

# Mémoire

## Groupe des Courbes elliptiques et application à la cryptographie

Bebba Yann-Arby

Mémoire rendu à  
*l'Université Picardie Jules Verne*  
dirigé par Mme R.Abdelatif

dans le cadre de la première année de  
MASTER MATHÉMATIQUES



# Table des matières

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	Cryptographie . . . . .	2
1.2	Les courbes elliptiques . . . . .	4
1.2.1	Cercles et courbes elliptiques . . . . .	4
1.2.2	Diophante et courbes elliptiques . . . . .	5
<b>2</b>	<b>Le plan projectif et courbes sur le plan projectif</b>	<b>6</b>
<b>3</b>	<b>Définitions générales sur les courbes elliptiques</b>	<b>8</b>
3.1	Définition . . . . .	8
3.2	Partie affine et point à l'infini . . . . .	12
3.3	Points rationnels d'une courbe elliptique . . . . .	13
<b>4</b>	<b>Loi de groupe</b>	<b>15</b>
4.1	Point de vue géométrique . . . . .	15
4.2	Droites de $\mathbb{P}^2$ . . . . .	15
4.3	Tangente à $E$ en un point . . . . .	16
4.4	Loi de composition des cordes-tangentes . . . . .	19
4.5	Loi de groupe . . . . .	23
<b>5</b>	<b>Applications</b>	<b>26</b>
5.1	Protocole de signature . . . . .	26
5.1.1	Choix du corps de définition . . . . .	26
5.1.2	Choix de la courbe elliptique . . . . .	27
5.1.3	ECDSA . . . . .	28
5.2	Protocole d'échange de clé . . . . .	28

# Chapitre 1

## Introduction

Dans ce mémoire, je vais m'intéresser au groupe des courbes elliptiques et son application dans le domaine de la cryptographie.

L'application première de notre construction étant la cryptographie, il me semble nécessaire de poser les bases de cette branche des mathématiques. Ceci nous permettra d'avoir une idée claire des différents concepts et enjeux qui la compose.

### 1.1 Cryptographie

La cryptographie trouve ses origines avec l'invention de l'écriture, en effet on en retrouve des traces dès l'époque des Égyptiens vers 2000 a.v. J.C.

Elle a longtemps été considéré comme un art. Un art bien souvent en relation avec l'art de la guerre.

À ce stade, on est en droit de se demander ce que signifie la cryptographie. C'est un mot d'étymologie d'origine grec. On peut le traduire par le fait de cacher ce qui est écrit.

On peut donc en conclure que c'est l'intention de transmettre un message de façon secret. Autrement dit, on souhaiterait transmettre par écrit un message dont seul le destinataire et l'expéditeur connaisse la signification du dit "message secret".

On comprend donc tout l'importance de la cryptographie et son rôle important avec la guerre.

Un premier exemple bien connu de cryptographie est appelé le chiffrement de César. **date et attribution**

Cette méthode consiste à prendre les lettres de l'alphabet et d'effectuer une transposition  $n \in \mathbb{N}$ , on peut ainsi définir sur  $\mathbb{Z}/26\mathbb{Z}$  une bijection entre les lettres de l'alphabet et ce groupe. L'entier  $n$  est alors ce que l'on appelle la clé secrète, qui va permettre à la fois de chiffrer et de déchiffrer un éventuel message.

il a d'autres exemples, comme le chiffrement de Vigenère, inventé par Blaise de Vigenère en 1586 dans le traité des chiffres paru en 1586 (on retrouve cependant une méthode analogue dans un court traité de Giovan Battista Bellano paru en 1553), le chiffrement de Vigenère repose sur le même principe que le chiffrement de César. À ceci près que la transposition  $n$  est remplacé explicitement par une clé secret que l'on peut noter  $k$ , qui est un mot secret ou bien une suite de lettre. Ainsi on effectue la même opération que pour le chiffrement de César à la différence près que notre  $n$  cette fois ci varie dans  $\mathbb{Z}/26\mathbb{Z}$  selon les lettres qui compose notre clé secrète  $k$ .

C'est deux exemples ne sont plus sûr. En effet, bien que le chiffrement de Vigenère essaye de contourner le problème de l'analyse de fréquence d'apparition des lettres, qui permet de rendre inefficace les chiffrement du type chiffrement de César avec un seul alphabet. Il aura tout de même fallu III siècle après son apparition, pour qu'en 1863 le major prussien Friedrich Kasiski publie une méthode pour percé le chiffrement de Vigenère.

Cependant encore récemment, la machine enigma utilisé par les Allemands lors de la seconde guerre mondial utilisé encore le principe liés au chiffrement Vigenère que l'on nomme chiffrement par substitution polyalphabétique.

On retiendra que ces méthodes n'ont pas résisté à l'analyse de leurs fonctionnement.

Ceci m'amène donc à parler d'un principes fondateur sur lequel est basé la cryptographie moderne, qui repose essentiellement sur l'avènement de l'informatique qui à permit à la cryptographie un renouveau historique. En effet, aujourd'hui elle n'est plus considéré comme un art mais une vrai science avec tout le formalise que l'on est en droit d'attendre.

On appelle ce principe, le principe de Kerckhoffs, énoncé par Augustus Kerckhoffs en 1883 dans un article en deux parties, "La cryptographie militaire". Ce principe nous dit que la sécurité ne dépend pas de la méthode de chiffrement mais sur le secret de la clé. Autrement dit, d'après Kerckhoffs, une bonne méthode de chiffrement, ne doit pas se reposer sur le secret de sa méthode mais sur le fait que même si elle est connue tant que l'on ne peut pas à partir de celle-ci en déduire une méthode efficace pour retrouver la clé. Notre système cryptographique est considéré comme sûr.

C'est ainsi, qu'en 1976 W.Diffie et M.Hellman, lors de la National Computer Conference, énonce une nouvelle méthode basé sur le principe de Kerckhoffs, sans pouvoir cependant en fournir un exemple d'application. **à vérifier**

Cette nouvelle méthode est la pierre fondatrice de la cryptographie moderne basé sur le principe de clé publique et clé secret, qui sont deux clés distinctes. On parle alors de cryptographie asymétrique ou cryptographie à clé publique. L'asymétrie, ici est une asymétrie de l'information entre les clé ou l'une est publique, donc connue, et l'autre non publique donc inconnue. De plus, chaque clé à sa propre fonction, c'est à dire que la clé publique sert au chiffrement et la clé secrète au déchiffrement.

On peut se représenter le principe, en considérant deux personnes, traditionnellement nommées Alice, Bob.

Soit  $\mathcal{M}$  un ensemble de chiffrements. On prend souvent pour  $\mathcal{M}$  l'ensemble  $\mathbb{Z}/n\mathbb{Z}$  ou bien un corps fini comme  $\mathbb{F}_q$ . Alice souhaite pouvoir se faire envoyer des messages chiffrés de  $\mathcal{M}$  de façon privée. Elle choisit une bijection  $f_A : \mathcal{M} \rightarrow \mathcal{M}$  qui sera rendu publique, et elle seul en connaît la réciproque  $f_A^{-1}$ . Le principe repose sur la grande difficulté de trouver  $f_A^{-1}$  à partir de  $f_A$ .

Dans la situation où Bob envoie un message  $x \in \mathcal{M}$ . Il lui suffit d'envoyer à Alice en clair l'élément  $y = f_A(x)$ . Pour déchiffrer le message Alice calcul donc  $f_A^{-1}(y)$ , et retrouve le message  $x$  de Bob. On appelle ce genre de fonction des fonctions à sens unique, car leurs réciproques sont difficiles à expliciter.

L'enjeu de la cryptographie à clé publique est donc de trouver ce type de fonction. C'est à dire des opérations faciles à calculer mais dont le cheminement inverse est le plus difficile possible.

La cryptographie d'aujourd'hui est basée sur une hypothèse mathématiques éprouvée et sur deux problèmes issus de la théorie des nombres. On a d'un côté l'hypothèse qu'il existe des fonctions à sens unique, c'est à dire dont la réciproque est inexistante. Et de l'autre, on a le problème de la factorisation d'un entier et celui du logarithme discret.

Le problème de la factorisation est basé sur le fait qu'il est facile de multiplier des entiers pour en trouver d'autres mais il est difficile d'effectuer l'opération inverse à savoir trouver les facteurs premiers d'un entier.

Le problème du logarithme discret est le suivant :

Soit  $(G, \cdot)$  un groupe abélien. Étant donné  $g \in G$  et  $n \in \mathbb{N}^*$ , connaissant  $g$  et  $g^n$ , trouver  $n$ .

Ces deux problèmes sont la base sur lesquelles s'appuient bon nombre de systèmes cryptographiques. On peut citer notamment RSA, protocole Diffie-Hellman ou encore l'algorithme d'El-Gamal.

## 1.2 Les courbes elliptiques

En parallèle de l'histoire de la cryptographie. Se déroulaient deux histoires tout aussi anciennes liées à deux problèmes qui trouvent leurs sources dans l'Antiquité.

### 1.2.1 Cercles et courbes elliptiques

La première histoire est celle du cercle. En effet, depuis l'antiquité grecque, l'homme s'est fortement intéressé à l'étude du cercle. Très vite, il s'est posé la question de connaître la longueur du rayon d'un cercle et plus généralement la longueur d'un arc de cercle.

Cette idée fut réintroduite, mais cette fois-ci dans un contexte encore plus générale avec celui du calcul de la longueur d'un arc d'ellipse. En effet, entre le XVII<sup>ème</sup> et XVIII<sup>ème</sup> siècle les mathématiciens Abel () et Jacobi (), pour ne citer qu'eux, se sont mis à l'étude. Et par la suite Weierstrass introduisit ce qu'on appelle aujourd'hui, les équations normales de Weierstrass. **explique eq W**

En étudiant ce problème dans le corps des nombres complexes, on arrive à dégager une structure de groupes sur les points rationnels de la courbe.

En 1985, indépendamment l'un de l'autre N.Koblitz et , on fournit un exemple d'application possible du groupes des courbes elliptiques dans un corps fini à la cryptographie. C'est ce groupes qui va nous intéresser.

### 1.2.2 Diophante et courbes elliptiques

La seconde histoire est celle des équations diophantiennes qui sont attribué à Diophante.

Le principe est de trouver tous les solutions entières d'une équation polynômiale à une ou plusieurs inconnues dont les solutions sont des entiers.

Par exemple, une des équation diophantienne les plus simples à résoudre est l'équation  $ax + by = c$  avec les coefficients  $a, b, c \in \mathbb{Z}$  et les inconnues  $x, y \in \mathbb{Z}$  également. Sa résolution s'appuie sur l'algorithme d'Euclide, le théorème de Bachet-Bézout et le lemme de Gauss.

Cependant, certaines équation diophantiennes ont nécessité les efforts conjugués de nombreux mathématiciens sur plusieurs siècles pour les résoudre.

Ainsi, comme on peut s'en douter elle joue un rôle prépondérant dans la cryptographie moderne qu'il s'agisse des plus connues comme l'équation présenté si dessus, ou des plus sophistiquées, comme celles étudiées par L.Mordell du type  $y^2 = x^3 + ax + b$  qui va nous intéresser.

Le groupe des courbes elliptiques est le fruit de la rencontre entre ces trois histoires.

## Chapitre 2

# Le plan projectif et courbes sur le plan projectif

La définition que nous allons utiliser pour les courbes elliptiques étant dans le plan projectif.

Introduisons brièvement, ce qu'est un espace projectif, ainsi que les objets dont nous aurons besoin à savoir des points et des droites.

Intuitivement, un espace projectif permet de rendre homogène un espace vectoriel. On entend par là, de raisonner indépendamment des proportionalités pour ne plus considérer que les directions. L'idée nous vient de la formalisation mathématique de la perspective. L'espace projectif nous permet d'identifier des droites à des points. Ce qui rend possible le fait de raisonner en termes de coordonnées et de pouvoir effectuer des calculs formels.

Dans un premier temps, voici la définition du plan projectif.

**Définition 2.1.** Le plan projectif sur  $\overline{K}$ , que l'on note  $\mathbb{P}^2(\overline{K})$  ou  $\mathbb{P}^2$ , est l'ensemble quotient

$$\overline{K}^3 - \{(0, 0, 0)\} / \sim$$

où  $\sim$  est la relation d'équivalence telle que pour tous  $(x, y, z)$  et  $(x', y', z')$  non nuls de  $\overline{K}^3$ ,

$$(x, y, z) \sim (x', y', z') \Leftrightarrow \exists \lambda \in \overline{K}^* \quad (x', y', z') = \lambda(x, y, z).$$

Pour tous  $(x, y, z)$  non nuls dans  $\overline{K}^3$ , on note  $[x, y, z]$  sa classe d'équivalence appelée coordonnées homogènes.

Pour définir la notion de courbe sur le plan projectif, on utilise pour cela des polynômes à trois variables. La définition du plan projectif, nous dit qu'un point peut être représenté par plusieurs triplets différents mais équivalents. Il semble alors naturel de ne considérer que des polynômes  $F(X, Y, Z) \in K[X, Y, Z]$  tels que si  $F(x, y, z) = 0$  alors  $F(\lambda x, \lambda y, \lambda z) = 0$  pour tout  $\lambda$  non nul.

**Définition 2.2.** Un polynôme  $F(X, Y, Z)$  est homogène de degré  $d$  s'il vérifie l'égalité suivante :

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X, Y, Z). \quad (2.1)$$

Ces polynôme sont une somme de monômes de la forme  $\sum_{i+j+k=d} X^i Y^j Z^k$  et vérifie l'égalité (2.1).

On peut maintenant énoncé la définition d'une courbe sur le plan projectif.

**Définition 2.3.** Une courbe  $C$  sur le plan projectif  $\mathbb{P}^2$  est l'ensemble des solutions d'une équation polynomiale

$$C : F(X, Y, Z) = 0,$$

où  $F$  est un polynôme homogène de degré supérieur ou égal à 1. Le degré de la courbe est le degré de ce polynôme.

Un point  $P = (x, y, z) \in C$ , s'il vérifie que  $F(x, y, z) = 0$ . En effet si on choisit une autre représentation de ce point dans le plan projectif  $\mathbb{P}^2$ , par exemple pour  $P' = \lambda P$ , on a

$$F(P') = F(\lambda P) = \lambda^d F(P) = 0.$$

Toute représentation d'un point de la courbe est un zéro du polynôme  $F$ .

**Définition 2.4.** Une courbe  $D \in \mathbb{P}^2$  définie par un polynôme homogène de degré 1 est appelée une droite.

Une courbe  $C \in \mathbb{P}^2$  définie par un polynôme homogène de degré 3 est appelée une cubique.



## Chapitre 3

# Définitions générales sur les courbes elliptiques

### 3.1 Définition

La définition générale d'une courbe est la suivante

**Définition 3.1.** Soit un corps  $K$ . Une courbe elliptique sur  $K$  est une cubique, non singulière, définie comme l'ensemble des solutions du plan projectif  $\mathbb{P}_2(K)$  de l'équation de Weierstrass homogène suivante :

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

avec  $a_1, a_2, a_3, a_4$  et  $a_6$  dans  $K$ .

Le terme non singulière, signifie que la courbe est lisse. Ce qui signifie que si on écrit l'équation précédente sous la forme d'une équation homogène  $F(X, Y, Z) = 0$ , alors les dérivées partielles de  $F$  ne doivent pas s'annuler simultanément en un point de la courbe.

Autrement dit, il n'existe pas de point  $P = [x_0, y_0, z_0] \in \mathbb{P}^2$  tel que, en posant

$$F(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3,$$

on ait

$$F(x, y, z) = \frac{\partial F}{\partial x} = \frac{\partial F}{\partial y} = \frac{\partial F}{\partial z} = 0.$$

En d'autres termes, on peut définir une unique tangente à la courbe au point  $P$ .

On peut par changement linéaire de variable lorsque  $\text{car}(K) \neq 2, 3$  se ramener à la forme simplifiée de l'équation de Weierstrass que l'on utilise dans la définition suivante.

C'est pourquoi, dans la totalité de ce qui suit la lettre  $K$  désignera un corps de caractéristique 0 ou un corps fini de caractéristique distincte de 2 et 3. Autrement dit, on peut voir  $K$  comme étant l'un des corps commutatifs suivant  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  ou  $\mathbb{F}_q$ .

### CHAPITRE 3. DÉFINITIONS GÉNÉRALES SUR LES COURBES ELLIPTIQUES

---

On désignera la clôture algébrique de  $K$ , choisi implicitement, par la notation  $\overline{K}$ .

**Définition 3.2.** Une courbe elliptique définie sur  $K$  est une courbe projective plane d'équation

$$y^2z = x^3 + axz^2 + bz^3. \quad (3.1)$$

où  $a$  et  $b$  sont des éléments de  $K$  vérifiant la condition

$$4a^3 + 27b^2 \neq 0. \quad (3.2)$$

Comme par définition, c'est une courbe sur le plan projectif, on dispose du polynôme homogène de degré 3,  $F(X, Y, Z)$  dans l'anneau de polynôme  $K[X, Y, Z]$ . Étant données  $a, b \in K$ .

Posons

$$F = Y^2Z - (X^3 + aXZ^2 + bZ^3).$$

Comme  $F$  est homogène de degré 3. Par la définition (2.3), on a donc  $E$  la courbe sur le plan projectif  $\mathbb{P}_2$  qui est l'ensemble des solutions de l'équation polynômiale

$$E: \quad F(X, Y, Z) = 0,$$

Si  $(x, y, z)$  est un éléments non nul de  $\overline{K}^3$ , cette condition ne dépend que de sa classe dans  $\mathbb{P}_2(\overline{K})$ .

Soit  $P = [x, y, z]$  un point de  $\mathbb{P}^2(\overline{K})$ . On dit que  $P$  est un zéro de  $F$  dans  $\overline{K}$ , ou plus simplement un zéro de  $F$ , si l'on a  $F(x, y, z) = 0$ . On signifie par, courbe projective plane d'équation (3.1), l'ensemble des zéros de  $F$  dans  $\overline{K}$ .

Quant à la condition (3.2), elle signifie que les racines dans  $\overline{K}$  du polynôme

$$f = X^3 + aX + b$$

sont simples.

Le lemme suivant nous garanti que la courbe est lisse.

**Lemme 3.3.** Le discriminant de  $f$  est  $\Delta = -(4a^3 + 27b^2)$ . En particulier, les racines de  $f$  sont simples, si et seulement si  $\Delta \neq 0$ .

Pour demontrer ce lemme, on utilise la proposition suivante :

**Proposition 3.4.** Soit  $g$  un polynôme unitaire à coefficients dans  $K$  de degré  $n \geq 1$ . Soient  $\alpha_1, \dots, \alpha_n$  ses racines dans  $\overline{K}$  comptées avec multiplicités. Le discriminant  $\Delta$  de  $g$  est défini par l'égalité

$$\Delta = \prod_{i < j} (\alpha_i - \alpha_j)^2.$$

C'est un élément de  $K$ .

### CHAPITRE 3. DÉFINITIONS GÉNÉRALES SUR LES COURBES ELLIPTIQUES

---

**Démonstration.** Montrons tout d'abord que le discriminant de  $f$  est  $\Delta = -(4a^3 + 27b^2)$ .

Soit  $\Delta$  le discriminant de  $f$ . Soient  $\alpha, \beta, \gamma$  les racines de  $f$  dans  $\overline{K}$  et  $f'$  le polynôme dérivé de  $f$ .

À l'aide de la proposition 3.4, on veut montrer que le discriminant est de la forme suivante :

$$\begin{aligned}\Delta &= (-1)(\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 \\ &= -f(\alpha)'f(\beta)'f(\gamma)'. \end{aligned}$$

Vérifions que c'est bien le cas.

D'après le théorème d'Alembert-Gauss comme  $f \in \overline{K}$ , on dispose de la forme scindé de  $f$ .

$$f = (X - \alpha)(X - \beta)(X - \gamma).$$

En dérivant  $f$  sous cette forme on obtient :

$$\begin{aligned}f &= (X - \alpha)((X - \beta)(X - \gamma))' + (X - \beta)(X - \gamma) \\ &= (X - \alpha)((X - \beta) + (X - \gamma)) + (X - \beta)(X - \gamma). \end{aligned}$$

Donc

$$f' = (X - \alpha)(X - \beta) + (X - \alpha)(X - \gamma) + (X - \beta)(X - \gamma).$$

On a alors successivement :

$$f(\alpha)' = (\alpha - \beta)(\alpha - \gamma),$$

$$f(\beta)' = (\beta - \alpha)(\beta - \gamma),$$

et

$$f(\gamma)' = (\gamma - \alpha)(\gamma - \beta).$$

En multipliant ces trois expressions, on obtient :

$$\begin{aligned}f(\alpha)'f(\beta)'f(\gamma)' &= (\alpha - \beta)(\alpha - \gamma)(\beta - \alpha)(\beta - \gamma)(\gamma - \alpha)(\gamma - \beta) \\ &= (X - \alpha)(\alpha - \gamma)(-1)(\alpha - \beta)(\beta - \gamma)(-1)(\alpha - \gamma)(-1)(\beta - \gamma) \\ &= (-1)^3(\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 \\ &= -\Delta. \end{aligned}$$

Et donc

$$\Delta = -f'(\alpha)f'(\beta)f'(\gamma).$$

En partant de la forme  $f : x^3 + ax + b$ , on remarque que  $f' : 3x^2 + a$ . Par suite on obtient,

$$\begin{aligned}\Delta &= -f'(\alpha)f'(\beta)f'(\gamma) \\ &= -(3\alpha^2 + a)(3\beta^2 + a)(3\gamma^2 + a). \end{aligned}$$

### CHAPITRE 3. DÉFINITIONS GÉNÉRALES SUR LES COURBES ELLIPTIQUES

---

Ce qui donne :

$$\begin{aligned}\Delta &= -((9\alpha^2\beta^2 + 3a(\alpha^2 + \beta^2) + a^2)(3\gamma^2 + a)) \\ &= -\left(27(\alpha\beta\gamma)^2 + 9a(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + 3a^2(\alpha^2 + \beta^2 + \gamma^2) + a^3\right).\end{aligned}$$

On peut écrire

$$\begin{aligned}\alpha^2 + \beta^2 + \gamma^2 &= (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \alpha\gamma + \beta\gamma), \\ \alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 &= (\alpha\beta + \alpha\gamma + \beta\gamma)^2 - 2\alpha\beta\gamma(\alpha + \beta + \gamma).\end{aligned}$$

Donc d'après les relations entre coefficients et racine (i.e relation de Viète), pour un polynôme de la forme  $ax^3 + bx^2 + cx + d$ , on a :

$$\begin{aligned}\alpha + \beta + \gamma &= -\frac{b}{a}, \\ \alpha\beta + \alpha\gamma + \beta\gamma &= \frac{c}{a}, \\ \alpha\beta\gamma &= -\frac{d}{a}.\end{aligned}$$

Ici dans  $f$  on a  $a = 1$ ,  $b = 0$ ,  $c = a$  et  $d = b$ .

D'où,

$$\alpha + \beta + \gamma = 0, \alpha\beta + \alpha\gamma + \beta\gamma = a \text{ et } \alpha\beta\gamma = -b.$$

Ce qui donne :

$$\begin{aligned}\alpha^2 + \beta^2 + \gamma^2 &= 0^2 - 2a = -2a \\ \alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 &= a^2 + 2b \times 0.\end{aligned}$$

Donc le discriminant vaut :

$$\begin{aligned}\Delta &= -(27b^2 + 9a^3 - 6a^3 + a^3) \\ &= -(4a^3 + 27b^2).\end{aligned}$$

Montrons maintenant que les racines de  $f$  sont simple, si et seulement si,  $\Delta \neq 0$

Raisonnons par contraposition et montrons que les racine de  $f$  sont multiples, si et seulement si,  $\Delta = 0$ .

Supposons que  $\Delta = 0$ . On a alors :

$$\begin{aligned}-(4a^3 + 27b^2) = 0 &\Leftrightarrow -f(\alpha)'f(\beta)'f(\gamma)' = 0 \\ &\Leftrightarrow (f(\alpha)' = 0) \vee (f(\beta)' = 0) \vee (f(\gamma)' = 0) \\ &\Leftrightarrow \alpha \text{ ou } \beta \text{ ou } \gamma \text{ est une racine multiple.}\end{aligned}$$

D'où le résultat. □

On dit que la courbe elliptique d'équation 3.1 est définie sur  $K$  pour préciser que  $a$  et  $b$  sont dans  $K$ . Ceci pour  $a$  et  $b$  vérifiant la condition (3.2)

**Remarque.**

## 3.2 Partie affine et point à l'infini

parle de  $\mathbb{P}^2(\mathbb{R})$

Posons

$$U = \{[x, y, z] \in \mathbb{P}^2(\overline{K}) \mid z \neq 0\}.$$

On dispose de l'application  $\varphi : U \rightarrow \overline{K}^2$  définie par

$$\varphi([x, y, z]) = \left(\frac{x}{z}, \frac{y}{z}\right).$$

C'est une bijection, dont l'application réciproque est donnée par la formule

$$\varphi^{-1}(x, y) = [x, y, 1].$$

Considérons des éléments  $a$  et  $b$  de  $K$  tels que  $4a^3 + 27b^2 \neq 0$ . Soit  $E$  la courbe elliptique définie sur  $K$  d'équation

$$y^2 z = x^3 + axz^2 + bz^3.$$

L'ensemble des points  $[x, y, z] \in E$  tels que  $z = 0$  est réduit au singleton  $\{O\}$  où

$$O = [0, 1, 0].$$

En effet, dans l'équation (3.1), il vient

$$y^2 \times 0 = x^3 + ax \times 0^2 + b \times 0^3,$$

donc  $x = 0$ , ainsi on peut prendre pour représentant de classe de cet élément la classe de  $O$ .

Par ailleurs,  $E \cap U$  s'identifie via  $\varphi$  à l'ensemble des éléments  $(x, y)$  de  $\overline{K}^2$  vérifiant l'égalité

$$y^2 = x^3 + ax + b. \tag{3.3}$$

On dira que  $E \cap U$  est la partie affine de  $E$  et que  $O$  est le point à la l'infini de  $E$ .

Dans toute la suite, on identifiera  $E \cap U$  et le sous-ensemble de  $\overline{K}^2$  formé des éléments  $(x, y)$  vérifiant (3.3). Avec cette identification, on a

$$E = \{(x, y) \in \overline{K} \times \overline{K} \mid y^2 = x^3 + ax + b\} \cup \{O\}.$$

**les objets qui compose  $\mathbb{P}^2(E)$**

Ainsi,  $E$  est la courbe affine d'équation (3.3) à laquelle on adjoint le point à l'infini  $O$ . C'est pourquoi on définira souvent une courbe elliptique par sa partie affine, sans préciser le point  $O$ .

**Remarque.** On retiendra qu'une courbe affine d'équation de la forme (3.3) est une courbe elliptique si et seulement si, par définition, la condition (3.2) est satisfaite.

### 3.3 Points rationnels d'une courbe elliptique

pas encore bien clair

Soit  $L$  une extension de  $K$  dans  $\overline{K}$ .

**Définition 3.5.** Soit  $P = [x, y, z]$  un point de  $\mathbb{P}^2$ . On dit que  $P$  est rationnel sur  $L$  s'il existe  $\lambda \in \overline{K}^*$  tel que  $\lambda x$ ,  $\lambda y$  et  $\lambda z$  soient dans  $L$ . On note  $\mathbb{P}^2(L)$  l'ensemble des points de  $\mathbb{P}^2$  rationnels sur  $L$ .

D'après la définition, un point non nul  $P$  est dans  $\mathbb{P}_2(L)$ , si sa classe est dans  $L$ . Autrement dit,

$$\mathbb{P}_2(L) = \left\{ P \in \overline{K}^3 \mid \exists \lambda \in \overline{K}^*, P = \lambda P \right\}.$$

Cela justifie la notation  $\mathbb{P}^2 = \mathbb{P}^2(\overline{K})$ .

**Remarque.** Étant donné un point  $[x_1, x_2, x_3] \in \mathbb{P}^2$ , le fait qu'il soit rationnel sur  $L$  n'implique pas que les  $x_i$  soient dans  $L$ . Cela signifie qu'il existe  $i$  tel que  $x_i$  soit non nul, et que chaque  $\frac{x_i}{x_i}$  appartienne à  $L$ .

En effet, soit un point  $P \in \mathbb{P}_2$  non nul. Si  $P \in \mathbb{P}_2(L)$ , comme il est non nul, il existe  $x \neq 0$ , et pour  $\lambda = x$ , on a  $P = [1, \frac{y}{x}, \frac{z}{x}]$  et on a bien  $\frac{y}{x}, \frac{z}{x} \in L$  et pourtant ce sont des variables indéterminées de  $\overline{K}$ .

Soit  $E$  une courbe elliptique définie sur  $K$  d'équation (3.1).

**Définition 3.6.** Un point de  $E$  est dit rationnel sur  $L$  s'il appartient à  $E \cap \mathbb{P}^2(L)$ . On note  $E(L)$  l'ensemble des points de  $E$  rationnels sur  $L$ .

Par définition, on a donc

$$E = E(\overline{K}).$$

Le point  $O = [0, 1, 0]$  appartient à  $E(K)$ . Soit  $(x, y) \in \overline{K}^2$  un point de la partie affine de  $E$ . Par définition, il est rationnel sur  $L$  si et seulement si  $x$  et  $y$  sont dans  $L$ . Il en résulte que l'on a

$$E = \{(x, y) \in L \times L \mid y^2 = x^3 + ax + b\} \cup \{O\}.$$

**Exemple.** Soit la courbe  $E$  définie sur  $\mathbb{F}_5$  d'équation

$$y^2 = x^3 + x + 1.$$

Cette courbe vérifie bien la condition (3.2).

En effet, on a  $\Delta = -(4 \times 1^3 + 27 \times 1) = -31$ .

L'ensemble des points de la courbe est le suivant :

$$E(\mathbb{F}_5) = \{(0, 1), (0, 4), (2, 1), (2, 4), (3, 1), (3, 4), (4, 2), (4, 3)\} \cup \{O\}.$$

En effet, comme la courbe est symétrique, il nous suffit de vérifier que pour tous les valeurs de  $x$  dans  $\mathbb{F}_5$ , lesquelles sont un carré dans  $\mathbb{F}_5$ .

### CHAPITRE 3. DÉFINITIONS GÉNÉRALES SUR LES COURBES ELLIPTIQUES

---

Par exemple, pour  $x = 0$ , on a  $y^2 = 0^3 + 0 + 1$  donc  $y = \pm 1$ , ce qui nous donne les points d'abscisse  $x = 0$  et d'ordonnées  $y = \pm 1$  dans  $\mathbb{F}_5$ , par conséquent les points  $(0, 1)$  et  $(0, 4)$  vérifient l'équation  $f(x, y) = 0$  et sont donc des points de la courbe.

Maintenant si  $x = 1$ , l'équation de la courbe nous donne  $y^2 = 1^3 + 1 + 1 = 3$  donc il faut chercher si dans  $\mathbb{F}_5$ , s'il existe un carré modulo 5 égal à 3. Ce qui n'est pas le cas. En effet, dans  $\mathbb{F}_5$  les éléments sont  $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$  et on a successivement dans  $\mathbb{F}_5$

$$\begin{aligned}y^2 &= 0^2 = 0 \\y^2 &= 1^2 = \pm 1 \\y^2 &= 2^2 = 4 = -1 \\y^2 &= 3^2 = 9 = -1 \\y^2 &= 4^2 = 16 = 1 \\&\cdot\end{aligned}$$

Ainsi, il n'existe pas  $y \in \mathbb{F}_5$  qui vérifient l'équation de la courbe. Donc la courbe  $E$  ne possède pas de point de d'abscisse  $x = 1$ .

À voir si je mets  $\mathbb{F}_{25}$  je crois j'ai pigé faut que je vérifie ça ce midi ◇

# Chapitre 4

## Loi de groupe

Soit  $E$  une courbe elliptique définie sur  $K$ . Pour toute extension  $L$  de  $K$  dans  $\overline{K}$ , on va munir  $E(L)$  d'une structure naturelle de groupe abélien, d'élément neutre le point à l'infini.

### 4.1 Point de vue géométrique

**Proposition 4.1.** Soient une cubique irréductible non singulière  $E$  et une droite  $L$  définies sur  $K$ . Si la cubique  $E$  a au moins deux points d'intersection (comptés avec leur multiplicité) avec la droite  $L$ , alors le nombre de points d'intersection (comptés avec leur multiplicité) entre  $E$  et  $L$  est exactement 3.

**Démonstration.** En effet, comme  $E$  est irréductible, nous savons grâce à la proposition **ref** que le nombre de points à l'intersection de  $E$  et  $D$  est fini. Soit la droite  $D : aX + bY + cZ = 0$  où nous supposons  $c \neq 0$ . Les points  $P = (X, Y, Z)$  sont racines du polynôme  $F(X, Y, -\frac{aX+bY}{c})$  où  $F$  est le polynôme homogène de degré 3 qui définit  $E$ .

Notons :

$$q(X, Y) = F(X, Y, -\frac{aX+bY}{c}),$$

et soient  $P = (x_P, y_P, z_P)$  et  $Q = (x_Q, y_Q, z_Q)$  deux point, non nécessairement distinct, à l'intersection entre  $E$  et  $D$ . Comme  $q(x_P, y_P) = q(x_Q, y_Q) = 0$ , on peut écrire :

$$q(X, Y) = v(X, Y)(y_P X - x_P Y)(y_Q X - x_Q Y),$$

où  $v$  est un polynôme homogène de degré 1. Il n'a donc qu'une racine que nous noterons  $(x_R, y_R)$ . Le point  $R = (x_R, y_R, -\frac{ax_R+by_R}{c})$  est alors le troisième point de l'intersection entre  $E$  et  $D$ .  $\square$

### 4.2 Droites de $\mathbb{P}^2$

Le première objet dont l'on a besoin pour construire notre groupe et que le l'on va manipuler tout on l'on du processus est la droite projective.



**Définition 4.2.** Une droite de  $\mathbb{P}^2$  est une partie de  $\mathbb{P}^2$  formée des points  $[x, y, z]$  tels que

$$D : ux + vy + wz = 0,$$

où  $u, v$  et  $w$  sont des éléments non tous nuls de  $\overline{K}$ .

**reformule moi ça avec tes propres mots** On parle alors de la droite d'équation  $D$ . Une droite d'équation  $x = \lambda z$ , où  $\lambda \in \overline{K}^*$ , est dite vertical. Une telle droite passe par le point  $O = [0, 1, 0]$ .

En fait toute droite passant par le point  $O$  a une équation de la forme  $ux + wz = 0$ .

Comme on l'a vu avec le lien

La première question que l'on se pose alors est de savoir s'il existe une droite qui passe par deux points du plan projectif et si elle existe est-elle unique ?

La réponse à cette question est donné par le lemme suivant :

**Lemme 4.3.** Soient  $P = [a_1, a_2, a_3]$  et  $Q = [b_1, b_2, b_3]$  deux points distincts de  $\mathbb{P}^2$ . Il existe une unique droite de  $\mathbb{P}^2$  passant par  $P$  et  $Q$ . C'est l'ensemble des points  $[x, y, z] \in \mathbb{P}^2$  tels que le déterminant de la matrice

$$M = \begin{pmatrix} a_1 & b_1 & x \\ a_2 & b_2 & y \\ a_3 & b_3 & z \end{pmatrix}$$

soit nul. Autrement dit, c'est la droite d'équation  $ux + vy + wz = 0$ , avec

$$u = a_2b_3 - a_3b_2, \quad v = a_3b_1 - a_1b_3, \quad w = a_1b_2 - a_2b_1.$$

**Démonstration. A TERMINER**

Montrons qu'il existe une droite  $D$  passant par  $P$  et  $Q$ .

Les éléments  $u, v$  et  $w$  ne sont pas tous nuls car  $P$  et  $Q$  sont distincts.

En effet, si  $P = Q$  alors  $a_1 = b_1, a_2 = b_2$  et  $a_3 = b_3$  donc  $u = v = w = 0$  or  $P \neq Q$  donc il existe  $x \in \{u, v, w\}$  tel que  $x \neq 0$ .

□

### 4.3 Tangente à $E$ en un point

Le deuxième objet, dont l'on est amené à utiliser est la tangente.

En effet, il est naturel de se demander se qu'il se passe lorsque deux points du plan projectif ne sont pas distinct.

Ceci, nous permet de traité les cas où un point de la courbe possède une tangente à la courbe  $E$ , qui intersecte la courbe en un deuxième point ou qui est vertical à la courbe.

Soit

$$E : y^2z = x^3 + axz^2 + bz^3,$$

l'équation de  $E$ , où  $a, b \in K$ .

Notons

$$F = Y^2Z - (X^3 + aXZ^2 + bZ^3) \in K[X, Y, Z],$$

$$F_X = \frac{\partial F}{\partial X}, \quad F_Y = \frac{\partial F}{\partial Y}, \quad F_Z = \frac{\partial F}{\partial Z},$$

c'est-à-dire,

$$F_X = -(3X^2 + aZ^2), \quad F_Y = 2YZ, \quad F_Z = Y^2 - (2aXZ + 3bZ^2).$$

La première question que l'on doit se poser est de savoir si en tout point de la courbe il existe une tangente à la courbe en ce point.

Comme vu dans la définition ??, la courbe doit être lisse et par conséquent en tout point de la courbe il existe une tangente à la courbe  $E$ .

**Lemme 4.4.** Il n'existe pas de point  $P \in E$  tel que

$$F_X(P) = F_Y(P) = F_Z(P) = 0.$$

**Démonstration.** Supposons par l'absurde, qu'il existe un tel point  $P \in E$ . Remarquons que  $F_Z(O) = 1 \neq 0 = F_Z(P)$  donc par hypothèse  $P$  est distinct de  $O$ .

Pour fixer les idées posons  $P = [x, y, 1]$ .

Puisque  $\text{car}(K) \neq 2$ , on a

$$(F_Y = 0) \Leftrightarrow (2YZ = 0) \Leftrightarrow (Y = 0),$$

donc  $y = 0$ .

Donc  $P$  serait de la forme  $[x, 0, 1]$ .

On obtient alors

$$F_X = -(3X^2 + a) = 0 \text{ et } F_Z = -(2aX + 3b) = 0.$$

— Supposons  $a \neq 0$ , on alors à partir de  $F_Z$

$$X = -\frac{3b}{2a}.$$

Donc par  $F_X$

$$\begin{aligned} -\left(3\left(-\frac{3b}{2a}\right)^2 + a\right) &= 0 \\ -(27b^2 + 4a^3) &= 0. \end{aligned}$$

Ce qui est absurde car  $F$  est elliptique. D'après le lemme 3.3

— Supposons que  $a = 0$ , alors

$$(3b = 0) \underbrace{\Rightarrow}_{\text{car}(K) \neq 3} (b = 0).$$

Donc on  $a = b = 0$  donc  $-(27b^2 + 4a^3) = 0$  absurde car  $F$  est elliptique.  
(lem 3.3)

D'où le résultat.

□

Voici l'équation de la tangente en un point de la courbe.

**Définition 4.5.** Pour tout  $P \in E$ , la tangente à  $E$  en  $P$  est la droite d'équation

$$F_X(P)x + F_Y(P)y + F_Z(P)z = 0.$$

Maintenant que l'on sait qu'en tout point de la courbe il existe une tangente en ce point, et que l'on connaît l'équation de cette dernière. On est amené à étudier le comportement de la tangente à un point de la courbe dans le plan projectif. Ainsi, soit la tangente est vertical, soit elle intersecte la courbe en un nouveau point.

**Lemme 4.6. 1)** L'équation de la tangente à  $E$  au point  $O$  est  $z = 0$ .

**2)** Soit  $P = [x_0, y_0, 1]$  un point de  $E$  distinct de  $O$ . L'équation de la tangente à  $E$  en  $P$  est

$$F_X(P)(x - x_0z) + F_Y(P)(y - y_0z) = 0.$$

**Démonstration. 1)** Soit  $O \in E$  le point à l'infini. D'après l'équation de la tangente à  $E$  au point  $O$ . On a successivement

$$F_X(O) = 0, F_Y(O) = 0 \text{ et } F_Z(O) = 1.$$

Ainsi on retrouve bien  $z = 0$ .

**2)** Soit  $P$  un tel point, d'après l'équation (cite ? set up snippet -nommé + cité) de la tangente et de l'égalité  $y_0^2 = x_0^3 + ax_0 + b$  on a,

$$\begin{aligned} & F_X(P)x + F_Y(P)y + F_Z(P)z = 0 \\ & -(3x_0^2 + a)x + (2y_0)y + (y_0^2 - (2ax_0 + 3b))z = 0 \\ & -3x_0^2x - ax + 2y_0y + y_0^2z - 2ax_0z - 3bz = 0 \\ & -3x_0^2x - ax + 2y_0y + y_0^2z - 2ax_0z - 3z(y_0^2 - x_0^3 - ax_0) = 0 \text{ (i.e } b = y_0^2 - (x_0^3 + ax_0)) \\ & -3x_0^2x - ax + 2y_0y + y_0^2z - 2ax_0z - 3y_0^2z + 3x_0^3z + 3ax_0z = 0 \\ & -(3x_0^2 + a)x + 2y_0y - 2y_0^2z + (3x_0^2 + a)x_0z = 0 \\ & -(3x_0^2 + a)(x - x_0) + 2y_0(y - y_0z) = 0. \end{aligned}$$

D'où le résultat.

□

## 4.4 Loi de composition des cordes-tangentes

La proposition ?? nous permet de définir la loi de composition des cordes-tangentes :

1. Si  $P, Q \in E$ , distinct, nous pouvons définir la droite  $D = (PQ)$  la corde à la courbe passant par  $P$  et  $Q$ . Grâce à la proposition 4.8 on sait que cette corde prolongé à une droite intersect la courbe  $E$  en un unique troisième point qui appartient à  $E \cap D$ . Nous noterons ce troisième point  $f(P, Q)$ .
2. Si  $P \in E$ , et que  $Q = P$ , on peut définir la tangente  $D = (PP)$  à  $E$  au point  $P$ . De nouveau, la proposition ?? nous garantie l'existence d'un troisième point unique en comptant les multiplicités qui appartient à  $E \cap D$ . On notera ce dernier  $f(P, P)$ .

**Proposition 4.7.** Pour tous points  $P_1, P_2, Q_1$  et  $Q_2$  de  $E(K)$ , on a :

$$f(f(P_1, P_2), f(Q_1, Q_2)) = f(f(P_1, Q_1), f(P_2, Q_2)).$$

Pour une démonstration de ce résultat, voir

**Proposition 4.8.** Soient  $P$  et  $Q$  des points de  $E$ . Soit  $D$  la droite de  $\mathbb{P}^2$  passant par  $P$  et  $Q$  si  $P \neq Q$ , ou bien la tangente à  $E$  en  $P$  si  $P = Q$ . On a

$$D \cap E = \{P, Q, f(P, Q)\},$$

où  $f(P, Q)$  désigne le point de  $E$  défini par les conditions suivantes.

1) Supposons  $P \neq Q$ ,  $P \neq O$  et  $Q \neq O$ .

i) Supposons  $x_P \neq x_Q$ . Posons

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} \text{ et } \nu = \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}.$$

On a

$$f(P, Q) = [\lambda - x_P - x_Q, \lambda(\lambda^2 - x_P - x_Q) + \nu, 1]. \quad (4.1)$$

ii) Si  $x_P = x_Q$ , on a  $f(P, Q) = O$ .

2) Supposons  $P \neq O$  et  $Q = O$ . On a

$$f(P, O) = [x_P, -y_P, 1]. \quad (4.2)$$

De même, si  $P = O$  et  $Q \neq O$ , on a  $f(O, Q) = [x_Q, -y_Q, 1]$

3) Si  $P = Q = O$ , on a  $f(O, O) = O$ .

4) Supposons  $P = Q$  et  $P \neq O$ .

i) Si  $y_P = 0$ , on a  $f(P, P) = O$ .

ii) Supposons  $y_P \neq 0$ . Posons

$$\lambda = \frac{3x_P^3 + a}{2y_P} \text{ et } \nu = \frac{-x_P^3 + ax_P + 2b}{2y_P}.$$

On a

$$f(P, P) = [\lambda^2 - 2x_P, \lambda(\lambda^2 - 2x_P) + \nu, 1]. \quad (4.3)$$

**Démonstration.** Soient  $P = [x_P, y_P, 1]$  et  $Q = [x_Q, y_Q, 1]$  des points de  $E$  tels qu'ils sont distincts. Alors il existe une droite  $D \in \mathbb{P}^2$  qui passe par  $P$  et  $Q$ .

1) Supposons  $P \neq Q$ ,  $P \neq O$  et  $Q \neq O$ . Donc comme  $D$  existe, il existe un point  $M \in D \cap E$  et on cherche donc à connaître son comportement dans le plan  $E$ .

i) Supposons  $x_P \neq x_Q$ . Comme  $P, Q \neq O$ , le point à l'infini n'appartient pas à  $D$ . Comme  $M \in D$ , il est de la même forme que  $P$  et  $Q$ . Posons  $M = [x_0, y_0, 1]$  avec  $x_0, y_0$  des coordonnées sur  $\overline{K}$ .

Comme  $M \in E$ , on a la première égalité

$$y_0^2 = x_0^3 + ax_0 + b. \quad (4.4)$$

Ensuite avec  $M \in D$  d'après le lemme 4.3 on a la matrice suivante

$$\begin{pmatrix} x_P & x_Q & x_0 \\ y_P & y_Q & y_0 \\ 1 & 1 & 1 \end{pmatrix},$$

qui nous permet d'obtenir une seconde égalité.

$$(y_P - y_Q)x_0 - (x_P - x_Q)y_0 + (x_P y_Q - x_Q y_P) = 0$$

$$y_0 = \frac{y_P - y_Q}{x_P - x_Q} x_0 + \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}.$$

Posons

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} \text{ et } \nu = \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}.$$

Donc l'équation de  $D$  est de la forme

$$y = \lambda x + \nu z,$$

c'est-à-dire dans notre cas on a

$$y_0 = \lambda x_0 + \nu.$$

En remplaçant dans (4.4), il vient

$$\begin{aligned} (\lambda x_0 + \nu)^2 &= x_0^3 + ax_0 + b \\ \lambda^2 x_0^2 + 2\lambda \nu x_0 + \nu^2 &= x_0^3 + ax_0 + b \\ x_0^3 - \lambda^2 x_0^2 + (a - 2\lambda \nu)x_0 + b - \nu^2 &= 0. \end{aligned}$$

Donc  $x_0$  est une racine du polynôme

$$H = X^3 - \lambda X^2 + (a - 2\lambda\nu)X + b - \nu^2.$$

On remarque que  $H(x_P) = H(x_Q) = 0$  donc  $x_P$  et  $x_Q$  sont aussi des racines de  $H$ . Par les relations coefficients racines obtient la valeur de  $x_0$

$$\begin{aligned} x_0 + x_P + x_Q &= -(-\lambda^2) \\ x_0 &= \lambda^2 - x_P - x_Q. \end{aligned}$$

Ainsi les racines de  $H$  sont

$$x_P, \quad x_Q \quad \text{et} \quad \lambda^2 - x_P - x_Q.$$

Il en résulte que  $D \cap E$  est formé de  $P$ , et du point  $M = f(P, Q)$ .  
Donc

$$\begin{aligned} f(P, Q) &= [x_0, y_0, 1] \\ &= [\lambda^2 - x_P - x_Q, \lambda x_0 + \nu, 1] \\ &= [\lambda^2 - x_P - x_Q, \lambda(\lambda^2 - x_P - x_Q), 1]. \end{aligned}$$

D'où l'assertion.

- ii) Supposons  $x_P = x_Q$ . Comme  $P$  et  $Q$  sont distincts, on a alors  $y_P = -y_Q$ . D'après le lemme 4.3, la matrice suivante

$$\begin{pmatrix} x_P & x_Q & x \\ y_P & -y_Q & y \\ 1 & 1 & z \end{pmatrix}.$$

D'où l'équation de la droite suivante

$$\begin{aligned} 2y_P x - 2y_P x_P z &= 0 \\ x &= x_P z. \end{aligned}$$

Donc le point  $O$  est aussi un point de la droite  $D$  donc de  $D \cap E$ . Soit  $M \in D \cap E$  distincts de  $O$ . Si  $M = [0, 1, 0]$ , d'après la situation on a  $x_0 = x_P$  et  $y_0 = \pm y_P$ , donc  $M = P$  ou  $M = Q$ . Or on a  $P, Q \neq O$ . Donc on a nécessairement  $M = O$ . Ainsi on a bien  $D \cap E = \{P, Q, f(P, Q) = O\}$ , d'où l'assertion dans ce cas ci.

- 2) Supposons  $P \neq O$  et  $Q = O$ . Donc d'après lemme 4.3, on a

$$\begin{pmatrix} x_P & 0 & x \\ y_P & 1 & y \\ 1 & 0 & z \end{pmatrix}.$$

À partir de la deuxième ligne on obtient l'équation de la droite suivante

$$\begin{aligned} x_P z - x &= 0 \\ x &= x_P z. \end{aligned}$$

Si  $M = [x_0, y_0, 1]$  est un point de  $D \cap E$ , on a donc  $x_0 = x_P$  d'où  $y_0 = \pm y_P$ . On a ainsi  $D \cap E = \{P, O, f(P, O)\}$ , où  $f(P, O) = [x_P, -y_P, 1]$ .

- 3) Supposons  $P = Q = O$ , par le lemme 4.6 la tangente  $D$  à  $E$  au point  $O$  à pour  $z = 0$ . Par suite,  $O$  est le seul point de  $D \cap E$ , d'où  $f(O, O) = O$ .
- 4) Supposons  $P = Q$  et  $P \neq O$ . L'équation de la tangente  $D$  à  $E$  en  $P$  a donc pour équation

$$F_X(P)(x - x_P z) + F_Y(P)(y - y_P z) = 0.$$

- i) Si  $y_P = 0$ , on a

$$x_P^3 + ax_P + b = 0.$$

Donc  $x_P$  est racine simple de ce polynôme. De plus,  $F_X(P) \neq 0$ . En effet, si  $F_X(P) = 0$  on a

$$\begin{aligned} -(3x_P^2 + a) &= 0 \\ x_P^2 &= -\frac{a}{3}, \end{aligned}$$

ce qui est absurde.

Ainsi à partir de l'équation de la tangente  $D$  on a

$$\begin{aligned} F_X(P)(x - x_P z) = 0 &\Rightarrow (F_X(P)) = 0 \vee (x - x_P z) = 0 \\ &\Rightarrow x - x_P z = 0. \end{aligned}$$

Donc pour  $D$  on a

$$D : x = x_P z.$$

Le seul point de  $D \cap E$  distinct de  $P$  est donc le point  $O$ , d'où  $D \cap E = (P, O)$ , d'où l'assertion.

- ii) Supposons  $y_P \neq 0$ . Du lemme 4.6 et de l'équation  $b = y_P^2 - x_P^3 - ax_P$  on obtient

$$\begin{aligned} -(3x_P^2 + a)(x - x_P z) + 2y_P(y - y_P z) &= 0 \\ -3x_P^2 x + 3x_P^3 z - ax + ax_P z + 2y_P y - 2y_P^2 z &= 0 \\ 2y_P y = 3x_P^2 x - 3x_P^3 z + ax - ax_P z + 2y_P^2 z \\ 2y_P y - ax_P z &= 3x_P^2 x + ax - x_P^3 z + 2b \\ y &= \frac{3x_P^2 + a}{2y_P} x + \frac{-x_P^3 + ax_P + 2b}{2y_P} z. \end{aligned}$$

On pose  $\lambda = \frac{3x_P^2 + a}{2y_P}$  et  $\nu = \frac{-x_P^3 + ax_P + 2b}{2y_P}$  et on obtient l'équation de  $D$ , c'est-à-dire

$$y = \lambda x + \nu z.$$

Le point  $O$  n'est donc pas sur  $D$ . Soit  $M = [x_0, y_0, 1]$  un point de  $E \cap D$ . On a par le même raisonnement que dans le cas (1-i) (utilise ref?) les deux équations suivantes

$$y_0^2 = x_0^3 + ax_0 + b \quad \text{et} \quad y_0 = \lambda x_0 + \nu.$$

Par suite  $x_0$  est une racine du polynôme

$$G = X^3 - \lambda^2 X^2 + (a - 2\lambda\nu)X + b - \nu^2.$$

Le polynôme dérivé de  $G$  est

$$G' = 3X^2 - 2\lambda^2 X + a - 2\lambda\nu.$$

On a

$$\begin{cases} G(x_P) = (0) \Leftrightarrow x_P^3 - \lambda^2 x_P^2 + (a - 2\lambda\nu) x_P + b - \nu^2 = 0 \\ y_P^2 = x_P^3 + ax_P + b \Rightarrow b = y_P^2 - x_P^3 - ax_P \quad \text{et} \quad y_P = \lambda x_P + \nu \Rightarrow \nu = y_P - \lambda x_P \end{cases}.$$

Donc,

$$\begin{aligned} G(x_P) &= x_P^3 - \lambda^2 x_P^2 + (a - 2\lambda(y_P - \lambda x_P)) x_P + y_P^2 - x_P^3 - ax_P - (y_P - \lambda x_P)^2 \\ &= x_P^3 - \lambda^2 x_P^2 + ax_P - 2\lambda x_P y_P + 2\lambda^2 x_P^2 + y_P^2 - x_P^3 - ax_P - y_P^2 + 2\lambda x_P y_P - \lambda^2 x_P^2 \\ &= 2\lambda^2 x_P^2. \end{aligned}$$

Par suite,

$$\begin{aligned} G'(x_P) = 0 &\Leftrightarrow 3x_P^2 - G(x_P) + a - 2\lambda\nu = 0 \\ &\Leftrightarrow G(x_P) = 3x_P^2 + a - 2\lambda\nu \\ &\Leftrightarrow G(x_P) = 0 \\ &\Leftrightarrow x_P \text{ racine de } G. \end{aligned}$$

Ainsi,  $x_P$  est une racine d'ordre au moins 2 de  $G$ . Les racines de  $G$  sont donc

$$x_P \quad \text{et} \quad \lambda^2 - 2x_P.$$

On obtient donc par le même raisonnement que (1-i) la formule annoncée.

□

On obtient alors une loi de composition interne sur  $E$ , appelée loi de composition des cordes-tangentes,  $f : E \times E \rightarrow E$  qui à tout couple de point  $(P, Q)$  de la courbe associe le point d'intersection de la corde ou tangente associé  $f(P, Q) \in E$  défini dans la proposition 4.8

**Exemple.**

◇

## 4.5 Loi de groupe

Considérons comme précédemment  $a$  et  $b$  des éléments de  $K$  tels que  $4a^3 + 27b^2 \neq 0$  et  $E$  la courbe elliptique définie sur  $K$  d'équation

$$y^2 = x^3 + ax + b.$$

Notons  $+$  la loi de composition interne sur  $E$ , définie pour tous  $P$  et  $Q$  dans  $E$  par l'égalité

$$P + Q = f(f(P, Q), O). \quad (4.5)$$

Géométriquement,  $P + Q$  s'obtient à partir de  $f(P, Q)$ , qui est le point d'intersection de la droite  $(PQ)$  à la courbe, par symétrie par rapport à l'axe des abscisses. Cette loi de composition est une loi de groupe sur  $E$ .



**Théorème 4.9.** Le couple  $(E, +)$  est un groupe abélien, d'élément neutre  $O$ . La loi interne  $+$  est décrite explicitement par les formules suivantes.

Soient  $P$  et  $Q$  des points de  $E$  distincts de  $O$ . Posons  $P = (x_P, y_P)$  et  $Q = (x_Q, y_Q)$ .

1) Supposons  $x_P \neq x_Q$ . Posons

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} \quad \text{et} \quad \nu = \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}.$$

On a

$$P + Q = (\lambda^2 - x_P - x_Q, -\lambda(\lambda^2 - x_P - x_Q) - \nu). \quad (4.6)$$

2) Si  $x_P = x_Q$  et  $P \neq Q$ , on a  $P + Q = O$ .

3) Supposons  $P = Q$  et  $y_P \neq 0$ . Posons

$$\lambda = \frac{3x_P^2 + a}{2y_P} \quad \text{et} \quad \nu = \frac{-x_P^3 + ax_P + b}{2y_P}.$$

On a

$$2P = (\lambda^2 - 2x_P, \lambda(\lambda^2 - 2x_P) - \nu). \quad (4.7)$$

4) Si  $P = Q$  et  $y_P = 0$ , on a  $2P = O$ .

5) L'opposé de  $P$  est le point

$$-P = (x_P, -y_P). \quad (4.8)$$

**Démonstration.** 1) Supposons  $x_P \neq x_Q$ , compte tenu de (4.5), (4.1) et (4.2) on a

$$\begin{cases} (4.1) \Leftrightarrow f([\lambda^2 - x_P - x_Q, \lambda(\lambda^2 - x_P - x_Q) + \nu, 1], [0, 1, 0]) \\ (4.2) \Leftrightarrow f(P, O) = [x_P, -y_P, 1] \end{cases}.$$

On retrouve bien la formule (4.6).

2) Supposons  $x_P = x_Q$  et  $P \neq Q$  c'est à dire  $y_P \neq y_Q$ .

D'après la proposition 4.8 (1-i), on a  $f(P, Q) = O$  donc  $f(f(P, Q), O) = f(O, O) = O$ . D'où la formule énoncé.

3) Supposons  $P = Q$  et  $y_P \neq 0$ , en prenant compte (4.5), (4.2) et (4.3) on obtient

$$\begin{cases} (4.3) \Leftrightarrow f([\lambda^2 - 2x_P, \lambda(\lambda^2 - 2x_P) + \nu, 1], [0, 1, 0]) \\ (4.2) \Leftrightarrow f(P, O) = [x_P, -y_P, 1] \end{cases}.$$

Ce qui permet de retrouver la formule (4.7).

4) Supposons  $P = Q$  et  $y_P = 0$ , d'après l'assertion (4-i) de la proposition 4.8, on a  $f(P, P) = O$  d'où  $2P = f(f(P, P), O) = f(O, O) = O$ .

- 5) Pour l'opposer on cherche un point  $M \in E$  tel que  $P \neq M$  et  $P, Q \neq O$  d'après le théorème énoncé assertion 2) on a donc  $x_P = x_M$  et donc nécessairement  $y_M = -y_P$  donc le point recherché est  $M = (x_M, y_M) = (x_P, -y_P) = -P$ .

□

**Remarque.** Pour ce qui est de l'associativité de la loi de groupe, il faudrait traiter chaque cas et montrer que les formules sont bien associatives. Ce qui long et fastidieux. Cependant, l'avantage de notre loi étant qu'elle a une interprétation géométrique on peut donner une preuve géométrique que notre loi de composition est bien une loi de groupe sur  $E$ .

**Démonstration** (géométrique du théorème 4.9). 1) La loi  $+$  défini par  $P + Q = f(f(P, Q), O)$  est bien interne.

En effet, c'est l'intersection d'une droite et la courbe, c'est à dire un point de la courbe.

- 2) La loi  $+$  est associative (cite Fig).

En effet, si  $P, Q$  et  $R$  sont trois points de la courbe, on a :

$$\begin{aligned} f(P, (Q + R)) &= f(P, f(f(Q, R), O)) \\ &= f(f(f(P, Q), Q), f(f(Q, R), O)) \text{ car } P = f(f(P, Q), Q) \\ &= f(f(f(P, Q), O), f(f(Q, R), O)) \end{aligned}$$

□

**Exemple.** mettre exemple de calcul de  $2P$  pour la suite

◇

## Chapitre 5

# Applications

Le groupe abélien  $(E, +)$  des courbes elliptiques et même les courbes elliptiques en générale, ont de nombreuses applications que ce soit dans le domaine pratique, ou bien dans le domaine théorique.

En effet, on peut notamment citer leurs utilisation dans la mécanique classique dans la description du mouvement des toupies. Elles interviennent également en théorie des nombres, dans la démonstration du dernier théorème de Fermat.

Enfin, on les retrouve aussi en cryptologie, dans le problème de la factorisation des entiers.

Dans ce mémoire, on s'intéresse à leur application en cryptographie. Où elles ont permit notamment la réduction de la taille des clés cryptographique.

Aujourd'hui, le groupe  $E$  des courbes elliptique intervient notamment pour l'échange de clé et les signatures numériques.

La révolution qui à permit à la cryptographie de passer du domaine de l'art au domaine des sciences est l'invention du concept d'échange de clé public.

### 5.1 Protocole de signature

Un protocole de signature est un protocole d'authentification. On peut faire le parallèle avec la signature manuscrit que l'on utilise pour signer des documents officiel. Le principe est le même mais avec des chiffres. Dans notre cas il se repose sur le logarithme discret sur une courbe elliptique. Cependant, dans ce cadre comme pour celui du  $(\mathbb{Z}/p\mathbb{Z})^*$ , il faut éviter certaines situation qui sont faibles du point de vue de la sécurité.

#### 5.1.1 Choix du corps de définition

Avant tout chose comme la courbe elliptique est défini sur un corps, il faut choisir ce dernier pour éviter certaines attaques avant même d'avoir commencé le chiffrement.

Il est donc préférable de choisir :

- Soit un corps premier  $\mathbb{F}_p$ , où  $p$  est un grand nombre premier. De l'ordre de 256 bit, c'est à dire, un nombre composé de plus de 77 chiffres. **VÉRIFIE QUAND MÊME CE QUE TU RACONTES.**
- Soit un corps  $\mathbb{F}_{p^r}$  de caractéristique  $p$  petite (en général  $p = 2$ ), où  $r$  est un nombre premier tel que l'ordre de 2 dans  $\mathbb{F}_r^*$  est grand (en particulier, il faut éviter les nombres premiers de Fermat et Mersenne).

### 5.1.2 Choix de la courbe elliptique

Le corps  $k = \mathbb{F}_q$  étant choisi, on note  $p$  sa caractéristique. Soit  $E$  la courbe elliptique considérée,  $t$  la trace du Frobenius,  $G \in E(\mathbb{F}_q)$  le point de base et  $\ell$  son ordre dans  $E(\mathbb{F}_q)$ .

Pour éviter de nouveau certaines attaque, il est à noter que :

- Si  $\ell$  n'est pas premier, il est possible de simplifier le calcul du logarithme discret. (réduction de Pohlig-Helman)
- Si  $t = 1$ , on dit que la courbe  $E$  est anormale, bien que ce soit un cas rare. De plus, si  $q = p$  est premier, le problème du logarithme discret sur  $E$  peut être résolu en un temps linéaire. (attaque de Smart)
- Si  $v$  est le plus petit entier tel que  $\ell \mid q^v - 1$ , alors on peut ramener le problème de logarithme discret sur le corps fini  $\mathbb{F}_{q^v}$  grâce au pairing de Weil. (attaque de Menezes-Okamoto-Vanstone).

Le degré MOV est défini comme le plus petit entier  $v$  pour lequel on a  $\text{Card}(E(\mathbb{F}_q)) \mid q^v - 1$ . On doit donc s'assurer que  $v$  ne soit pas petit sans pour autant le calculer explicitement. En particulier, la courbe  $E$  ne doit pas être supersingulière. Si  $E$  est une courbe supersingulière, on peut montrer que son degré MOV est  $\leq 6$  donc vulnérable.

**Exemple.** Considérons l'exemple de  $E$  définie par  $y^2 = x^3 + 33x + 69$  dans le corps  $\mathbb{F}_p = \mathbb{F}_{1000033}$ . On a

- $\ell = 1001041$  qui est du même ordre de grandeur que  $p$ .
- $t = -1007$ , la courbe n'est ni anormale, ni supersingulière.
- Le degré MOV de la courbe vaut 10320.

Calculer le degré MOV d'une courbe elliptique revient en fait à trouver  $v$  tel que  $q^v \equiv 1 \pmod{|\text{Card}(E(\mathbb{F}_q))|}$ . C'est donc trouver l'ordre de  $q$  dans  $(\mathbb{Z}/|\text{Card}(E(\mathbb{F}_q))|\mathbb{Z})^*$ .

Une bonne stratégie pour générer des courbes satisfaisante est de les construire au hasard et de s'assurer qu'elles semblent raisonnables en vue de nos critères.

◇

**Algorithme.** ·Entre : corps fini  $K$ .

·Sortie : une courbe elliptique  $E(K)$ , un point  $G \in E$  ayant un grand ordre.

Étape 1 : Choisir au hasard une courbe elliptique  $E$  définie sur  $K$ .

Étape 2 : Calculer  $\text{Card}(E(K))$  et vérifier que la courbe n'est pas anormale et que son degré MOV est grand (sinon retour à l'étape 1).

Étape 3 : Factoriser  $\text{Card}(E(K))$ . Si cela prend trop de temps aller à l'étape 1. Si  $\text{Card}(E(k))$  n'est pas de la forme  $s\ell$  avec  $s$  petit et  $\ell$  premier grand, aller à l'étape 1.

Étape 4 : Chercher un point au hasard  $P \in E$ , si  $sP = \mathcal{O}$ , aller à l'étape 4 ou aller à l'étape 1 si la recherche d'un point convenable a échoué). Sinon, retourner  $E$  et  $G = sP$ .

### 5.1.3 ECDSA

Le protocole "Elliptic Curve Digital Signature Algorithm" repose sur le problème du logarithme discret.

Pour simplifier supposons que les courbes sont définies sur un corps  $K = \mathbb{F}_p$ , où  $p$  est un grand nombre premier. Soit  $E$  une courbe elliptique définie sur  $K$  et  $G \in E$  d'ordre premier  $\ell$ .

Supposons qu'Alice et Bob communiquent et qu'ils veulent pouvoir authentifier les messages de chacun.

Alice et Bob choisissent aléatoirement un nombre  $1 < n_A, n_B < \ell - 1$  et calcul respectivement  $P_A = n_A G$  pour Alice et  $P_B = n_B G$  pour Bob. C'est deux nouveau point sont alors leurs clé publique et les entiers  $n_A$  et  $n_B$  leur clé secrète respective.

Entrée : un message  $m$

Sortie : La signature du message  $m$  par Alice.

Étape 1 : Choisir un nombre aléatoire  $1 < k < \ell - 1$  et calculer  $kG = (x, y) \in E(K)$ . On peut toujours supposer que  $x$  est dans l'intervalle  $[0, p - 1]$  et c'est ce que l'on fait.

Étape 2 : Calculer  $r$  tel que  $r = x \pmod{\ell}$ . Si  $r = 0$  retourner à l'étape 1.

Étape 3 : Calculer  $s = k^{-1}(H(m) + n_A r) \pmod{\ell}$  où  $H$  est une fonction de hachage. Si  $s = 0$  retourner à l'étape 1.

Étape 4 : Retourner la signature  $(r, s)$ .

## 5.2 Protocole d'échange de clé