

# Cryptographie sur les courbes elliptiques

—  
**TIPE**

**Paul Chaudagne**

Mardi 30 septembre 2025

# Table des matières

1. Les courbes elliptiques .....	3
1.1. Définition des courbes elliptiques .....	3

# I - Les courbes elliptiques

## 1) Définition des courbes elliptiques

### Lemme 1

La relation  $\mathcal{R}$ , définie sur  $\mathbb{K}^3 \setminus \{(0, 0, 0)\}$  par :

$$\begin{aligned} \forall ((a, b, c), (a', b', c')) \in (\mathbb{K}^3 \setminus \{(0, 0, 0)\})^2, \\ (a, b, c) \mathcal{R} (a', b', c') \iff (\exists \lambda \in \mathbb{K} \setminus \{0\}, (a, b, c) = \lambda(a', b', c')) \end{aligned}$$

est une relation d'équivalence.

**Preuve :**

Par définition d'un corps, on a :

- $\mathcal{R}$  est réflexive car  $1 \in \mathbb{K}$
- $\mathcal{R}$  est symétrique car pour tout  $\lambda$  dans  $\mathbb{K} \setminus \{0\}$ ,  $\lambda^{-1} \in \mathbb{K}$
- $\mathcal{R}$  est transitive car pour tous  $\lambda, \mu \in \mathbb{K}$ ,  $\lambda\mu \in \mathbb{K}$

Donc  $\mathcal{R}$  est une relation d'équivalence.

### Définition 1 (Plan projectif)

Soit  $\mathbb{K}$  un corps, on appelle plan projectif l'ensemble des classes d'équivalence pour la relation  $\mathcal{R}$ , noté :

$$\mathbb{P}^2(\mathbb{K}) = (\mathbb{K}^3 \setminus \{(0, 0, 0)\}) / \mathcal{R}$$

Cela revient à projeter l'espace sur une demi-sphère centrée en  $(0, 0, 0)$ , où chaque classe d'équivalence correspond à une droite passant par l'origine et un unique point de la demi-sphère, soit en dimension 1 :

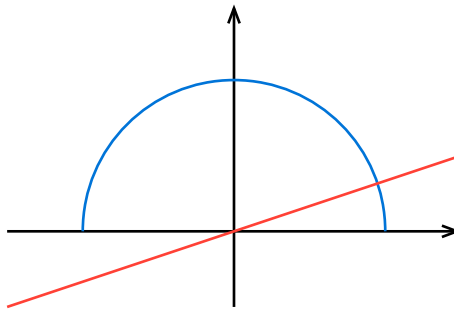


Fig. 1. – Représentation de l'espace projectif en dimension deux.

finir schéma

### Définition 2 (Polynôme homogène)

Un polynôme homogène est un polynôme en plusieurs indéterminées dont tous les monômes non nuls sont de même degré total.

Par exemple, un polynôme de degré 3 homogène en trois variables s'écrit sous la forme :

$$P(X, Y, Z) = aX^3 + bY^3 + cZ^3 + dX^2Y + eX^2Z + fY^2X + gY^2Z + hZ^2X + iZ^2Y + jXYZ$$

**Définition 3 (Courbe elliptique)**

On appelle courbe elliptique sur un corps  $\mathbb{K}$ , l'ensemble des solutions dans le plan projectif  $\mathbb{P}^2(\mathbb{K})$  de l'équation  $F(X, Y, Z) = 0$ , où  $F$  est un polynôme homogène de degré 3 en trois variables.

Formellement, pour  $F$  polynôme homogène de  $\mathbb{K}_3[X, Y, Z]$ , on note :

$$E(\mathbb{K}) = \{[x : y : z] \in \mathbb{P}^2(\mathbb{K}), F(x, y, z) = 0\}$$

En l'absence d'ambiguïté sur le corps, on notera indistinctement  $E(\mathbb{K})$  et  $E$  les courbes elliptiques considérées.

**Définition 4 (Singularité)**

Un point  $P = [x : y : z]$  d'une courbe elliptique est dit singulier lorsque :

$$\left( \frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P) \right) = (0, 0, 0)$$

On dira d'une courbe elliptique qu'elle est lisse (ou non singulière) si elle ne possède aucun point singulier, soit :

$$\forall P \in E(\mathbb{K}), \left( \frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P) \right) \neq (0, 0, 0)$$

**Proposition 1 (Mise sous forme normale de Weierstrass)**