1 Introduction

Most of the content of the first lecture is contained in the slides that were used in class, which aimed to give a broad overview of the theory and applications of elliptic curves. The purpose of these notes is to summarize the formal definitions we will use in future lectures and to provide additional details on using the Newton polygon to compute the genus of a plane curve. They imply, in particular, that all nonsingular cubics, including the Weierstrass equation $y^2 = x^3 + Ax + B$ with $-16(4A^3 + 27B^2) \neq 0$, are curves of genus 1, as are Edwards curves $x^2 + y^2 = 1 + cx^2y^2$ with $c \neq 0, 1$, which are the main cases of interest to us.

1.1 Formal definition of an elliptic curve

Definition 1.1. Let k be a field. An *elliptic curve* E/k is a smooth projective curve of genus 1 defined over k with a distinguished k-rational point O.

Note that the field k and the k-rational point O are part of the definition. To make this precise we need to define the terms "smooth", "projective curve", "genus 1", and "k-rational point" that appear in the definition. For any field k we use $\bar{k}$ to denote an *algebraic closure* of k, which can be formed by adjoining the roots of all polynomials in $k[x]$ to k.

Definition 1.2. Let k be a field. A *projective point in* $\mathbb{P}^n$ is an equivalence class of tuples $(x_0, \dots, x_n) \in \bar{k}^{n+1}$ with at least one $x_i \neq 0$ given by the equivalence relation

$$(x_0, \dots, x_n) \sim (\lambda x_0, \dots, \lambda x_n)$$

for all $\lambda \in \bar{k}^\times$. A projective point in $\mathbb{P}^n$ is *k-rational* if it contains a representative with $(x_0, \dots, x_n) \in k^{n+1}$, equivalently, it is a tuple $(x_0, \dots, x_n)$ with $x_i/x_j \in k$ for all $x_j \neq 0$. We use the notation $(x_0 : \cdots : x_n)$ to denote the equivalence class of the tuple $(x_0, \dots, x_n)$. The set of k-rational projective points in $\mathbb{P}^n$ is denoted $\mathbb{P}^n(k)$.

For $n = 2$ we typically use the coordinates x, y, z rather than x_0, x_1, x_2 and call $\mathbb{P}^2$ the *projective plane*. It will be convenient to distinguish the subset $(x : y : 1)$ of projective points in $\mathbb{P}^2$ with nonzero z-coordinate as the *affine plane* $\mathbb{A}^2$. The projective points in $\mathbb{P}^2$ that do not lie in the affine plane (those with z-coordinate zero) make up the *line at infinity*, which is isomorphic to the projective line $\mathbb{P}^1$. Of course the choice of the coordinate z is arbitrary, we could have chosen x or y, but z is most commonly used.

Definition 1.3. Let R be a commutative ring. A polynomial $f \in R[x_0, \dots, x_n]$ is *homogeneous* if every nonzero term of f has the same degree. For any nonzero polynomial $f \in R[x_0, \dots, x_n]$ we use $\deg f$ to denote the maximum of the degrees of its nonzero terms. For each $f \in R[x_0, \dots, x_{n-1}]$ there is a unique homogeneous polynomial $f^* \in R[x_0, \dots, x_n]$ with $\deg f^* = \deg f$ that satisfies $f^*(x_0, \dots x_{n-1}, 1) = f$. It can be computed by replacing each term t of f with the term $tx_n^{\deg f - \deg t}$. The polynomial f^* is the *homogenization* of f, and f is a *dehomogenization* of f^*.

Definition 1.4. Let k be a field. A *plane projective curve* $X\colon f(x, y, z) = 0$ is defined by a nonzero homogeneous polynomial $f \in k[x, y, z]$ that is irreducible as an element of $\bar{k}[x, y, z]$. For any extension K/k the set of *K-rational points* of X is the zero locus of f in $\mathbb{P}^2(K)$:

$$X(K) \coloneqq \{(x : y : z) \in \mathbb{P}^2(K) | f(x, y, z) = 0\}.$$

Because f is homogeneous, we have $f(\lambda x, \lambda y, \lambda z) = \lambda^{\deg f} f(x, y, z)$ for any nonzero λ. It follows that either f vanishes at every element of the equivalence class $(x : y : z)$, or it vanishes at none of them; this ensures that $X(K)$ is well defined.

For any nonzero $\lambda \in k$ the polynomial λf has the same zero locus in $\mathbb{P}^2(K)$ for every extension K/k. The polynomials f and λf thus define the same curve X because they have the same *functor of points* $K \mapsto X(K)$, which sends each field extension K/k to the set $X(K)$. Conversely, the functor of points $K \mapsto X(K)$ determines f up to multiplication by $\lambda \in \bar{k}^\times$ (in fact $X(\bar{k})$ is enough). A slightly more general perspective is to view the curve X as being defined by the ideal (f) that f generates; note that $(f) = (g)$ if and only if $g = \lambda f$ for some nonzero λ.

Our requirement that f is irreducible ensures that f generates a prime ideal in $k[x, y, z]$, equivalently, that the quotient ring $k[z, y, z]/(f)$ is an integral domain (has no zero divisors). The quotient ring $k[x, y, z]/(f)$ is the *coordinate ring* of the curve X, denoted $k[X]$, which will play a role in future lectures. We want it to be an integral domain so that we can consider its field of fractions, which we will use to define the *function field* $k(X)$.

We impose the stronger condition that f is irreducible in $\bar{k}[x, y, z]$ to ensure that f generates a prime ideal in $K[x, y, z]$ for any field extension K/k, so that $K[x, y, z]/(f)$ is always an integral domain (hence also has a field of fractions). Note that irreducibility in $\bar{k}[x, y, z]$ is sufficient even if K is not contained in $\bar{k}$; a polynomial in $\mathbb{Q}[x, y, z]$ that is irreducible in $\overline{\mathbb{Q}}[x, y, z]$ will also be irreducible in $\mathbb{C}[x, y, z]$, for example. But irreducibility in $k[x, y, z]$ is not sufficient: the polynomial $x^2 + y^2$ is irreducible in $\mathbb{Q}[x, y]$ but not in $\overline{\mathbb{Q}}[x, y]$, where it factors as $(x + iy)(x - iy)$, for example. Requiring irreducibility over $\bar{k}$ ensures that our curves are always *geometrically irreducible*.

We will often define plane curves using an affine equation of the form $g(x, y) = h(x, y)$ with $g, h \in k[x, y]$ distinct. Such an equation should be interpreted as defining the curve associated to the homogeneous polynomial $f(x, y, z) \coloneqq g^*(x, y, z) - h^*(x, y, z)$. In this course all curves will be plane projective curves, even when they are defined by an affine equation.

Definition 1.5. A plane projective curve X/k defined by $f \in k[x, y, z]$ is *smooth* at a point $P \in X(\bar{k})$ if at least one of the partial derivatives $\partial f/\partial x$, $\partial f/\partial y$, $\partial f/\partial z$ is nonzero at P (note that the partial derivatives are all homogeneous polynomials); otherwise P is a *singular* point of X. The curve X is *smooth* if it is smooth at every point in $X(\bar{k})$, equivalently, there are no points in the common zero locus of f and its partial derivatives.

Remark 1.6. One can define the notion of a projective curve in $\mathbb{P}^n$, for any $n \geq 2$, as an algebraic variety of dimension one. For $n > 2$ one uses the zero locus of a set of homogeneous polynomials (or more precisely, the ideal I that they generate, which we require to be a prime ideal in $\bar{k}[x_0, \ldots, x_n]$) to define the functor of points, and uses the *Krull dimension* (the maximal length of a chain of prime ideals) of the ring $\bar{k}[x_0, \ldots, x_n]/I$ to compute its dimension, which we require to be one. One then defines the notion of a smooth point using a matrix of partial derivatives with a row for each polynomial. Plane projective curves are the only curves we will consider in this course, in which case we can assume that I is generated by a nonzero homogeneous polynomial $f \in k[x, y, z]$ that is irreducible in $\bar{k}[x, y, z]$.

1.2 The genus of a plane curve

To formally define the genus of a curve over an arbitrary field requires material that is beyond the scope of this course (one needs the Riemann-Roch theorem). In this section we give a simple criterion for determining the genus of a plane projective curve defined by an

affine equation $f(x,y)=0$ for suitable polynomials $f\in k[x,y]$ that involves counting integer lattice points in the interior of its Newton polygon. This method can be used to compute the genus of all the curves we will consider. For those not familiar with the Riemann-Roch theorem, Proposition 1.11 below can be taken as the definition of the genus of a plane projective curve defined by a suitable polynomial $f\in k[x,y]$.

Let k be a field with algebraic closure $\bar{k}$. As above, for a polynomial $f\in k[x,y]$ we use $f^*\in k[x,y,z]$ to denote its homogenization.

Definition 1.7. For a polynomial $f(x,y)=\sum a_{ij}x^iy^j\in k[x,y]$, the *Newton polygon* $\Delta(f)$ of f is the convex hull of the set $\{(i,j):a_{ij}\neq 0\}\subseteq\mathbb{Z}^2$ in $\mathbb{R}^2$. The interior and boundary of $\Delta(f)$ are denoted $\Delta^\circ(f)$ and $\partial\Delta(f)$, respectively, and for each edge $\gamma\subseteq\Delta(f)$ we define the polynomial $f_\gamma(x,y):=\sum_{(i,j)\in\gamma}a_{ij}x^iy^j$.

Theorem 1.8 (Baker's Theorem)**.** *Let $f(x,y)\in k[x,y]$ be irreducible in $\bar{k}[x,y]$, and let $F:=\mathrm{Frac}(k[x,y]/(f))$ denote the corresponding function field, with genus $g(F)$. Then*

$$g(F)\leq \#\{\Delta^\circ(F)\cap\mathbb{Z}^2\}.$$

Proof. See [1, Theorem 2.4] for a short proof based on the Riemann–Roch theorem. □

Definition 1.9. A polynomial $f\in k[x,y]$ is *nondegenerate* with respect to an edge γ of $\partial\Delta(f)$ if the polynomials $f_\gamma, x\frac{\partial f_\gamma}{\partial x}, y\frac{\partial f_\gamma}{\partial y}$ have no common zero in $(\bar{k}^\times)^2$. The polynomial f is *nondegenerate* with respect to $\Delta(f)$ if it is nondegenerate with respect to every edge of $\partial\Delta(f)$ and not divisible by x or y.

Remark 1.10. For any edge γ of $\Delta(f)$, if either of the partial derivatives of $f_\gamma(x,y)$ is a monomial, then f is nondegenerate with respect to γ, since monomials have no zeros in $(\bar{k}^\times)^2$.

Proposition 1.11. *Let $f(x,y)\in k[x,y]$ be an irreducible polynomial in $\bar{k}[x,y]$ that is nondegenerate with respect to $\Delta(f)$, and suppose $f^*(x,y,z)$ has no singularities outside $\{(0:0:1),(0:1:0),(1:0:0)\}$. Then*

$$g(F)=\#\{\Delta^\circ(f)\cap\mathbb{Z}^2\}.$$

Proof. See [2, Theorem 4.2]. □

Example 1.12. Let $f(x,y)=y^2-x^3-Ax-B$, with $A,B\in k$, and $-16(4A^3+27B^2)\neq 0$. Then $f(x,y)$ is irreducible in $\bar{k}[x,y]$, and $\partial\Delta(f)$ has the three edges $\gamma_1=[(0,0),(3,0)]$, $\gamma_2=[(0,0),(0,2)]$, and $\gamma_3=[(0,2),(3,0)]$. We have

$$\begin{aligned}f_{\gamma_1}(x,y)&=-x^3-Ax-B,\\ f_{\gamma_2}(x,y)&=y^2-B,\\ f_{\gamma_3}(x,y)&=y^2-x^3.\end{aligned}$$

The polynomial $f(x,y)$ is not divisible by x or y, and the fact that the discriminant of x^3+Ax+B is nonzero implies that f is nondegenerate with respect to γ_1. By Remark 1.10, f is also nondegenerate with respect to the edges γ_2 and γ_3. Thus $f(x,y)$ is nondegenerate, and $f^*(x,y,z)$ has no singularities at all, so Proposition 1.11 implies that

$$g(f)=\#\{\Delta^\circ(f)\cap\mathbb{Z}^2\}=\#\{(1,1)\}=1.$$

Example 1.13. Let $f(x,y) = x^2 + y^2 - 1 - cx^2y^2$ with $c \neq 0, 1$. Then $f(x,y)$ is irreducible in $\bar{k}[x,y]$, and $\partial\Delta(f)$ has the four edges $\gamma_1 = [(0,0),(2,0)]$, $\gamma_2 = [(0,0),(0,2)]$, $\gamma_3 = [(0,2),(2,2)]$, and $\gamma_4 = [(2,0),(2,2)]$. We have

$$\begin{aligned} f_{\gamma_1}(x,y) &= x^2 - 1, \\ f_{\gamma_2}(x,y) &= y^2 - 1, \\ f_{\gamma_3}(x,y) &= y^2 - cx^2y^2, \\ f_{\gamma_4}(x,y) &= x^2 - cx^2y^2. \end{aligned}$$

The polynomial $f(x,y)$ is not divisible by x or y and Remark 1.10 applies to all four f_{γ_i}, thus f is nondegenerate. The homogenized polynomial $f^*(x,y,z)$ is singular only at $(0:1:0)$ and $(1:0:0)$, so f satisfies the hypothesis of Proposition 1.11 and

$$g(F) = \#\{\Delta^\circ(F) \cap \mathbb{Z}^2\} = \#\{(1,1)\} = 1.$$

References

[1] Peter Beelen, *A generalization of Baker's theorem*, Finite Fields and Their Applications **15** (2009), 558–568.

[2] Peter Beelen and Ruud Pellikaan, *The Newton polygon of plane curves with many rational points*, Designs, Codes and Cryptography **21** (2000), 41–67.

18.783 / 18.7831 Elliptic Curves
Fall 2025