TIPE

—

Cryptographie sur les courbes elliptiques

Paul Chaudagne

Jeudi 25 septembre 2025

Sommaire

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 :
>
> $$\forall((a,b,c),(a',b',c')) \in \left(\mathbb{K}^3 \setminus \{(0,0,0)\}\right)^2,\\ (a,b,c)\mathcal{R}(a',b',c') \Longleftrightarrow (\exists\lambda \in \mathbb{K}\setminus\{0\}, (a,b,c) = \lambda(a',b',c')) \tag{1.1}$$
>
> 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 λ 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 :
>
> $$\mathbb{P}^2(\mathbb{K}) = \left(\mathbb{K}^3 \setminus \{(0,0,0)\}\right)/\mathcal{R} \tag{1.2}$$

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 deux :

Schéma

Définition 2 (Courbe elliptique) :

Proposition 1 :