ELLIPTIC CURVES AND THEIR MODULI SPACES

ANDREAS MIHATSCH

Contents

1. Introduction

1.1. **Elliptic curves.** Let k be a field. Elliptic curves over k can be defined in three equivalent ways:

- As marked smooth cubic curves in $\mathbb{P}^2_k$.
- As marked proper smooth connected k-curves of genus 1.
- As 1-dimensional proper smooth connected group schemes over k.

We will get to know all these definitions during the course and will show their mutual equivalence. In this first lecture, I will stick to the first one because it is the most concrete.

Definition 1.1. An elliptic curve over a field k is a pair (E, O) that consists of a smooth curve $E/\operatorname{Spec} k$ together with a rational point $O \in E(k)$. We moreover require that E can be embedded as a cubic curve into $\mathbb{P}^2_k$. That is, we assume that there exist a homogeneous polynomial $F \in k[X, Y, Z]$ of degree 3 and an isomorphism

$$E \xrightarrow{\sim} V_+(F) \subset \mathbb{P}^2_k. \tag{1.1}$$

Remark 1.2. Condition (1.1) also ensures that E is proper and connected. The smoothness of E then further implies that E is irreducible.

We still need to define what it means for $E/\operatorname{Spec} k$ to be smooth. There are several different definitions which are all powerful, and we will learn about them soon in this course. Today, we go with the so-called Jacobi criterion which is especially useful for studying concrete equations such as (1.1).

Definition 1.3. (1) The partial derivatives $\partial f/\partial T_j$ of a polynomial $f \in k[T_1, \dots, T_n]$ are defined by the rules from analysis. Note that this is a purely algebraic definition which makes sense over any field. The Jacobi matrix of a tuple $f_1, \dots, f_m \in k[T_1, \dots, T_n]$ is the matrix of all partial derivatives

$$\left(\frac{\partial f_i}{\partial T_j}\right)_{i,j} \in M_{m\times n}\left(k[T_1, \dots, T_n]\right). \tag{1.2}$$

(2) Consider $U = V(f_1, \dots, f_m) \subseteq \mathbb{A}^n_k$ and a point $x \in U$. Let $d = \dim_x U$ denote the local dimension of U in x. We say that the Jacobi criterion holds in x if there exist subsets $I \subseteq \{1, \dots, m\}$, $J \subseteq \{1, \dots, n\}$ with $|I| = |J| = n - d$ and such that the (I, J)-minor $(\partial f_i \,/\, \partial T_j)_{i\in I, j\in J}$ is invertible in x. The latter is the case if and only if the polynomial

$$\det\left((\partial f_i \,/\, \partial T_j)_{i\in I, j\in J}\right) \in k[T_1, \dots, T_n]$$

does not vanish in x.

Date: April 9, 2024.

(3) Let X be a k-scheme of locally finite type. Then X is said to be smooth in $x \in X$ if there exist integers $n, m \geq 0$, polynomials $f_1, \ldots, f_m$ as before, an affine open neighborhood $x \in U$, and an isomorphism $U \xrightarrow{\sim} V(f_1, \ldots, f_m) \subseteq \mathbb{A}^n_k$ such that the Jacobi criterion holds in x. We call X smooth if it is smooth in every point.

Remark 1.4. The Jacobi criterion is well-known from the implicit function theorem in analysis. (Recall that this theorem states that the vanishing set $V(f_1, \ldots, f_m) \subseteq \mathbb{R}^n$ of a tuple of smooth functions with $\det(\partial f_i/\partial T_j)(x) \neq 0$ is isomorphic to $\mathbb{R}^{n-m}$ near x.) Definition 1.3 is an algebraic incarnation of the same idea.

Our next aim is to construct elliptic curves. Let $h(x) = x^3 + ax + b$ be a monic cubic polynomial (without x^2-term). A polynomial of the form

$$f = y^2 - h(x) \tag{1.3}$$

is called a *simplified Weierstrass equation*. Let

$$F(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3 \tag{1.4}$$

be the homogenization of f, and let $E = V_+(F) \subset \mathbb{P}^2_k$ be its vanishing locus.

Lemma 1.5. *Assume that* $\mathrm{char}(k) \neq 2$ *and that* h *is separable. Then* E *is a smooth curve.*

Proof. First observe by direct substitution in (1.4) that $E \cap V_+(Z) = \{[0:1:0]\}$. Thus we can proceed by checking the Jacobi criterion on $E \cap D_+(Z)$ and for the point $[0:1:0]$.

By definition, we have

$$E \cap D_+(Z) \xrightarrow{\sim} V(y^2 - h(x)) \subset \mathbb{A}^2_k.$$

The Jacobi matrix of the Weierstrass polynomial is the gradient

$$(\partial f/\partial x,\ \partial f/\partial y) = (-h'(x),\ 2y). \tag{1.5}$$

Let $e = (e_1, e_2) \in E \cap D_+(Z)$ be an arbitrary point. If $e_2 \neq 0$, then also $2e_2 \neq 0$ by our assumption $\mathrm{char}(k) \neq 2$, meaning $2y$ does not vanish in e. If $e_2 = 0$, however, then $h(e_1) = 0$ since $f(e_1, e_2) = 0$. We have assumed that h is separable, which is equivalent to $h(x)$ and $h'(x)$ being coprime. Thus $h'(e_1) \neq 0$. In summary, we have seen that the gradient (1.5) does not vanish in e.

We now consider the point $[0:1:0]$. An affine chart is given by

$$E \cap D_+(Y) \xrightarrow{\sim} V(z - x^3 - axz^2 - bz^3) \subset \mathbb{A}^2_k.$$

In these coordinates, $[0:1:0]$ maps to $(0,0)$. Moreover, the gradient of that equation is

$$(-3x^2 - az^2,\ 1 - 2axz - bz^2). \tag{1.6}$$

Its second entry does not vanish in $(0,0)$, so the Jacobi criterion holds in $(0,0)$. The proof of the lemma is now complete. □

Definition 1.6. Assume that $\mathrm{char}(k) \neq 2$ and that $h(x) = x^3 + ax + b$ is separable. Let F be as in (1.4). The elliptic curve defined by the Weierstrass equation $y^2 - h(x)$ is the pair

$$(E, O) := \big(V_+(F),\ [0:1:0]\big).$$

1.2. **Group structure.** The following will be one of our first major results.

Theorem 1.7. *Let* (E, O) *be an elliptic curve over* k. *Then* E *has a unique group scheme structure such that* O *becomes the identity element. This group structure is abelian.*

We will define group schemes later in the course. Here, we will discuss how to endow the set of rational points $E(k)$ with a group structure.

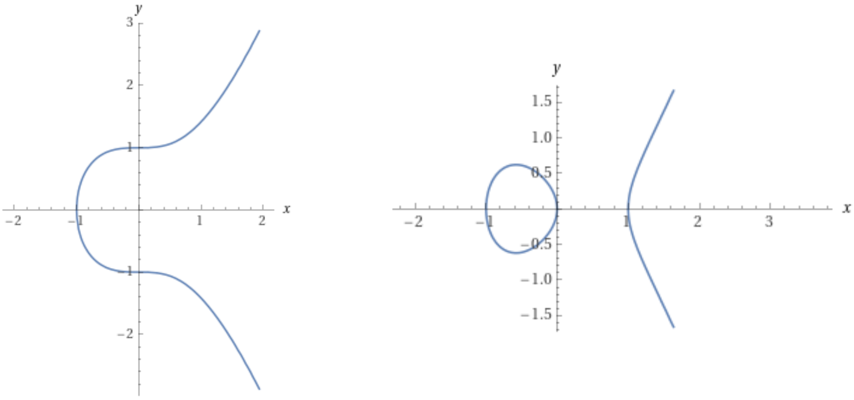

FIGURE 1. The $\mathbb{R}$-points of the two Weierstrass equations $y^2 = x^3 + 1$ and $y^2 = x^3 - x$. Note that $V(y^2 - (x^3 - x)) \subset \mathbb{A}^2_{\mathbb{R}}$ is a connected scheme. Only its $\mathbb{R}$-points endowed with the real topology are disconnected.

Lemma 1.8. *Let $F \in k[X, Y, Z]$ be homogeneous of degree 3 without linear factor and let $E = V_+(F)$. Let $L \subset \mathbb{P}^2_k$ be any line. Then E intersects L in three points when counted with multiplicities. More precisely, $E \cap L = \operatorname{Spec} A$ for a k-algebra A with $\dim_k(A) = 3$.*

Here, by line we mean a curve of the form $V_+(aX + bY + cZ)$, where $(a, b, c) \neq (0, 0, 0)$.

Proof. After a linear change of coordinates, we may assume that $L = V_+(Z)$. Since F has no linear factor, $Z \nmid F$. Thus $F|_L = F(X, Y, 0)$ is a non-zero homogeneous polynomial of degree 3 and hence has three zeroes (counted with multiplicities) as claimed. $\square$

Construction 1.9. Let $E = V_+(F) \subset \mathbb{P}^2_k$ be a smooth cubic curve with a fixed point $O \in E(k)$. Given $P_1, P_2 \in E(k)$, define a line $L \subset \mathbb{P}^2_k$ as follows:

(1) If $P_1 \neq P_2$, then let L be the unique line that passes through P_1 and P_2.
(2) If $P_1 = P_2$, then let L be the tangent line to E in that point.

The definition of the tangent uses the smoothness of E. (In a local chart, take the line perpendicular to the gradient of the equation defining E.) The smoothness of E also implies that F has no linear factor. Hence Lemma 1.8 applies and shows that E and L intersect in three points (counting multiplicities). But two of these points are known to be P_1 and P_2 which lie in $L(k)$! And if a cubic polynomial has two rational roots, then the third root is rational as well. Thus there exists a unique third rational intersection point $P_3 \in (E \cap L)(k)$. Repeating this construction with O, P_3 instead of P_1, P_2, defines a fourth point $P_4 \in E(k)$.

Remark 1.10. A nice illustration of the above construction can be found here.

Definition 1.11. The sum of $P_1, P_2 \in E(k)$ is defined as $P_1 + P_2 := P_4$.

It is true, but not obvious, that this indeed defines a group structure on $E(k)$. The fun and easy part is to show that O is a neutral element and that every element has an inverse (exercise). It is moreover clear that the operation $(P_1, P_2) \mapsto P_1 + P_2$ is commutative, which is why we have written it additively.

A difficulty is to show associativity. Moreover, it is true, but again not obvious, that the construction of P_3 and P_4 only depends on (E, O) and not on the (auxiliary) choices of F and $E \xrightarrow{\sim} V_+(F)$. During the course, we will take a different approach to the group structure on E which will be in terms of line bundles. All the mentioned properties will then follow immediately.

1.3. **Small panoramic outlook.** Elliptic curves play a central role in many branches of algebraic geometry and number theory. In this last section of today's introduction, I want to mention some important aspects and results.

Example 1.12. First consider the case $k = \mathbb{C}$. A general theorem provides an equivalence of categories

$$\left\{\begin{matrix}\text{Connected proper smooth}\\ \text{algebraic curves over } \mathbb{C}\end{matrix}\right\} \xrightarrow{\sim} \left\{\begin{matrix}\text{Connected compact}\\ \text{Riemann surfaces}\end{matrix}\right\}. \tag{1.7}$$

Under this equivalence, elliptic curves are precisely the compact Riemann surfaces of the form $\mathbb{C}/\Lambda$ for a $\mathbb{Z}$-lattice $\Lambda \subset \mathbb{C}$. The group structure here is the additive group structure on $\mathbb{C}/\Lambda$.

Note that while one can always find an isomorphism of real Lie groups

$$\mathbb{C}/\Lambda \xrightarrow{\sim} \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}, \tag{1.8}$$

it is not true that the quotients $\mathbb{C}/\Lambda$ (for varying lattices Λ) are isomorphic as Riemann surfaces. In fact, their isomorphism classes form a 1-dimensional space which is called the modular curve. This space coincides with the $\mathbb{C}$-points of the moduli space we will construct later in the course.

Example 1.13. Now assume that $k = \mathbb{F}_q$ is a finite field, $p = \mathrm{char}(k)$. There are only finitely many elliptic curves over $\mathbb{F}_q$ (up to isomorphism) because there are only finitely many cubic homogeneous polynomials in three variables over $\mathbb{F}_q$.

Note that the n-torsion $(\mathbb{C}/\Lambda)[n]$ of a complex elliptic curve is isomorphic to $(\mathbb{Z}/n)^{\oplus 2}$ which is clear from (1.8). A fascinating result we will show during the course is that for an elliptic curve E over $\mathbb{F}_q$, the n-torsion $E[n]$ is also a group scheme of degree n^2. If $(n,p) = 1$, then it behaves just like $(\mathbb{Z}/n)^{\oplus 2}$. If $p \mid n$, however, then $E[n]$ will be a non-reduced group scheme. We will study its structure in the course and learn about the ordinary/supersingular distinction.

Another feature over $\mathbb{F}_q$ is the existence of the q-Frobenius endomorphism $\mathrm{Frob}_q \in \mathrm{End}(E)$. Its characteristic polynomial determines the number of points $E(\mathbb{F}_{q^r})$ for every r, and enables a classification of elliptic curves over $\mathbb{F}_q$ by the Honda–Tate theorem.

Example 1.14. Finally, assume that k is a number field, i.e. a finite extension of $\mathbb{Q}$. The central structure theorem goes back to Mordell (1922):

Theorem 1.15 (Mordell's Theorem)**.** *For every elliptic curve $(E, O)/k$, the group $E(k)$ is finitely generated.*

By the structure theorem for finitely generated abelian groups, we can thus write

$$E(k) \xrightarrow{\sim} E(k)_{\mathrm{tors}} \oplus \mathbb{Z}^r \tag{1.9}$$

for a unique integer $r \geq 0$ called the algebraic rank of E. This rank is a central object of study in number theory. For example, the Birch and Swinnerton-Dyer conjecture, one of the seven Clay Millennium problems, asserts that it equals the vanishing order of the L-function of E at its center of symmetry.

Fixing the number field k, there is an upper bound on the size $\#E(k)_{\mathrm{tors}}$ of the torsion group. For example, $\#E(\mathbb{Q})_{\mathrm{tors}} \leq 16$ for every elliptic curve $E/\mathbb{Q}$ (Mazur's torsion theorem). It is an open question, however, whether or not the rank r in (1.9) is similarly bounded in terms of k. We refer to the homepage of Dujella for a list of rank records.

References