n_K$ is written $(X_0 : \cdots : X_n)$, where at least one coordinate is nonzero; multiplying all its coordinates by the same nonzero scalar does not change the point.

The affine plane K^2 is identified with the part of $\mathbb{P}^2_K$ on which $Z \neq 0$, by

$$(x, y) \longmapsto (x : y : 1), \qquad (X : Y : Z) \longmapsto \left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

The remaining points, with $Z = 0$, form the *line at infinity*. In particular, $(0 : 1 : 0)$ is a legitimate point of the projective plane, even though it cannot be represented as $(x : y : 1)$.

Remark 1.1 (Homogenisation)**.** If $f(x, y)$ has degree d, its projective closure is defined by the homogeneous polynomial

$$F(X, Y, Z) = Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

The right-hand side is interpreted as a polynomial after denominators cancel. Conversely, setting $Z = 1$ recovers the affine equation.

A line and a plane curve

Proposition 1.1 (Intersection with a line)**.** Suppose K is algebraically closed. Let $C \subseteq \mathbb{P}^2_K$ be the zero locus of a nonzero homogeneous polynomial F of degree d, and let L be a projective line that is not a component of C. Then C and L meet in exactly d points, *counted with intersection multiplicities*.

Proof. After a linear change of homogeneous coordinates, we may assume that L is given by $X = 0$. Restricting the equation of C to L gives

$$G(Y, Z) = F(0, Y, Z).$$

Since L is not a component, G is a nonzero homogeneous polynomial of degree d in two variables. Over an algebraically closed field a binary form splits into d homogeneous linear factors, with repetitions:

$$G(Y, Z) = c\,(\alpha_1 Y + \beta_1 Z)\cdots(\alpha_d Y + \beta_d Z).$$

Each factor determines one point of $L \simeq \mathbb{P}^1_K$, and repeated factors record the intersection multiplicities. Notice that this also accounts for a possible intersection at $Z = 0$. □

For a cubic, the conclusion is especially suggestive: a line through two points of the curve generally meets it at a third point. When two intersections merge, the line becomes tangent and the repeated intersection is counted twice.

A second intersection theorem is needed for the geometric explanation of associativity. We will use the following classical form, without proof.

Theorem 1.1 (Nine-point theorem for plane cubics)**.** Let C_1, C_2 be plane cubic curves over an algebraically closed field, with no common component, and suppose that they meet in nine distinct points $P_1, \dots, P_9$. If a third cubic passes through $P_1, \dots, P_8$, then it passes through P_9 as well.

This result is a special case of the Cayley–Bacharach theorem. It is not an immediate consequence of the line-intersection proposition. We use it only in the generic configuration where the nine intersection points are distinct; repeated intersections require the corresponding statement with multiplicities. See [3] for an algebraic-geometric treatment.

2 Smooth Weierstrass cubics

Smooth points and tangent lines

Definition 2.1 (Smoothness)**.** Let a projective plane curve C be defined by a homogeneous polynomial $F(X, Y, Z)$. A point $P \in C$ is *smooth* if

$$\Big(F_X(P), F_Y(P), F_Z(P)\Big) \neq (0, 0, 0).$$

At such a point the *tangent line* is

$$F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0.$$

The curve is *smooth* if all its points are smooth.

The tangent formula is homogeneous: changing the chosen coordinates of P merely rescales its equation. On the affine chart $Z = 1$ it agrees with the familiar tangent equation obtained by implicit differentiation.

Definition 2.2 (Short Weierstrass equation)**.** Let K be a field with $\operatorname{char} K \neq 2, 3$. Given $a, b \in K$, consider the projective cubic

$$E: \qquad Y^2Z = X^3 + aXZ^2 + bZ^3. \tag{1}$$

We put

$$\delta = -4a^3 - 27b^2, \qquad \Delta = 16\delta = -16(4a^3 + 27b^2).$$

If $\Delta \neq 0$, the curve is a *smooth elliptic curve in short Weierstrass form*. Its affine part has equation

$$y^2 = x^3 + ax + b. \tag{2}$$

The quantity Δ is the usual discriminant of the Weierstrass model. The equivalent normalisation δ yields the same nonsingularity condition because $16 \neq 0$ in K. More generally, an elliptic curve is a smooth projective curve of genus one equipped with a specified rational point. In characteristic different from 2 and 3 it can be presented in the form above after a suitable choice of coordinates; we work exclusively with this concrete model.

Proposition 2.1 (Discriminant and smoothness)**.** The projective cubic in (1) is smooth if and only if $\Delta \neq 0$.

Proof. Write

$$F(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3.$$

The points at infinity satisfy $Z = 0$, hence $X = 0$. There is therefore exactly one such point,

$$O = (0 : 1 : 0).$$

Since $F_Z(O) = Y^2 = 1$, this point is always smooth.

We may consequently search for singularities in the affine chart $Z = 1$. There the curve is defined by

$$f(x, y) = y^2 - x^3 - ax - b,$$

and the vanishing of its first derivatives requires

$$2y = 0, \qquad 3x^2 + a = 0.$$

Because $\operatorname{char} K \neq 2$, a singular point must have $y = 0$. Thus it corresponds exactly to a common root of

$$g(x) = x^3 + ax + b \quad \text{and} \quad g'(x) = 3x^2 + a.$$

For this cubic the two polynomials have a common root precisely when $4a^3 + 27b^2 = 0$. One can also see the relation directly: at a common root t we have $a = -3t^2$ and $b = 2t^3$, which gives $4a^3 + 27b^2 = 0$. Conversely, if this expression vanishes, then $t = -3b/(2a)$ is a common root when $a \neq 0$; when $a = 0$, necessarily $b = 0$ and one may take $t = 0$. Hence smoothness is equivalent to $\Delta \neq 0$. □

Example 2.1. Consider the real curve

$$E: \quad y^2 = x^3 - x + 1. \tag{3}$$

Here $a = -1$ and $b = 1$, so $\delta = 4 - 27 = -23$ and $\Delta = -368 \neq 0$. The points $P = (0,1)$, $Q = (1,1)$ and $R = (-1,1)$ all belong to E. We will use these points to illustrate addition and doubling.

A distinguished point and reflection

On the Weierstrass cubic there is exactly one point at infinity, O. In addition, reflecting a point in the x-axis preserves the affine equation:

$$P = (x,y) \in E \quad \Longrightarrow \quad -P = (x,-y) \in E.$$

In projective coordinates the reflection is $(X : Y : Z) \mapsto (X : -Y : Z)$; it fixes O as a projective point. We shall see that this reflection is precisely the inverse operation for the group law. When $y = 0$, a point is its own reflection.

3 The chord-and-tangent addition law

The geometric construction

Suppose K is algebraically closed. Given two points P, Q on the smooth cubic E, take the line joining them; if $P = Q$, take the tangent line at P. By Proposition 1.1 the line intersects E in three points, counted with multiplicity. Write R for the remaining intersection, and define

$$P + Q = -R.$$

The word "remaining" includes the possibility that the third intersection coincides with one of the given points. The same construction works over a non-algebraically-closed field for K-rational points: the third intersection is K-rational because the cubic equation along the line already has two roots over K, counted with multiplicity.

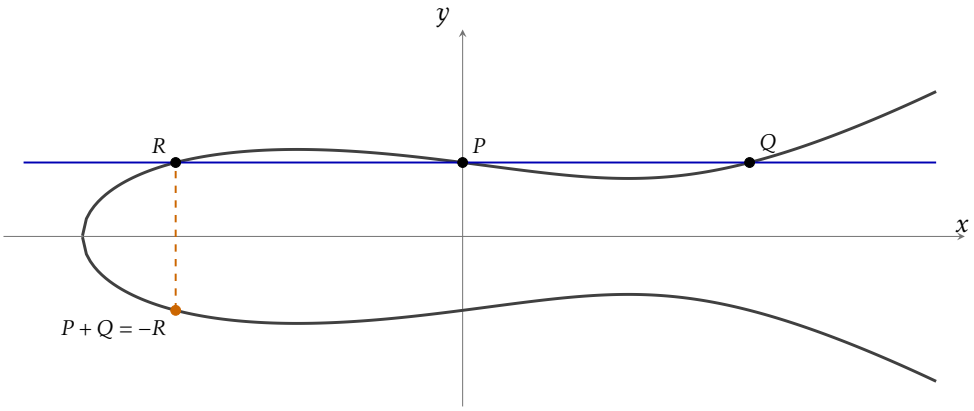


Figure 1: The chord construction on $y^2 = x^3 - x + 1$. The horizontal line meets the cubic at $R = (-1,1)$, $P = (0,1)$, and $Q = (1,1)$. Reflecting R gives $P + Q = (-1,-1)$.

The distinguished point O is declared to be the neutral element. This is also consistent with the line construction: the projective line through P and O is vertical, and its third intersection is $-P$. Hence

$$P + O = P, \qquad P + (-P) = O.$$

The construction is symmetric in P, Q, so $P + Q = Q + P$. Associativity, which is not visible directly from the picture, is the substantial remaining assertion.

Coordinate formulas

For explicit calculations write $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$. Suppose first that $Q \neq -P$. Let

$$y = \lambda x + \mu$$

be the chord or tangent involved in the construction. Then

$$\lambda = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P}, & P \neq Q, \\ \dfrac{3x_P^2 + a}{2y_P}, & P = Q,\ y_P \neq 0, \end{cases} \qquad \mu = y_P - \lambda x_P. \tag{4}$$

Proposition 3.1 (Addition formulas)**.** Let P, Q be affine points with $Q \neq -P$. Then

$$\begin{aligned} x_{P+Q} &= \lambda^2 - x_P - x_Q, \\ y_{P+Q} &= \lambda(x_P - x_{P+Q}) - y_P, \end{aligned} \tag{5}$$

where λ is given by (4). If $Q = -P$, then $P + Q = O$. In particular, if $y_P = 0$, then $2P = O$.

Proof. A point (x, y) on the chord or tangent satisfies $y = \lambda x + \mu$. Substituting into the Weierstrass equation gives

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + (b - \mu^2) = 0.$$

Its three roots, counted with multiplicity, are x_P, x_Q, x_R. Comparing the coefficient of x^2 yields

$$x_P + x_Q + x_R = \lambda^2, \qquad x_R = \lambda^2 - x_P - x_Q.$$

The third intersection has $y_R = \lambda x_R + \mu$. Since $P + Q = -R$ and $\mu = y_P - \lambda x_P$, we obtain

$$y_{P+Q} = -y_R = \lambda(x_P - x_R) - y_P.$$

The slope in the tangent case follows from implicitly differentiating $y^2 = x^3 + ax + b$, namely $2y\,dy/dx = 3x^2 + a$. □

Example 3.1 (Adding two points)**.** On the curve in Example 2.1, take $P = (0, 1)$ and $Q = (1, 1)$. The chord is horizontal, so $\lambda = 0$. Therefore

$$x_{P+Q} = 0^2 - 0 - 1 = -1, \qquad y_{P+Q} = 0(0 + 1) - 1 = -1.$$

Thus $P + Q = (-1, -1)$, as in Figure 1.

Example 3.2 (Doubling a point)**.** For $P = (0, 1)$ on the same curve, the tangent has slope

$$\lambda = \frac{3 \cdot 0^2 - 1}{2 \cdot 1} = -\frac{1}{2}.$$

Consequently

$$x_{2P} = \frac{1}{4}, \qquad y_{2P} = -\frac{1}{2}\left(0 - \frac{1}{4}\right) - 1 = -\frac{7}{8}.$$

Hence $2P = \left(\frac{1}{4}, -\frac{7}{8}\right)$. Notice that this lies on the curve, since $(7/8)^2 = (1/4)^3 - 1/4 + 1$.

4 Why the addition is a group law

The properties established so far are commutativity, the existence of a neutral element O, and an inverse $-P$ for every point P. The issue is whether

$$(P + Q) + R = P + (Q + R)$$

for arbitrary points. This identity is not an obvious consequence of ordinary geometry; showing it is one of the remarkable features of elliptic curves.

Theorem 4.1 (The elliptic-curve group law)**.** The chord-and-tangent operation turns the points of a smooth Weierstrass cubic into an abelian group with identity $O = (0 : 1 : 0)$. For a field K of characteristic different from 2 and 3, the K-rational points $E(K)$ form a subgroup.

Associativity: the nine-point argument

We explain the geometric heart of the associativity proof. This argument is classical; see [1, 3] for approaches to the remaining configurations and multiplicities.

Fix points $P, Q, R \in E$. Assume temporarily that all intersections below are distinct and transverse. Construct:

- T: the third point on the line PQ, so $P + Q = -T$;
- S: the third point on the line QR, so $Q + R = -S$;
- U: the third point on the line $R(-T)$, so $(P + Q) + R = -U$;
- V: the third point on the line $P(-S)$, so $P + (Q + R) = -V$.

Now take two *reducible cubic curves*, each a union of three lines:

$$C_1 = (PQ) \cup (TO) \cup \big(R(-T)\big),$$
$$C_2 = (QR) \cup (SO) \cup \big(P(-S)\big).$$

Their intersections with E consist respectively of

$$E \cap C_1 = \{P, Q, R, O, T, -T, S, -S, U\},$$
$$E \cap C_2 = \{P, Q, R, O, T, -T, S, -S, V\}.$$

Here the sets are written without multiplicities, under our genericity assumption. The cubics C_1 and E share nine distinct points. The cubic C_2 passes through the first eight. Applying Theorem 1.1 therefore forces it to pass through U. Since its ninth intersection with E is V, it follows that $U = V$, and hence

$$(P + Q) + R = -U = -V = P + (Q + R).$$

Remark 4.1 (What the argument proves)**.** The preceding argument proves associativity in the generic situation. It is a *proof outline*, not by itself a complete proof of Theorem 4.1: coincident points, tangent lines, and repeated intersections require care. One can complete the proof using the corresponding Cayley–Bacharach statement with multiplicities, or by verifying the addition law algebraically in the exceptional cases. A complete treatment is given in the references; the geometric construction above is intended to explain why a nine-point theorem naturally appears in the proof.

A few consequences and further directions

The addition law is *algebraic*: on the open sets where the fractions in (4) are defined, the coordinates of $P + Q$ are rational expressions in the coordinates of P and Q. Other coordinate descriptions cover the vertical and tangent cases, producing a globally defined group operation on the smooth projective curve.

There are two complementary ways to view the construction. Geometrically, the projective point O completes the chord-and-tangent rule and makes it possible to speak about sums of points. Algebraically, the formulas allow us to perform exact computations, for example with rational points on curves defined over $\mathbb{Q}$. The resulting group structure is the starting point for the arithmetic of elliptic curves, including rational-point problems, descent, and elliptic-curve cryptography.

Remark 4.2 (Characteristic 2 or 3)**.** The short equation $y^2 = x^3 + ax + b$ and the slope formulas used here rely on 2 and 3 being invertible. Elliptic curves also exist in characteristics 2 and 3, but one works with more general Weierstrass equations and modified formulas. The group law itself remains available on every smooth elliptic curve.

References

[1] F. Friedl, *An elementary proof of the group law for elliptic curves*.

[2] W. Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry*.

[3] A. Pirutka, *Introduction à la géométrie algébrique et courbes elliptiques*, MAT562 course notes (2014–2015).