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

Département de Mathématiques
LAMFA
CNRS 33 Rue Saint-Leu, 80000 Amiens, France

May 11, 2022

Table des matières

Chapitre 1

1.1 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 clair des différents concepts et enjeux qui la compose.

1.2 Cryptographie

La cryptographie trouve ses origines avec l'invention de l'écriture, en effet on en retrouve des traces dés 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 ce 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 souhaiterai transmettre par écrit un message dont seul le déstinataire 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 première exemple bien connu de cryptographie est appelé le chiffrement de César.

Cette méthode consiste à prendre les lettres de l'aphabet et d'éffectuer 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 Végenère, inventé par Blaise de

Vigenère en 1586 dans traité des chiffre paru en 1586 (on retrouve cependant une méthode analogue dans un court traité de Giovan Battista Bellano paru en 1553), le chiffrement de Vegenère repose sur le même principe que le chiffrement de César. À ceci prés que 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 prés 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 Vegenère essaye de contourner le problème de l'analyse de fréquence d'apparition des lettres, qui permet de rendre innéficace les chiffrement du type chiffrement de César avec un seul alphabet. 3 siècle aprés son apparition en 1863 le major prussien Friedrich Kasiski à publié une méthode pour percé le chiffrement de Vegenère.

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 le nomme chiffrement par substitution polyalphabétique.

On retiendra que ces méthodes non 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 considérer 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 millitaire". 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'aprés 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 cryptosystème, pour utiliser un terme plus précis, est considérer comme sûr.

Un cryptosystème est la méthode de chiffrement et de dechiffrement qui permet de transmettre ou recevoir des informations secrètes. On peut en retrouver une description plus précise dans cette article cite culture maths

C'est ainsi, qu'en 1976 Diffie et 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.

Cette nouvelle méthode est la pierre fondadrice de la cryptographie moderne basé sur le principe de clé publique et clé secret, qui sont deux clés disctinctes. 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 secrete au déchiffrement.

On peut se représenter le principe, en considérant deux personnes, traditionnelement 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. Alice souhaite pouvoir se faire envoyer des messages chiffrés de $\mathcal{M}$ de façon privée. Elle choisit une bijection $f_A : \mathcal{M} \to \mathcal{M}$ qui sera rendu publique, et elle seul en connaît la reciproque 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 appel ce genre de fonction des fonctions à sens unique, car leurs reciproques sont difficiles à expliciter.

L'enjeux 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 inverses est le plus difficiles possible.

La cryptographie d'aujourd'hui est basé sur deux problèmes issu de la Théorie des nombres. À savoir le problème de la factorisation des entiers et celui du logarithme discret.

introduit les deux problèmes et dit pourquoi ils sont difficils

1.3 Les courbes elliptiques

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

l'objectif ici et d'introduire les courbes elliptiques à partir de leur histoire. resume en gros les principales problématiques et ce qu'elles ont apporté par notamment de l'application d'abel et jacobi qui amene le groupe dans $\mathbb{C}$

en parallé parle de diophante et de l'idée derrière l'addition les lignes relie le blog math u prog

FIGURE 1.1 – Exemple

Chapitre 2

Le plan projectif $\mathbb{P}^2(\overline{K})$

La définition que nous allons utilisé 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 indépendammenent 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 formel.

Dans un premier temps pour comprendre les concepts liées aux espaces projectif. Partons de la droite projective qui est un espace projectif de dimension 1.

Définition 2.1. La droite projective sur $\overline{K}$, que l'on note $\mathbb{P}^1(\overline{K})$ ou $\mathbb{P}^1$, est l'ensemble quotient

$$\overline{K}^2 - \{(0,0)\} / \sim$$

où $\sim$ est la relation d'équivalence telle que pour tous (x, y) et (x', y') non nuls de $\overline{K}^2$,

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

Pour tous (x, y) non nuls dans $\overline{K}^2$, on note $[x, y]$ sa classe d'équivalence appelée coordonnées homogènes.

Un point de la droite projective est donc définie par les droites vectorielles privée de l'origine.

On a alors deux types de point, les points de la forme $[x, 1]$ et ceux de la forme $[x, 0]$.

Pour le premier type, comme $y \neq 0$ on a naturellement $\lambda = \frac{1}{y}$. On obtient alors l'intersection de tous les droites vectorielles avec la droite affine $y = 1$, ceux qui forme la droite sur K.

Le deuxième type correspond à l'ensemble des droites affines parallèle à l'ordonné, de plus pour tous $x \neq 0$, on a $\lambda = \frac{1}{x}$, donc peut importe la valeur de x les droites s'intersectent au point $[1, 0]$.

Intuivement, la droite projective sur K est une droite affine sur K complétée par un point, appelé point à l'infini que l'on note $\mathcal{O}$. Ainsi dans l'espace projectif deux droites parallèles s'intersectent en un point à l'infini. Quand on parle de droite à l'infini, on désigne par cette droite l'ensemble des points à l'infini.

Le point à l'infini étant l'intersection des droites paralléles

Définition 2.2. 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 $\overline{K}^3$,

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

Donnons également, la définition de la droite projective espace projectif de dimension 1,

L'espace projectif permet de formaliser et généraliser à toute dimension la notion de droite à l'infini dans le plan projectif.

Le plan projectif permet d'introduire la notion d'homogénéisation des équations de courbes algébrique. Ce procédé permet à partir de l'équation initial d'une courbe algébrique du plan usuel, admettant une équation de la forme $P(x, y) = 0$ où $P \in K[X, Y]$, d'obtenir une équation d'une courbe qui est dans le plan projectif, et donc de prolonge la courbe initiale à la droite à l'infini. Autrement dit, on définit un plan affine en choisissant une droite projective quelconque associée à ce plan, qui est la droite à l'infini

Pour bien comprendre ce qu'est le plan projectif, parlons d'abord de la droite projective $\mathbb{P}^1$, qui est un espace projectif de dimension 1.

Si K est le corps des nombres réels, alors la droite projective réelle est obtenue en intersectant les droites vectorielles de $\mathbb{R}^2$ avec le cercle unité.

On a donc l'ensemble des droites vectorielles de $\mathbb{R}^2$ qui sont de la forme $[x, y]$ avec $y \neq 0$.

Ceci permet d'obtenir à partir de l'équation initiale, une nouvelle équation qui prolonge la courbe initiale à la droite infini. C'est ce qui nous permet de construire un élément neutre qui soit bien définie pour la loi du groupe.

Pour se donner une idée des parties qui compose le plan projectif raisonnons avec les réels.

Pour $K = \mathbb{R}$, par définition le plan projectif $\mathbb{P}^2(\mathbb{R})$, est l'ensemble quotient de tous les vecteurs colinéaire de $\mathbb{R}^3$ privée de l'origine. Ainsi, pour tous vecteurs $(x, y, z) \in \mathbb{P}^2$, un représentant de classe est de la forme $(\lambda x, \lambda y, \lambda z)$, et on note $[x, y, z]$ sa classe d'équivalence.

Ainsi, on a les points de la forme $[x, y, 0]$ qui forme la droite à l'infini et les autres points peuvent tous être écrit de la forme $[x, y, 1]$ et il forme le plan affine.

Pour comprendre ce que sont la droite à l'infini et le plan affine, parlons de l'homogénéisation des droites.

Les équations d'une droite dans le plan affine sont de la forme $ax + by + c = 0$, où a et b deux réels non tous deux nuls et c un réels quelconque. Ainsi, l'équation homogène associé est de la forme $P(x, y, z) = ax+by+cz = 0$, c'est un polynome à plusieurs indéterminées dont tous les monômes non nuls sont de même degré total, donc un polynôme homogène de degré 1.

On a alors qu'un point du plan projectif de coordonées homogène $[x, y, z]$ est sur la droite projective si et seulement si $P(x, y, z) = 0$. Autrement dit, les zéros du polynôme homogène sont les points du plan affine dans $\mathbb{P}^2$ et ceci indépendament du choix des coordonnées homogènes.

En effet, comme $[x, y, z] = \left\{(x, y, z) \in \mathbb{R}^3 \mid \exists\lambda \in \mathbb{R}^*,\ (x, y, z) = \lambda(x, y, z)\right\}$, par homogénéité, on a

$$P(\lambda x, \lambda y, \lambda z) = \lambda P(x, y, z)$$

donc $P(x, y, z) = 0$.

Traditionnelement, on prend pour z la valeur 1, ainsi un point dans le plan affine est de la forme $[x, y, 1]$ tel que $P(x, y, 1) = P(x, y)$, ce qui montre que le point $[x, y, 1]$ est sur la droite projective si et seulement si le point (x, y) est sur la droite affine. Ainsi, on a bien opéré un prolongement de la droite affine initial en une droite projective.

Si l'on pose

$$U_0 = \left\{[x, y, z] \in \mathbb{P}^2(\mathbb{R}) \mid z \neq 0\right\},$$

on a l'application $\varphi : U_0 \to \mathbb{R}^2$ définie par :

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

C'est une bijection dont la réciproque est donnée par :

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

Le plan affine dans l'espace projectif est donc une représentation du plan euclidien $\mathbb{R}^2$. L'image suivante permet de comprendre ce que l'on obtient.

Par suite, si $z = 0$, on a deux choix qui s'offre à nous à savoir $x \neq 0$ ou $y \neq 0$. Pour fixer les idées prennons $y = 1$. Ainsi, un point de la droite projective est de la forme $[x, 1, 0]$ tel que P(x,1,0)=P(x,1). Ainsi, le point $[x, 1, 0]$ est sur la droite projective si et seulement si le point $(x, 1)$ est sur la droite affine initial.

bijection

image

droite à l'infini

droite et point les cas

presente une courbe la canonique

parle du determinant et de son influence sur la courbe

parle de la forme normal de W

Chapitre 3

Définitions générales

Dans tout ce qui suit, je vais prendre pour fil rouge le cours de Mr Alain Kraus [Kra10]. Dans cette optique, je vais essayer de completer ce cours, en y ajoutant soit des détails supplémentaires lors des différentes démonstration, soit en explicitant des concepts où je juge cela nécéssaire.

3.1 Définition

Dans cette partie, je vais définir le contexte autour duquel la théorie est construite.

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.

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

Définition 3.1. Une courbe elliptique définie sur K est une courbe projective plane d'équation

$$y^2z = x^3 + axz^3 + bz^2. \tag{3.1}$$

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

$$4a^3 + 27b^2 \neq 0. \tag{3.2}$$

D'aprés la définition ci-dessus, une courbe elliptique est un objet de la géométrie projective, que l'on représente dans le plan projectif.

D'abord donnons la définition de ce qu'est le plan projectif $\mathbb{P}^2$,

Définition 3.2. Le plan projectif $\mathbb{P}^2(\overline{K})$ est l'ensemble quotient

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

où $\sim$ est la relation d'équivalence qui pour tous (x_1, y_1, z_1) et (x_2, y_2, z_2), non nuls de $\overline{K}^3$ on a

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2) \Leftrightarrow \exists \lambda \in \overline{K},\ (x_2, y_2, z_2) = \lambda(x_1, y_1, z_1).$$

Pour tous $(x, y, z) \in \overline{K}^3$, non nul, on notera alors $[x, y, z]$ sa classe d'équivalence.

Parle des coordonnées homogène et droite projective Signe de delta Point de rebroussement homogénéité entre f et F des solutions

Donnons nous a et b des éléments de K. Dans l'anneau des polynômes $K[X, Y, Z]$, posons

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

Comme F est un polynôme homogène de degré 3. Grâce à au plan projectif. Si (x, y, z) est un élément non nul de $\overline{K}^3$, la condition $F(x, y, z) = 0$, 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.

lemme pour eviter les courbes non lisse

Lemme 3.3. Soit $\Delta = -(4a^3 + 27b^2)$ le discriminant $f = x^3 + ax + b$. Les racines de f sont simples, si et seulement si $\Delta \neq 0$.

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

Soit Δ le discriminant de f. Soient α, β, γ les racines de f dans $\overline{K}$ et f' le polynôme dérivé de f.

Tout d'abord montrons que :

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

D'après le théorème de d'Alembert on peut écrire f sous la forme :

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

En dérivant f sous cette forme on obtient :

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

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,

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

Ce qui donne :

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

On peut écrire

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha+\beta+\gamma)^2 - 2(\alpha\beta + \alpha\gamma + \beta\gamma),$$

$$\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 = (\alpha\beta + \alpha\gamma + \beta\gamma)^2 - 2\alpha\beta\gamma(\alpha+\beta+\gamma).$$

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 :

$$\alpha + \beta + \gamma = -\frac{b}{a},$$

$$\alpha\beta + \alpha\gamma + \beta\gamma = \frac{c}{a},$$

$$\alpha\beta\gamma = -\frac{d}{a}.$$

Donc pour 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 :

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

Maintenant, supposons que $\Delta = 0$. On a alors :

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

D'où le résultat. □

3.2 Partie affine et point à l'infini

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

Posons

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

On dispose de l'application $\varphi : U \to \overline{K}^2$ 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 φ 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 identifira $E \cap U$ et le sous-ensemble de $\overline{K}^2$ formé des éléments (x, y) vérifiant (3.3). Avec cette identification, on a

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

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 3.4. 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 λx, λy et λz soient dans L. On note $\mathbb{P}^2(L)$ l'ensemble des points de $\mathbb{P}^2$ rationnels sur L.

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 $\frac{x_j}{x_i}$ appartienne à L.

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

Définition 3.5. 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

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

Exemple. ◇

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

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

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

reformule moi ça avec tes propres mots

ce lemme garantit l'unicité et l'existence d'une droite qui passe par deux points de la courbe

Lemme 4.2. Soient $P = [a_1, a_2, a_3]$ et $Q = [b_1, b_2, b_3]$ deux points distincs 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

$$u = a_2b_3 - a_3b_2,\ v = a_3b_1 - a_1b_3,\ w = a_1b_2 - a_2b_2.$$

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 $x \neq 0$.

□

4.2 Tangente à E en un point

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

Soit

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

l'équation de E, où $a, b \in K$.

Notons

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

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

c'est-à-dire,

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

comprend à quoi y sert ce lemme

Lemme 4.3. 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 disctinct de O.

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

Puisque $\mathrm{car}(K) \neq 2$, 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

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

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

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

Donc par F_X

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

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 $-\left(27b^2 + 4a^3\right) = 0$ absurde car F est elliptique. (lem 3.3)
D'où le résultat.

□

Définition 4.4. Pour tout $P \in E$, la tangente à E en P est la droite d'équation

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

c'est le lemme qui nous permet de traiter les cas de la tangente en E vertical et non vertical

Lemme 4.5. 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

$$F_X(P)\,(x - x_0 z) + F_Y(P)\,(y - y_0 z) = 0.$$

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,

$$F_X(P)x + F_Y(P)y + F_Z(P)z = 0$$
$$-\left(3x_0^2 + a\right)x + (2y_0)\,y + \left(y_0^2 - (2ax_0 + 3b)\right)z = 0$$
$$-3x_0^2 x - ax + 2y_0 y + y_0^2 z - 2ax_0 z - 3bz = 0$$
$$-3x_0^2 x - ax + 2y_0 y + y_0^2 z - 2ax_0 z - 3z\left(y_0^2 - x_0^3 - ax_0\right) = 0 \left(\text{i.e } b = y_0^2 - \left(x_0^3 + ax_0\right)\right)$$
$$-3x_0^2 x - ax + 2y_0 y + y_0^2 z - 2ax_0 z - 3y_0^2 z + 3x_0^3 z + 3ax_0 z = 0$$
$$-\left(3x_0^2 + a\right)x + 2y_0 y - 2y_0^2 z + \left(3x_0^2 + a\right)x_0 z = 0$$
$$-\left(3x_0^2 + a\right)(x - x_0) + 2y_0\,(y - y_0 z) = 0.$$

D'où le résultat.

□

4.3 Loi de composition des cordes-tangentes

Ainsi munie de la droite et de la tangente, on a tous les armes pour se confronter aux différentes situation.

Proposition 4.6. 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

$$f(P,Q) = \left[\lambda - x_P - x_Q, \lambda\left(\lambda^2 - x_P - x_Q\right) + \nu, 1\right]. \tag{4.1}$$

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

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

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

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

$$f(P,P) = \left[\lambda^2 - 2x_P, \lambda\left(\lambda^2 - 2x_P\right) + \nu, 1\right]. \tag{4.3}$$

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 connaitre 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

$$y_0^2 = x_0^3 + ax_0 + b. \tag{4.4}$$

Ensuite avec $M \in D$ d'après le lemme 4.2 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.

$$\begin{aligned} (y_P - y_Q)\, x_0 - (x_P - x_Q)\, y_0 + (x_P y_Q - x_Q y_P) &= 0 \\ y_0 = \frac{y_P - y_Q}{x_P - x_Q} x_0 + \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}&. \end{aligned}$$

Posons

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

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 remplacent 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

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

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

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

D'où l'assertion.

ii) Supposons $x_P = x_Q$. Comme P et Q sont distinct, on a alors $y_P = -y_Q$. D'après le lemme 4.2 , 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 4.2 , 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 4.5 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

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

i) Si $y_P = 0$, on a

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

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

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

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 4.5 et de l'équation $b = y_P^2 - x_P^3 - ax_P$ on obtient

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

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

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

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 annoncé.

□

4.4 Loi de groupe sur E

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

$$P + Q = f(f(P, Q), O). \tag{4.5}$$

Géométriquement, $P+Q$ s'obtient à partir de $f(P, Q)$ par symétrie par rapport à l'axe des abscisses. Cette loi de composition est une loi de groupe sur E.

Théorème 4.7. 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_{PQ}. 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

$$P + Q = \left(\lambda^2 - x_P - x_Q, -\lambda\left(\lambda^2 - x_P - x_Q\right) - \nu\right). \tag{4.6}$$

2) Si $x_P = x_Q$ et P, 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

$$2P = \left(\lambda^2 - 2x_P, \lambda\left(-\lambda^2 - 2x_P\right) - \nu\right). \tag{4.7}$$

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

5) L'opposé de P est le point

$$-P = (x_P, -y_P)\,. \tag{4.8}$$

Démonstration. 1) Supposons x_{PQ}, compte tenu de (4.5), (4.1) et (4.2) on a

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

On retrouve bien la formule (4.6).

2) Supposons $x_P = x_Q$ et $P \neq Q$ c'est à dire y_{PQ}.
D'après la proposition 4.6 (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

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

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 4.6 , 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 $M = (x_M, y_M) = (x_P, -y_P) = -P$.

□

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

Chapitre 5

Cryptosystèmes

5.0.1 Algorithme d'El Gamal

Alice souhaite envoyer un message chiffré à Bob. Pour se faire elle choisit un corps fini K, une courbe elliptique E définie sur K de sorte que le problème du logarithme discret soit difficile à résoudre dans le groupe $E(K)$. Elle choisit ensuite un point $P \in E(K)$. Enfin elle choisit sont entier naturel secret, non nul, s et calcul et calcul le point $A = sP$.

Elle rend ainsi public le quadruplet

$$(K, E, P, A).$$

C'est la base de ce qui va permettre à Alice et Bob de pouvoir communiquer de façon confidentiel entre eux.

Ainsi, pour que Bob puisse envoyer un message chiffré $M \in E(K)$ à Alice, il choisit secrétement un entier non nul k et calcules les points

$$M_1 = kP \quad \text{et} \quad M_2 = M + kA.$$

Il transmet alors publiquement à Alice le couple (M_1, M_2). C'est donc la phase d'encryptage du message M.

Pour qu'Alice puisse déchiffrer le message M, elle doit calculer le point

$$M_2 - sM_1.$$

Ce qui lui permet grâce au calcul suivant de retrouver M :

$$M_2 - sM_1 = M + kA - s(kP) = M + k(sP) - s(kP) = M + skP - skP = M.$$

5.0.2 Protocol Diffie-Hellman

Alice et Bob souhaite s'échanger publiquement une clé secrète commune. Pour cela ils se mettent d'accord pour la construire selon le procédé suivant :

1) Ils choisissent un corps fini K et une courbe elliptique E définie sur K, pour que le problème du logaritme discret soit difficile à résoudre dans le groupe $E(K)$. Ils choisissent un point $P \in E(K)$. Ils rendent alors publique le triplet (K, E, P).

2) Alice choisit un entier naturel secret non nun a et calcul le point $P_a = aP$, qu'elle transmet publiquement à Bob.

3) Bob procède de la même façon en choisissant un entier naturel secret, non nul, b, et il calcul de son côté le point $P_b = bP$, qu'il transmet publiquement à Alice.

4) Alice calcul le point $aP_b = a(bP)$.

5) Bob calcul le point $bP_a = b(aP)$.

Ils ont ainsi construit leur clé secret commun qui est le point abP.

Références

[Kra10] Alian Kraus. *Courbes elliptiques*. 2009/10. URL : https://www.math.univ-paris13.fr/~boyer/enseignement/crypto/Chap7.pdf.