

Cryptographie sur les courbes elliptiques

—
TIPE

Paul Chaudagne

Samedi 25 octobre 2025

Table des matières

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

1 - Les courbes elliptiques

1) Définition des courbes elliptiques

Lemme 1

La relation \sim , définie sur $\mathbb{K}^n \setminus \{(0, \dots, 0)\}$ par :

$$\begin{aligned} &\forall ((a_1, \dots, a_n), (a'_1, \dots, a'_n)) \in (\mathbb{K}^n \setminus \{(0, \dots, 0)\})^2, \\ &(a_1, \dots, a_n) \sim (a'_1, \dots, a'_n) \iff (\exists \lambda \in \mathbb{K} \setminus \{0\}, (a_1, \dots, a_n) = \lambda(a'_1, \dots, a'_n)) \end{aligned}$$

est une relation d'équivalence.

Preuve :

Par définition d'un corps, on a :

- $1 \in \mathbb{K}$ donc \sim est réflexive
- Pour tout $\lambda \in \mathbb{K} \setminus \{0\}$, $\lambda^{-1} \in \mathbb{K}$ donc \sim est symétrique
- Pour tous $\lambda, \mu \in \mathbb{K} \setminus \{0\}$, $\lambda\mu \in \mathbb{K}$ donc \sim est transitive.

Conclusion, \sim est une relation d'équivalence.

Définition 2 - Espace projectif

Soit \mathbb{K} un corps, on appelle **espace projectif de dimension n** l'ensemble des classes d'équivalence pour la relation \sim , noté :

$$\mathbb{P}^n(\mathbb{K}) = (\mathbb{K}^{n+1} \setminus \{(0, \dots, 0)\}) / \sim$$

Pour $P = (x_1, \dots, x_{n+1}) \in \mathbb{K} \setminus \{(0, \dots, 0)\}$, on notera $[x_1 : \dots : x_{n+1}]$ la **classe d'équivalence** de P pour la relation \sim .

On appellera en particulier **plan projectif** l'espace projectif de dimension 2.

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 :

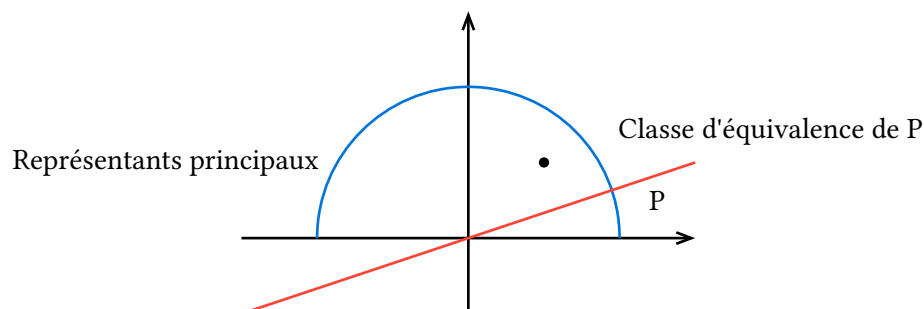


Fig. 1. – Représentation de l'espace projectif de dimension 1.

Définition 3 - 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 :

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

On remarque en particulier que si P est un polynôme homogène en trois variables de degré d , et que $P(x, y, z) = 0$, alors :

$$\forall (x', y', z') \in [x : y : z], P(x', y', z') = \lambda^d P(x, y, z) = 0$$

Dans le plan projectif, l'annulation d'un polynôme homogène ne dépend donc pas du représentant choisi.

Définition 4 - 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 à coefficients dans \mathbb{K} .

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 5 - 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 :

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

Par la suite, nous ne considérerons que des courbes elliptiques non singulières définies sur un corps \mathbb{K} de caractéristique différente de 2 ou 3.

Définition 6 - Tangente

Soit E une courbe elliptique, et $P \in E$ un point non singulier. Alors la **tangente à E en P** est donnée par :

$$\frac{\partial F}{\partial X}(P)(X - X_P) + \frac{\partial F}{\partial Y}(P)(Y - Y_P) + \frac{\partial F}{\partial Z}(P)(Z - Z_P) = 0$$

Définition 7 - Point d'inflexion

Soit E une courbe elliptique, on dit qu'un point $P \in E$ est un **point d'inflexion** si la tangente à E en P intersecte E en P avec une multiplicité égale à 3.

Proposition 8

Soit E une courbe elliptique non singulière sur \mathbb{K} . Soit P un point d'inflexion de E .

Alors un changement de variables linéaire inversible permet de transformer P en $[0 : 1 : 0]$ et la tangente en P en $Z = 0$.

Preuve :

Soit L la tangente à E en $P = [x_P : y_P : z_P]$. Soit $Q = [x_Q : y_Q : z_Q] \in L \setminus E$, les vecteurs (x_P, y_P, z_P) et (x_Q, y_Q, z_Q) sont linéairement indépendants car P et Q correspondent à deux points distincts du plan projectif.

On complète avec un vecteur C en une base de \mathbb{K}^3 . On obtient alors :

$$M = \begin{pmatrix} x_Q & x_P & \\ y_Q & y_P & C \\ z_Q & z_P & \end{pmatrix}$$

M est inversible. M^{-1} envoie P sur le point $[0 : 1 : 0]$ et Q sur le point $[1 : 0 : 0]$. Donc M^{-1} envoie L sur $Z = 0$ car c'est l'unique droite passant par P et Q .

Théorème 9 - Mise sous forme de Weierstrass

Soit E une courbe elliptique non singulière. Soit \mathcal{O} un point d'inflexion de E , si $\mathcal{O} = [0 : 1 : 0]$ et la tangente à E en \mathcal{O} est $Z = 0$, alors E est de la forme :

$$Y^2Z + a_1YXZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^4) \quad (1)$$

Preuve :

La forme générale du polynôme qui définit une courbe elliptique est :

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

Montrons que certains termes s'annulent.