Elliptic curves

Lecture 3

26th April 2024

Lecture 1&2: §1 Introduction

§2 Projective curves

Def 2.1 Let K be a field.

$n \geq 1$

Affine space: $\mathbb{A}^n(K) = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in K\}$

($n=2$: plane)

Projective space: $\mathbb{P}^n(K) = \mathbb{A}^{n+1}(K) \setminus \{(0, \ldots, 0)\} \Big/ \sim$,

where $(x_0, x_1, \ldots, x_n) \sim (y_0, \ldots, y_n)$ if $\exists \lambda \in K^\times$

with $x_i = \lambda y_i \quad \forall i = 0, \ldots, n$.

Notation: $[x_0, x_1, \ldots, x_n]$ for the class of $(x_0, \ldots, x_n)$.

homogeneous coordinates

(For motivation see [ST] Appendix A.)

We will be interested in the projective plane

$$\mathbb{P}^2(K) = \{[X,Y,Z] \mid (X,Y,Z) \neq (0,0,0)\}/\sim$$

$$\begin{array}{ccc} \mathbb{P}^2(K) & & [X,Y,1] \\ \cup & & \uparrow \\ \mathbb{A}^2(K) & & (X,Y) \end{array}$$

In §1 we considered affine curves

$$C: f(X,Y) = 0. \qquad f(X,Y) \in K[X,Y]$$

e.g. $\quad y^2 - x^3 - 1 = 0$

$\rightsquigarrow$ projective curve

homogeneous polynomial

$$\hat{C}: F(X,Y,Z) = 0 \qquad F(X,Y,1) = f(X,Y)$$

e.g. $\quad zy^2 - x^3 - z^3 = 0$

We get more points, e.g. $(0,1,0)$
"point at infinity" is in $\hat{C}(\mathbb{Q})$.

<u>Def 2.2</u> i) A projective plane curve over K
is given by a homogeneous polynomial

$$C : F(X,Y,Z) = 0 \qquad F(X,Y,Z) \in K[X,Y,Z]$$

degree of C

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X,Y,Z)$$

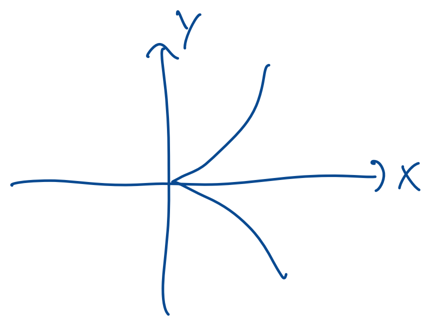
($d=3$: cubic)

ii) We say C is singular at $P \in \mathbb{P}^2(K)$
if
$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

Otherwise C is non-singular at P.

If C is non-singular at every P, we say
C is a smooth (or non-singular) curve.

<u>Example</u>: i) $C: ZY^2 - X^3 = 0$ is singular at $P = [0,0,1]$



$[x, y, 1]$

ii) $C: ZY^2 = X^3 + AXZ^2 + BZ^3$

non-singular $\iff \Delta = -16(4A^3 + 27B^2) \neq 0$

In the following we often assume $K = \mathbb{Q}$.

<u>Def 2.3</u> An <u>elliptic curve</u> over K is a smooth cubic projective curve E over K, with at least one point $O \in E(K)$

<u>origin</u> of E

__Proposition 2.4__ Let E be an elliptic curve over K with $\operatorname{char}(K) \notin \{2,3\}$. Then there exists a curve

Weierstrass equation / form.

$$\hat{E} : ZY^2 = X^3 + AXZ^2 + BZ^3$$

$A, B \in K$

with $4A^3 + 27B^2 \neq 0$ and an invertible change of variables $\psi : E \to \hat{E}$ of the form

$$\psi([X,Y,Z]) = \left[\frac{f_1(X,Y,Z)}{g_1(X,Y,Z)}, \frac{f_2(X,Y,Z)}{g_2(X,Y,Z)}, \frac{f_3(X,Y,Z)}{g_3(X,Y,Z)} \right]$$

such that $\psi(O) = [0,1,0]$. $\left(f_i, g_i \in K[X,Y,Z] \right)$

Proof: Idea see [ST], Chapter 1.3.

__Rem:__ If $\operatorname{Char}(K) \neq 2$ one can bring it on the form

$$ZY^2 = X^3 + AX^2Z + BXZ^2 + CZ^3$$

and in general

$$ZY^2 + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3.$$

Example: Consider the elliptic curve

$$E: \quad X^3 + Y^3 = dZ^3 \qquad \begin{array}{l} d \in \mathbb{Z} \\ d \neq 0. \end{array}$$

with $\mathcal{O} = [1,-1,0]$.

The change of variable

$$\varphi([X,Y,Z]) = [\underbrace{12dZ}_{\hat{X}}, \underbrace{36d(X-Y)}_{\hat{Y}}, \underbrace{X+Y}_{\hat{Z}}]$$

gives

$$\hat{E}: \quad \hat{Z}\hat{Y}^2 = \hat{X}^3 - 432d^2\hat{Z}^3.$$

$$\varphi([1,-1,0]) = [0, 72d, 0] = [0,1,0]$$

φ has inverse

$$\varphi^{-1}([X,Y,Z]) = \left[\frac{36dZ+Y}{72d}, \frac{36dZ-Y}{72d}, \frac{X}{12d}\right]$$

From now on we will usually use affine coordinates, e.g. just write $\hat{E}: \hat{Y}^2 = \hat{X}^3 - 432d^2$ with the understanding that there is still the point $\mathcal{O}$ "at infinity".

In affine coordinates: $\varphi(X,Y) = \left(\frac{12d}{X+Y}, \frac{36d(X-Y)}{X+Y}\right)$

<u>Def 2.5</u> Let $E: f(x,y)=0$ and $E': g(x,y)=0$ be elliptic curves/K with origins O and O'.

We say that E and E' are isomorphic/K if there is an invertible change of variables $\varphi: E \to E'$ defined by rational functions with coefficients in K, such that $\varphi(O) = O'$.

<u>Example</u>: Curves given by quartic polynomials can be isomorphic to curves given by a cubic polynomial, e.g.

$C: v^2 = u^4 + 1$ and $E: y^2 = x^3 - 4x$

are isomorphic/$\mathbb{Q}$ via $\varphi(u,v) = \left(\frac{2(v+1)}{u^2}, \frac{4(v+1)}{u^3}\right)$

§3 The group $E(\mathbb{Q})$

$A, B \in \mathbb{Q}$
$(4A^3+27B^2 \neq 0)$

Let $E/\mathbb{Q}: y^2 = x^3 + Ax + B$ be an elliptic curve with origin O. We want to define a group structure on

$$E(\mathbb{Q}) = \{(x,y) \in \mathbb{Q}^2 \mid y^2 = x^3 + Ax + B\} \cup \{O\}.$$

Def 3.1 The addition $+ : E(\mathbb{Q}) \times E(\mathbb{Q}) \to E(\mathbb{Q})$ is given as follows:

For $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E(\mathbb{Q}) \setminus \{O\}$ set $P_3 = P_1 + P_2 := (x_3, y_3)$ with

(I)

$$x_3 := -x_1 - x_2 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2, \qquad y_3 := \frac{(x_3 - x_2)y_1 - (x_3 - x_1)y_2}{x_2 - x_1} \qquad \text{if } x_1 \neq x_2;$$

(II)

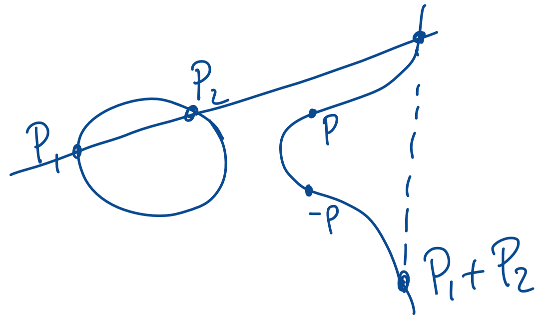
$$x_3 := -2x_1 + \left(\frac{3x_1^2 + A}{2y_1}\right)^2, \qquad y_3 := -y_1 - \frac{3x_1^2 + A}{2y_1}(x_3 - x_1) \qquad \text{if } x_1 = x_2 \text{ and } y_1 = y_2;$$

(III) $P_3 = O$ if $x_1 = x_2$ and $y_1 = -y_2$.

and $P + O = O + P = P$ for any $P \in E(\mathbb{Q})$

(Notice: the case $x_1 = x_2$ and $y_1 \neq \pm y_2$ does not exist)

This definition gives the explicit algebraic expression of the geometric interpretation of Lecture 2



Thm 3.2 $(E(\mathbb{Q}), +)$ is an abelian group

Proof: The addition is commutative by definition, O is the neutral element and $P=(x,y)$ has inverse $-P=(x,-y)$. The associativity can be checked by direct, but complicated, calculation. See S. Zwegers: "On the associativity of the addition on elliptic curves."