

# Courbes elliptiques

Alexandre Guillemot

5 décembre 2022

# Table des matières

<b>1</b>	<b>Sans nom pour le moment</b>	<b>3</b>
1.1	Courbes de Weierstrass . . . . .	3

# Introduction

# Chapitre 1

## Sans nom pour le moment

### 1.1 Courbes de Weierstrass

Dans tout le cours,  $\mathbb{K}$  est un corps commutatif et  $\overline{\mathbb{K}}$  une clôture algébrique de  $\mathbb{K}$ . On notera  $\mathbb{P}^n(\mathbb{K})$  l'espace projectif de dimension  $n$  sur  $\mathbb{K}$ , et  $[x_0 : \dots : x_n]$  un de ses éléments (remarquons que par définition de  $\mathbb{P}^n$ , les  $x_i$  ne peuvent pas être nuls simultanément).

|| **Définition 1.1.1.** Soit  $x = [x_0 : \dots : x_n] \in \mathbb{P}^n(\mathbb{K})$ , alors si  $x_n \neq 0$ , on dit que  $x$  est fini. Les points tels que  $x_n = 0$  définissent un hyperplan dit hyperplan à l'infini.

**Rq 1.1.1.** L'ensemble des points finis est isomorphe à  $\mathbb{A}^n(\mathbb{K})$ . Ainsi  $\mathbb{P}^n(\mathbb{K})$  est réunion (disjointe) de  $\mathbb{A}^n(\mathbb{K})$  et de l'hyperplan à l'infini. On note  $\mathbb{P}^n(\mathbb{K}) \simeq \mathbb{A}^n(\mathbb{K}) \sqcup H_\infty$  où  $H_\infty$  dénote l'hyperplan à l'infini.

**Notation.**  $\mathbb{P}^n$  désignera  $\mathbb{P}^n(\overline{\mathbb{K}})$ . Si on veut parler d'espace projectif sur un corps non algébriquement clos, on précisera  $\mathbb{P}^n(\mathbb{K})$ .

|| **Définition 1.1.2.** Une courbe de Weierstrass est une courbe définie dans le plan projectif  $\mathbb{P}^2$  par une équation homogène de Weierstrass  $F(X, Y, T) = 0$  où  $F \in \overline{\mathbb{K}}[X, Y, T]$  est le polynôme de Weierstrass défini par

$$F(X, Y, T) = (Y^2T + a_1XYT + a_3YT^2) - (X^3 + a_2X^2T + a_4XT^2 + a_6T^3)$$

|| avec  $a_i \in \overline{\mathbb{K}}$ . Si les coefficients sont dans  $\mathbb{K}$ , on dira que la courbe est définie sur  $\mathbb{K}$ .

**Rq 1.1.2.** La partie affine d'un courbe de Weierstrass est donnée par l'équation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

**Proposition 1.1.1.** *L'intersection d'une courbe de Weierstrass avec la droite à l'infini de  $\mathbb{P}^2$  est réduite au point  $[0 : 1 : 0]$ . C'est un point lisse, et la droite tangente à ce point est la droite d'équation  $T = 0$ .*

*Démonstration.* **Exercice** □

**Proposition 1.1.2.** *Un changement de coordonnées projectives transforme un polynôme homogène de Weierstrass en un autre polynôme homogène de Weierstrass (à une unité multiplicative près) si et seulement si il est de la forme*

$$\begin{cases} X = u^2X' + rT' \\ Y = u^3Y' + u^2sX' + tT' \\ T = T' \end{cases}$$

*avec  $u, r, s, t \in \overline{\mathbb{K}}$  et  $u \neq 0$ . Deux équations (ou deux courbes) de Weierstrass sont dites équivalentes si on passe de l'une à l'autre par un tel changement de coordonnées.*

On considère une courbe de Weierstrass  $E$  d'équation affine

$$(E) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Suivant la caractéristique de  $\mathbb{K}$ , on peut transformer cette équation en une équation équivalente plus simple en utilisant un changement de coordonnées comme dans la proposition précédente. On peut transformer  $(E)$  en une équation de la forme  $y^2 = x^3 + ax + b$  en caractéristique différente de 2 et 3.

**Proposition 1.1.3.** *Supposons que  $\text{car}\mathbb{K} \neq 2, 3$ . On a*

1. *Tout équation affine de Weierstrass est équivalente à l'équation de la forme  $y^2 = x^3 + ax + b$ .*
2. *Deux équations affines de Weierstrass de cette forme sont équivalentes si et seulement si on passe de l'une à l'autre par un changement de la forme  $(x, y) = (u^2x', u^3y')$  avec  $u \in \overline{\mathbb{K}}$  non nul.*
3. *Pour une équation  $E$  sous cette forme réduite, on a*

$$\begin{cases} c_4 = -48a \\ c_6 = -864b \end{cases} \quad \text{et} \quad \begin{cases} \Delta(E) = -16(4a^3 + 27b^2) \\ j(E) = \frac{2^8 3^3 a^3}{4a^3 + 27b^2} = -1728 \frac{(4a)^3}{\Delta(E)} \text{ si } \Delta(E) \neq 0 \end{cases}$$

**Rq 1.1.3.**  $\Delta(E) = 0$  si et seulement si  $X^3 + aX + b$  a une racine multiple.

|| **Proposition 1.1.4.** *Une courbe de Weierstrass  $E$  est lisse si et seulement si  $\Delta(E) \neq 0$ . Si  $\Delta(E) = 0$ , alors  $E$  admet un seul point singulier. Plus précisément, si  $c_4(E) \neq 0 \dots$*

|| **Définition 1.1.3.** Une courbe elliptique est un couple  $(E, \mathcal{O})$  où  $E$  est une courbe projective lisse de genre 1 et  $\mathcal{O}$  un point de  $E$ , qui est les point de base ou l'origine. Elle est définie sur  $\mathbb{K}$  si  $E$  est définie sur  $\mathbb{K}$  et si  $\mathcal{O} \in E(\mathbb{K})$ . On dira aussi que c'est une courbe pointée.

|| **Proposition 1.1.5.** *Soit  $(E, \mathcal{O})$  une courbe elliptique définie sur  $\mathbb{K}$ . Alors il existe des fonctions  $x, y \in \mathbb{K}(E)$  telles que l'application*

$$\begin{aligned} \phi := [x : y : 1] : E &\rightarrow \mathbb{P}^2 \\ p &\mapsto [x(p) : y(p) : 1] \end{aligned}$$

|| *soit un isomorphisme de  $E$  sur une courbe de weierstrass  $C \subseteq \mathbb{P}^2$  définie par une équation  $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ , et tel que  $\phi(\mathcal{O}) = [0 : 1 : 0] \in C$ . L'équation de  $C$  est l'équation de weierstrass de  $E$  correspondnat à  $\phi$ , et les coordonnées  $x$  et  $y$  qui interviennent dans cette équation sont des coordonnées de Weierstrass de  $E$ .*