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 22, 2022

Résumé

Table des matières

Chapitre 1

Introduction

Dans ce mémoire, je vais m'intéresser au groupe des points rationnels d'une courbe elliptique et donné des applications dans le domaine de la cryptographie.

L'application première de notre construction étant la cryptographie, il me semble nécessaire de poser d'en poser les bases. Ceci nous permettra d'avoir une idée clair 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 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 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 première exemple bien connu de cryptographie est appelé le chiffrement de César. Utilisé par Jules César pour chiffrer ses correspondances secrètes.

Cette méthode consiste à prendre les lettres de l'alphabet et d'effectuer une transposition $n \in \mathbb{N}$ ce dernier. 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. Cette méthode de chiffrement appelé chiffrement de Vigenère 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 Vigenère essaye de contourner le problème de l'analyse de fréquence d'apparition des lettres, qui permet de rendre inefficace les chiffrement monoalphabétique. 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 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'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 considérer 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.

Cette nouvelle méthode appelé protocole de Diffie-Hellman 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 $\mathbb{F}_p$, où p est premier. 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 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 appel ces 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 inverses est le plus difficiles possible.

La cryptographie d'aujourd'hui est basée sur une hypothèse mathématiques éprouvé et sur deux problèmes issu 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 ou très difficile à expliciter. Et de l'autre, on a le problème de la factorisation d'un entier et celui du logarithme discret.

C'est sur problème de la factorisation d'un entier, qu'est basé le système cryptographique RSA, inventé en 1977 par Rivest, Shamir et Adleman. Son efficacité repose sur le fait que connaissant un entier n, qui est produit de deux entier premiers p et q. Il est difficile de déterminer p et q. Cependant, les algorithmes de factorisation ayant énormément évolué, la taille des clé de chiffrement obtenue par RSA doivent être de plus en plus grande. Ainsi, pour des tailles de clé plus petite, disons 256-bit, le groupe des points rationnels offre une sécurité équivalente à des clé obtenue à l'aide du groupe $\mathbb{Z}/n\mathbb{Z}$ de taille 2048-bit. Ainsi, plus l'environnement est contraignant et plus l'avantage des courbes elliptique se fait ressentir.

L'efficacité du groupes des points rationnel d'une courbe elliptique est basé sur le problème du logarithme discret.

Le problème du logarithme discret est le suivant :

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

1.2 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 grec.

1.2.1 Origine des 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. Ce qui de nos jours, revient à étudié la courbe algébrique d'équation $x^2 + y^2 = 1$. Un problème qui a irrigué les commencement des mathématique est de déterminer la longueur d'un arc de cercle. Ceci revient à calculer l'intégrale

$$\int \frac{\mathrm{dx}}{\sqrt{1-x^2}}.$$

Ce qui nous permet d'obtenir la fonction $\arcsin(x)$ et par la méthode de Jacobi d'obtenir la fonction réciproque $\sin(x)$. Cette recherche de la réciproque de l'intégral obtenue à partir de l'équation d'un cercle, amène naturellement à la même question mais plus général sur les ellipses. Ainsi, en étudiant la courbe algébrique d'équation $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$, les mathématiciens du XVIIème et XVIIIème siècle on pu déterminer à l'aide d'une série convergente l'intégrale obtenue à partir de l'équation algébrique de l'ellipse. Toujours à cette époque, ils ont cherché à savoir si cette intégral pouvait être exprimé en termes de fonctions élémentaires. Liouville en 1837 prouva que cela n'est pas possible.

Ainsi, ils leur a fallu considérer cet intégral comme une fonction à part entière, cependant comme pour le cercle la fonction la plus naturelle est sa réciproque.

C'est ainsi qu'Abel en 1827 et indépendamment Jacobi en 1829 étudie la question de cette intégrale associé à une ellipse du point de vue des fonctions complexes, en considérant la réciproque.

Ce qui amène l'étude de l'intégrale elliptique de la forme

$$\int \frac{\mathrm{dx}}{\sqrt{4x^2-g_2-g_3}},$$

et l'introduction de la fonction elliptique ρ solution de l'équation

$$\rho'^2 = 4\rho^3 - g_2\rho - g_3,$$

où ρ est la réciproque de l'intégrale elliptique.

Ce qui en étudiant cette nouvelle équation est celle d'une courbe elliptique. Son étude dans le plan complexes permet la construction du groupe abélien des points rationnels d'une courbe elliptique.

Ainsi en 1985, indépendamment l'un de l'autre N.Koblitz **??** et V.Miller, on fournit un exemple d'application à la cryptographie, celui du groupes des points rationnels d'une courbe elliptique dans un corps fini. C'est ce groupes qui va nous intéresser.

1.2.2 Diophante

La seconde histoire est celle des équations diophantiennes. Ce parallèle permet d'introduire l'idée derrière la construction du groupe abélien des points rationnels d'une courbe elliptique.

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

Par exemple, une des équations diophantiennes la plus simple à résoudre est l'équation $ax+by=c$, avec les coefficients a, b, c des entiers relatifs et les indéterminées $x, y \in \mathbb{Z}$ 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 ci-dessus, ou des plus sophistiquées, comme celles étudiées par L.Mordell du type $y^2 = x^3 + ax + b$ qui va nous intéresser.

Les courbes elliptiques sont à la fois un problème facile à décrire, c'est "l'ensemble des solutions d'une cubique" et pourtant bien qu'elles semblent simple à première vue, de profond théorème régit leur comportement, et beaucoup de question naturel à propos des courbes elliptiques sont encore ouvertes.

Par exemple pour compter le nombre de sphère nécessaire pour formé une pyramide. On est amener à calculer la somme suivante

$$1 + 4 + 9 + 16 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6},$$

pour une pyramide de 4 étages ont à besoin de 30 sphère

$$1 + 4 + 9 + 16 = \frac{4(4+1)(2 \times 4 + 1)}{6} = 30.$$

Ainsi, si l'on étudie les solutions entières de l'équation suivante

$$y^2 = \frac{x(x+1)(2x+1)}{6},$$

cela revient à calculer les points rationnels de la courbe elliptique associée.

Mis à part, les points $(0, 0)$ et $(1, 1)$, quelles sont les autres solutions entière que l'on peut trouver l'idée et de partir de la droite qui intersectent les deux point à savoir $y = x$ et de résoudre le système d'équation que l'on obtient, c'est à dire

$$\begin{cases} y^2 & = \frac{x(x+1)(2x+1)}{6} \\ y & = x \end{cases}.$$

On obtient alors le polynôme

$$x^3 - \frac{3x^2}{2} + \frac{x}{2} = 0,$$

et l'on cherche alors sa troisième racines à l'aide des relations de Viète, on sait que la somme des racines vaut

$$r + 0 + 1 = \frac{3}{2}.$$

Ainsi, on obtient le point $\left(\frac{1}{2}, \frac{1}{2}\right)$ et par symétrie de la courbe par rapport à l'axe des abscisse le point $\left(\frac{1}{2}, -\frac{1}{2}\right)$. Bien que ce dernier ne soit pas une solution entière. On peut en répétant le même procéder en prenant les points $\left(\frac{1}{2}, -\frac{1}{2}\right)$ et $(1, 1)$. Cependant, l'intérêt de cet exemples n'est pas le calcul en lui même mais la méthode en elles-mêmes. J'entends par là, le fait de prendre deux points de la courbe et de tracer la droite entre ces deux. C'est cette action qui va nous intéresser et qui amène la question suivante.

Si l'on prend deux point d'une courbe elliptique, et que l'on trace la droite entre ces deux, cette droite intersecte elle toujours la courbe en un 3ème point ?

À première vue, la réponse à cet question est non. En effet, une tangente vertical à la courbe, c'est à dire parallèle à l'ordonnée n'intersecte pas la courbe elliptique. Cependant, à l'aide de la géométrie projective, on peut rendre cela possible. Ce qui rend possible la création du groupe des points rationnels d'une courbe elliptique.

Ce qui aujourd'hui, nous permet d'utiliser les courbes elliptiques pour construire des protocole de chiffrement robuste et largement répandue.

Le groupe des points rationnels d'une courbe elliptique est le fruit de la rencontre entre ces trois histoires que sont la cryptographie, le cercle et les équations diophantienne.

Références détaillées Une bibliographie complète est présente à la fin de ce mémoire. La liste détaillées des références principales pour chaque chapitre est la suivante :

— *Chapitre 1 :*
— *Chapitre 2 :*
— *Chapitre 3 :*
— *Chapitre 4 :*
— *Chapitre 5 :*

Merci à Mme Abdelatif pour avoir supervisé ce mémoire.

Chapitre 2

Géométrie projective

Dans ce chapitre, je défini et donne quelques propositions qui m'ont permis de mieux comprendre l'intéret de l'étude des courbes elliptiques dans le plan projectif. Ainsi que d'introduire les propositions qui me permettent de faire le parallèle entre la partie algébrique du raisonnement et l'interprétation géométrique associé. Notamment, j'introduis une proposition qui me permet de donner une la démonstration géométrique de l'associativité de la loi du groupe des points rationnels d'une courbe elliptique.

2.1 Le plan projectif et les courbes sur le plan projectif

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 le plan, 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 (i.e. les droites de l'espace). L'idée nous vient de la formalisation mathématique de la perspective.

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 et (x, y, z) sont appelées les 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 polynôme $F(X, Y, Z)$ dans l'anneau de polynômes $K[X, Y, Z]$ tels que si $F(x, y, z) = 0$ alors $F(\lambda x, \lambda y, \lambda z) = 0$ pour tout λ non nul.

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

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X, Y, Z). \tag{2.1}$$

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 E sur le plan projectif $\mathbb{P}_2$ est l'ensemble des solutions d'une équation polynomiale

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

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

$$E = \{(x, y, z) \in \mathbb{P}_2 \mid F(X, Y, Z) = 0\}.$$

Un point $P = [x, y, z] \in E$, s'il vérifie que $F(x, y, z) = 0$ ne dépend que de sa classe d'équivalence. En effet si on choisit un autre représentant de classe de ce point dans le plan projectif $\mathbb{P}_2$, par exemple pour $P' = \lambda P$, on a

$$F(P') = F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x, y, z) = 0.$$

Tous les représentant de classe d'un point de la courbe sont des zéro du polynôme F donc un point de la courbe.

Définition 2.4. Une courbe $D \in \mathbb{P}_2$ définie par un polynôme homogène de degré 1 est appelée une droite.

Une courbe $E \in \mathbb{P}_2$ définie par un polynôme homogène de degré 3 est appelée une cubique.

2.2 Lien avec la représentation affine

On peut faire le lien entre une courbe du plan projectif telle qu'on vient de la définir et une courbe du plan affine habituel, que l'on note $\mathbb{A}_2$ ou $\mathbb{A}_2(\overline{K})$.

Soit une courbe E de $\mathbb{P}_2(\overline{K})$, donnée par un polynôme homogène F de degré d tel que

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

Posons

$$U = \left\{[x, y, z] \in \mathbb{P}_2(\overline{K}) \mid z \neq 0\right\}.$$

On dispose de l'application $\varphi : U \to \mathbb{A}_2(\overline{K})$ 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

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

En effet, si $P = (x, y) \in \mathbb{A}_2$, on a

$$\varphi \circ \varphi^{-1}(x, y) = \varphi([x, y, 1]) = (x, y) \in \mathbb{A}_2,$$

et si $P = [x, y, z] \in U$ alors

$$\varphi^{-1} \circ \varphi([x, y, z]) = \varphi^{-1}(\frac{x}{z}, \frac{y}{z}) = [\frac{x}{z}, \frac{y}{z}, 1] = [x, y, z] \in U.$$

La bijection φ fait correspondre ce point du plan projectif avec un point $\varphi(P) = (\frac{x}{z}, \frac{y}{z})$ du plan affine K.

Il y a donc une correspondance entre les points du plan projectif et ceux du plan affine. On peut également remarquer comme il a été dit plutôt que deux représentants de classes distincts d'un même point P dans $\mathbb{P}_2$ donne lieu à un unique point dans $\mathbb{A}_2$.

Par ailleurs, si on a F un polynôme homogène de degré d et que $F(x, y, z) = 0$ alors

$$F(\frac{x}{z}, \frac{y}{z}, 1) = \lambda^d F(x, y, z) = 0,$$

avec $\lambda = \frac{1}{z}$.

On peut alors définir une courbe dans le plan affine $\mathbb{A}_2$ à partir d'une courbe dans le plan projectif $\mathbb{P}_2$, dont les points (x, y) seront solution de l'équation $f(x, y) = 0$, avec f définie par

$$f(x, y) = F(x, y, 1). \tag{2.2}$$

Autrement dit, si on identifie la partie affine à l'ensemble U, le plan projectif s'interprète comme la réunion de $\overline{K}^2$ avec la droite à l'infini. On note $\mathbb{P}_1 = \{(x, y, 0) \in \mathbb{P}_2 \mid F(x, y, 0) = 0\}$ l'ensemble des points à l'infini, on parle souvent de droite à l'infini quand on parle de $\mathbb{P}_1$.

Dans ce cas, on a :

$$\mathbb{P}_2 \approx U \cup \mathbb{P}_1.$$

Remarque. En ce qui concerne les courbes elliptique nous verrons que seul un point de la courbe appartient à $\mathbb{P}_1$.

2.3 Courbes irréductibles

Définition 2.5. Un polynôme P est factorisable lorsqu'il existe deux polynômes Q et R non constants de degré strictement inférieur à celui de P tels que

$$P(X, Y, Z) = Q(X, Y, Z)R(X, Y, Z).$$

Un polynôme est irréductible lorsqu'il n'est pas factorisable.

On peut factorisé un polynôme en un produit de polynômes irréductibles.

Si $F \in K[X, Y, Z]$ est un polynôme, il existe $P_1, \ldots, P_n \in K[X, Y, Z]$ des polynômes tous irréductible tels que

$$F(X, Y, Z) = P_1(X, Y, Z) \ldots P_n(X, Y, Z).$$

Les P_i sont appelées les composantes irréductibles du polymôme F.

Définition 2.6. Soit une courbe E définie par le polynôme $F(X, Y, Z) = 0$. La courbe est irréductible si le polynôme F est irréductible.

On dit que deux courbes E_1 et E_2 n'ont pas de composante commune quand leur composantes irréductibles sont distinctes.

2.4 Intersection d'une cubique et d'une droite dans le plan projectif

Proposition 2.7. L'ensemble des points à l'intersection d'une cubique E et d'une droite D est fini si, et seulement si, ces deux courbes n'ont pas de composante irréductible en commun.

Autrement dit, cela revient à montrer l'ensemble $E \cap D$ est fini, si et seulement si, les polynômes associés à E et D sont irréductibles.

Démonstration.
— Dans un premier temps, on montre que si E et D ont une composante commune alors $E \cap D$ est infini. Autrement dit, comme ils ont une composante commune, cela revient à dire que l'un est produit de l'autre. Ce qui nous permettra de conclure par contraposée.
Soient E l'ensemble des solutions de $F_1(X, Y, Z) = 0$ et D l'ensemble des solutions de $F_2(X, Y, Z) = 0$.
On a le degré de F_1 qui vaut trois et comme D est une droite, F_2 est un polynôme homogène de degré 1, il est donc irréductible.
Dire que E et D ont une composante irréductible commune, revient à dire qu'il existe une courbe C d'équation $F_3(X, Y, Z) = 0$ de degré $0 < d < 3$.
Ainsi, on peut écrire F_1 sous la forme

$$F_1(X, Y, Z) = F_2(X, Y, Z)F_3(X, Y, Z),$$

comme $F_1(X, Y, Z) = 0$, il vient

$$\begin{aligned} F_2(X,Y,Z)F_3(X,Y,Z) = 0 &\Leftrightarrow (F_2(X,Y,Z) = 0) \vee (F_3(X,Y,Z) = 0) \\ &\Leftrightarrow \exists P \in \mathbb{P}_2,\ P \in D \cup C = E. \end{aligned}$$

Donc D est contenu dans E. Comme il existe une infinité de droite, il existe une infinité de point intersection de la courbe et de la droite.

Ainsi, on a montré que si la courbe E et la droite D ont une composante irréductible commune alors il existe une infinité de points dans l'ensemble $D \cup C = E$, et comme $E \cap D = D$, par conséquent l'ensemble est infini.

Autrement dit, par contraposée, si E et D se coupent en un nombre fini de points, elles n'ont pas de composante commune.

— Dans un second temps, supposons que E et D n'ont pas de composante commune, ce qui revient à dire que les polynômes F_1 et F_2 sont irréductibes. Donc à montrer que F_1 est irréductible ce qui permettra de conclure grâce au nombre fini de racine de F_1.

La droite D est défini par un polynôme homogène de degré 1

$$D : F_2(X, Y, Z) = aX + bY + cZ.$$

Soit $P = [x, y, z]$ un point de l'intersection entre E et D.

— Si $z \neq 0$,

Les coordonnées affines du point P vérifient alors l'équation

$$f_2(x, y) = ax + by + c = 0.$$

On peut supposer, par symétrie, que $b \neq 0$. Dans ce cas, on a

$$y = -\frac{ax + c}{b}.$$

L'équation suivante doit alors être vérifié

$$f_1(x, -\frac{ax + c}{b}) = 0.$$

C'est un polynôme en x non nul car E et D n'ont pas de composante commune. Il admet donc un nombre fini de racines.

— Si $z = 0$ alors,

les coordonnées homogène de P vérifient alors le système d'équation suivante

$$\begin{cases} AX + bY &= 0 \\ F_1(X, Y, 0) &= 0 \end{cases}.$$

En supposant par symétrie, que $b \neq 0$, on voit que les coordonnées homogènes de P doivent vérifier

$$F_1(X, -\frac{a}{b}X, 0) = 0.$$

Cette équation est un polynôme en X non nul puisque E et D n'ont pas de composante commune. il admet donc un nombre fini de racines.

Ainsi, si E et D n'ont pas de composante commune. elles se coupent en un nombre fini de points.

□

Corollaire 2.8. Soit E une cubique irréductible et D une droite. La courbe plane E et la droite projective D se coupent en un nombre fini de points.

Démonstration. En effet, comme E est irréductible, son polynôme homogène associé $F(X,Y,Z) = 0$ est lui aussi irréductible et donc il ne possède pas de composante irréductible. D'où l'énoncé. □

Chapitre 3

Définitions générales sur les courbes elliptiques

Dans ce chapitre, on donne d'abord la définition générale d'une courbe elliptique. On fais le lien entre cette définition et la définition qui utilise une forme simplifié de l'équation général. On propose également un lemme qui permet de caractériser simplement les courbes non-lisses. Finalement, on donne la définition d'un points rationnels d'une courbe elliptique.

3.1 Définition générale

La définition générale d'une courbe elliptique est la suivante

Définition 3.1. Soient K un corps, $\overline{K}$ sa cloture algébrique, et K^* son groupe multiplicatif. Une courbe elliptique sur K est une cubique, non singulière, définie comme l'ensemble des solutions du plan projectif $\mathbb{P}_2(\overline{K})$ de l'équation de Weierstrass homogène suivante :

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{3.1}$$

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 veut dire 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

$$F(x_0, y_0, z_0) = \frac{\partial F}{\partial x}(x_0, y_0, z_0) = \frac{\partial F}{\partial y}(x_0, y_0, z_0) = \frac{\partial F}{\partial z}(x_0, y_0, z_0) = 0.$$

Dans une courbe elliptique la droite à l'infini ne contient qu'un seul élément, on le nomme point à l'infini et on le note $\mathcal{O} = [0, 1, 0]$.

Par la suite nous utiliserons la plupart du temps la représentation affine de l'équation de Weierstrass :

$$E : y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6. \tag{3.2}$$

avec les $a_i \in K$.

Pour $Z \neq 0$, un point $[x, y, z] \in \mathbb{P}_2$ solution de l'équation (3.1) correspond à un point $(x, y) \in \overline{K}^2$ solution de l'équation (3.2) avec $(x, y) = (\frac{X}{Z}, \frac{Y}{Z})$.

L'ensemble des solutions de l'équation (3.1) correspond à l'union entre les solutions de l'équation (3.2) et du point $\mathcal{O}$.

Ce qui revient à écrire que

$$\begin{aligned} E &= \Big\{(X, Y, Z) \in \overline{K}^2 \times \overline{K}^* \mid F(X, Y, Z) = 0\Big\} \cup \mathcal{O} \\ &= \Big\{(x, y) \in \overline{K}^2 \mid f(x, y) = 0\Big\} \cup \mathcal{O}. \end{aligned}$$

On peut, par un double changement linéaire de variable, obtenir l'équation courte de Weierstrass pour des corps de caractéristique différents de 2 et 3.

En effet, l'idée est d'effectuer un changement pour la variable y qui nous permet d'obtenir un polynôme de la forme

$$E' : \quad Y^2 = X^3 + k_1X^2 + k_2X + k_3,$$

où les k_i sont des constantes divisés par un multiples de deux.

Ensuite, en effectuant un changement de variable pour x, on se ramène au polynôme qui nous intéresse à savoir

$$E'' : \quad Y^2 = X^3 + k_1X + k_2. \tag{3.3}$$

où les k_i cette fois-ci sont divisés par des multiples de 2 et 3.

On peut ainsi, démontrer que K étant de caractéristique distincte de 2 et 3, une courbe lisse d'équation (3.1) est "isomorphe sur K" à une courbe de la forme (3.3) pour laquelle le discriminant du polynôme homogène associé soit non nul. La définition que l'on va utiliser n'est donc pas restrictive.

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 commutatif suivant $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{F}_q$.

On va plutôt se servir de la définition suivante qui est celle qui nous intéresse en vue de construire le groupe des courbes elliptiques appliqué à la cryptographie.

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

$$y^2z = x^3 + axz^3 + bz^2. \tag{3.4}$$

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

$$4a^3 + 27b^2 \neq 0. \tag{3.5}$$

Remarque. On dit que la courbe elliptique d'équation 3.4 est définie sur K pour préciser que a et b sont dans K. Ceci pour a et b vérifiant la condition (3.5)

On a donc le polynôme $F(X, Y, Z)$ dans l'anneau de polynôme $K[X, Y, Z]$ associé à la courbe et E est défini par l'ensemble des solutions de l'équation

$$E: \quad F(X, Y, Z) = Y^2Z - X^3 + aXZ^3 + bZ^2 = 0.$$

Remarque.

1. Les points du plan projectif qui satisfont cette équation sont appelé l'ensemble des zéros de F dans $\overline{K}$, ou plus simplement zéro de F. Cet ensemble est ce que l'on entend par courbe projective plane d'équation (3.4).
2. Si $\Delta < 0$, alors il admet une racine réel et deux racines complexes et on obtient des courbe de la forme suivante

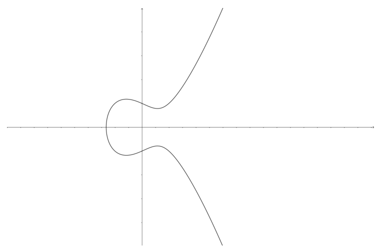

FIGURE 3.1 – Courbe elliptique d'équation $y^2 = x^3 - x + 1$

3. Si $\Delta > 0$, on a trois racines réels distinctes et donc des courbes elliptique de la forme suivante

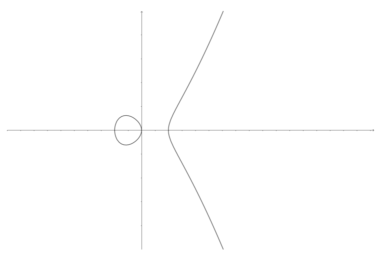

FIGURE 3.2 – Courbe elliptique d'équation $y^2 = x^3 - x$.

4. Si $\Delta = 0$ alors la courbe n'est pas elliptique et on obtient un point singulier.

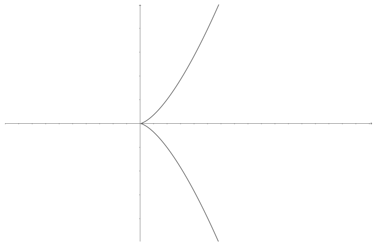

FIGURE 3.3 – Courbe elliptique d'équation $y^2 = x^3$.

Comme on vient de le voir, il est possible de se ramener à l'étude des solution de l'équation polynômial $f(x, y) = 0$ dans le plan affine. Ainsi la condition (3.5) signifie que les racines dans $\overline{K}$ du polynôme

$$f(x, y) = y^2 - x^3 + ax + b,$$

sont simples et le lemme suivant nous fourni un critère simple pour obtenir une courbe lisse. Ce qui nous permet d'éviter les courbes avec un point de multiplicité double qui nous fait perdre l'unicité de la tangente.

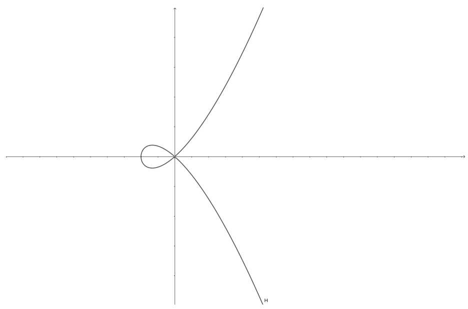

FIGURE 3.4 – Courbes d'équation $y^2 = x^3 + x^2$ admettant un point double.

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 démontrer ce lemme, on utilise la proposition que nous admettrons, qui est la suivante :

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

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

C'est un élément de K.

Démonstration (Lemme)**.** 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.

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'aprés 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 :

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

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 :

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

On peut écrire

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

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

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 :

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

Montrons maitenant 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 :

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

D'où le résultat. $\square$

3.2 Points rationnels d'une courbe elliptique

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

D'aprés la définition ci-dessus, 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 $\frac{x_j}{x_i}$ 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 (3.4).

Définition 3.6. Un point de E est dit rationnel sur L, ou encore L-rationnel, 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

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

Remarque.
1. Lorsque le contexte est clair on parlera de point rationnel de la courbe pour parler des points L-rationnels.
2. Le point $\mathcal{O}$ est défini sur K et par définition sur toute extension de K. Ainsi, si L/K est une extension du corps K, E peut-être considérée comme une courbe elliptique définie sur K et $\mathcal{O}$ est encore le point à l'infini de E/L.
   On a,
   $$E(L) = \left\{ (x, y) \in L^2 \mid y^2 = x^3 + ax + b \right\} \cup \mathbb{O}.$$
   De même,
   $$E(\overline{K}) = \left\{ (x, y) \in \overline{K}^2 \mid y^2 = x^3 + ax + b \right\} \cup \mathbb{O}.$$
   Ce qui revient à dire que, si $K \subset L \subset \overline{K}$ alors $E(K) \subset E(L) \subset E(\overline{K})$.

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

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

Cette courbe vérifie bien la condition (3.5).

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

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

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

exemple klaus F25

$\diamond$

Chapitre 4

Loi de groupe

Dans ce chapitre, on présente le point de vue géométrique de la construction de la loi de groupe, et en parallèle on introduit algébriquement les différents outils nécessaire à l'élaboration de la loi de groupe. On commence par montrer qu'il y exactement trois point d'intersection entre une droite et la courbe. Puis, nous montrerons l'existence et l'unicité de la droite qui intersecte deux points de la courbe, ainsi que de la tangente en un point de la courbe. Muni de ses deux outils nous nous consacreront à la construction de la loi des cordes-tangentes. Ce qui nous permettra de conclure avec le théorème qui régit la loi du groupe des points rationnels d'une courbe elliptique.

4.1 Point de vue géométrique

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

Démonstration. En effet, comme E est irréductible, nous savons grâce à la proposition 2.7 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 $R = (x_R, y_R, -\frac{ax_R+by_Q}{c})$ est alors le troisième point de l'intersection entre E et D. $\square$

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

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.

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 $\overline{K}$.

On parle alors de la droite d'équation $ux + vy + wz = 0$. Une droite d'équation $x = \lambda z$, où λ est dans $\overline{K}$, est dite verticale. Une telle droite passe par le point $O = [0, 1, 0]$. En fait, toute droite passant par O a une équation de la forme $ux + wz = 0$.

Lemme 4.3. Soient $P = [a_1, a_2, a_3]$ et $Q = [b_1, b_2, b_3]$ deux points distinct 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

$$u = a_2 b_3 - a_3 b_2, \; v = a_3 b_1 - a_1 b_3, \; w = a_1 b_2 - a_2 b_2.$$

Démonstration. 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. L'équation $ux + vy + wz = 0$ est donc celle d'une droite qui par définition contient P et Q.

Montrons que cette droite est unique.

Soit une droite de $\mathbb{P}_2$ passant par P et Q d'équation

$$u'x + v'y + w'z = 0.$$

Soient f et g les formes linéaires $\overline{K}^3 \to \overline{K}$ définies par

$$f(x, y, z) = ux + vy + wz \quad \text{et} \quad g(x, y, z) = u'x + v'y + w'z.$$

Le noyau de f et g est le plan de $\overline{K}^3$ engendré par (a_1, a_2, a_3) et (b_1, b_2, b_3). En particulier, f et g ont le même noyau. Dans le dual de $\overline{K}^3$, l'orthogonal du noyau de f (resp. g) est la droite engendrée par f (resp g). Il existe $\lambda \in \overline{K}$ non nul tel que $f = \lambda g$, d'où l'unicité. $\square$

4.3 Tangente à E en un point

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

Soit

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

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,

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

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 $\mathrm{car}(K) \neq 2$, 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 E est elliptique. D'après le lemme 3.3

— Supposons que $a = 0$, alors

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

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

□

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

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

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

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

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,

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

D'où le résultat.

□

4.4 Loi de composition des cordes-tangentes

La proposition 4.1 nous permet de définir la loi de composition des cordes-tangentes qui satisfait :

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 4.1 on sait que cette corde prolongé à une droite intersecte 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 4.1 nous garantie l'existence d'un troisième point unique en comptant les multiplicités qui appartient à $E \cap D$. On notera ce dernier $f(P, P)$.

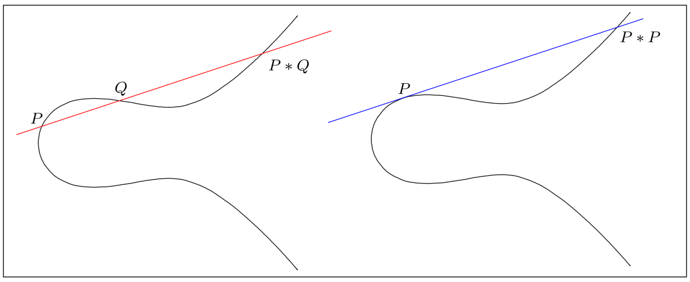

FIGURE 4.1 – Illustration de la loi des cordes-tangentes

On peut remarquer que sur la Figure 4.1, une droite verticale àla courbe E ne semble pas la couper en un troisième point. Ceci est lié à la difficulté de représenter le plan projectif $\mathbb{P}_2$ sur un plan. Ce troisième point existe, et appartient à la droite infini $\mathbb{P}_1$. Pour une courbe elliptique il correspond au $\mathcal{O}$.

Remarque. Le meilleur moyen de considérer $\mathbb{P}_1$ est de se représenter ses éléments comme l'ensemble des directions possibles des droites du plan affine. Dans le cas particulier des courbes elliptiques, on a vu que P_1 se limite à un seul élément, que l'on a noté $\mathcal{O}$, qui correspond à la direction des droites verticales.

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

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

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 trouver ses coordonnées.

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 4.3 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

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

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

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

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 4.3 , 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

$$\begin{aligned}2y_Px-2y_Px_Pz &= 0\\ x &= x_Pz.\end{aligned}$$

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

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

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

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

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

□

On obtient alors une loi de composition interne sur E, appelée loi de composition des cordes-tangentes, $f : E \times E \to E$ 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 4.1

Exemple. ◇

4.5 Loi de groupe

Théorème 4.9. Soit un corps K. Soit E une courbe elliptique définie sur K. Soient P et Q deux points de cette courbe. Alors,

$$P + Q = f(f(P, Q), \mathcal{O}),$$

définit une structure de groupe commutatif ayant $\mathcal{O}$ pour élément neutre de la loi.

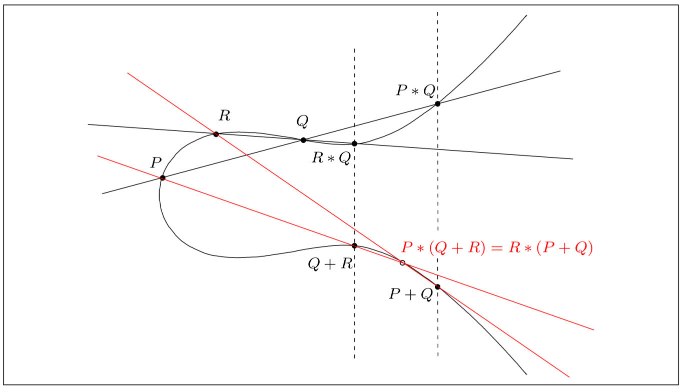

FIGURE 4.2 – Illustration de l'associativité de la loi de groupe

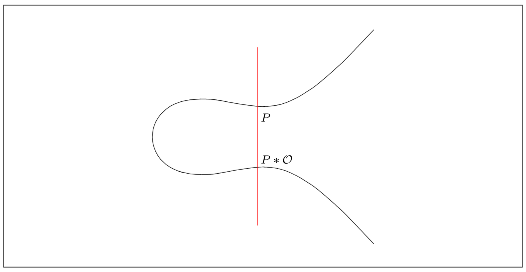

FIGURE 4.3 – L'élément neutre de la loi de groupe

Démonstration.

1. La loi $+$ est bien interne puisque $P+Q$ est l'intersection entre la courbe et une droite, c'est à dire un point de la courbe.
2. La loi $+$ est associative (voir Figure 4.2). En effet, si P, Q et R sont trois point de la courbe, on a

$$\begin{aligned} f(P, f(Q+R)) &= f(P, f(f(Q,R), \mathcal{O})) \\ &= f(f(f(P,Q),Q), f(f(Q,R),\mathcal{O})) \text{ car } P = f(f(P,Q),Q) \\ &= f(f(f(P,Q),\mathcal{O}), f(f(Q,R),Q)) \text{ voir la proposition 4.7} \\ &= f(f(f(P,Q),\mathcal{O}), R) \text{ voir la Figure 4.2} \\ &= f(f(P+Q), R). \end{aligned}$$

En appliquant $\mathcal{O}$ sur les deux membres de l'égalité, on trouve

$$P + (Q + R) = (P + Q) + R.$$

3. L'élément $\mathcal{O}$ est l'élément neutre de la loi additive (voir Figure 4.3).
   En effet,

$$P + \mathcal{O} = f(f(P, O)O) = P \quad \text{et} \quad \mathcal{O} + P = f(f(\mathcal{O}, P), \mathcal{O}) = P.$$

4. Tout point P possède un inverse pour la loi $+$. En effet, il faut vérifier que le point $-P = f(f(\mathcal{O}, \mathcal{O}), P)$ est bien l'inverse de P

$$\begin{aligned} P + (-P) &= f(f(P, -P), \mathcal{O}) \\ &= f(f(f(P, f(f(\mathcal{O}, \mathcal{O}), P), \mathcal{O}))) = f(f(\mathcal{O}, \mathcal{O}), \mathcal{O}) = \mathcal{O} + \mathcal{O} = \mathcal{O} \\ (-P) + P &= f(f(-P, P), \mathcal{O}) \\ &= f(f(f(f(\mathcal{O}, \mathcal{O}), P), P), \mathcal{O}) = f(\mathcal{O}, f(\mathcal{O}, \mathcal{O})) + \mathcal{O} + \mathcal{O} = \mathcal{O} \end{aligned}$$

.

5. Enfin la loi $+$ est commutative. C'est à dire que si P et Q sont deux points de la courbe, on a

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

□

Les propiétés de la loi de groupe sur une courbe elliptique sont représentées sur la Figure 4.4.

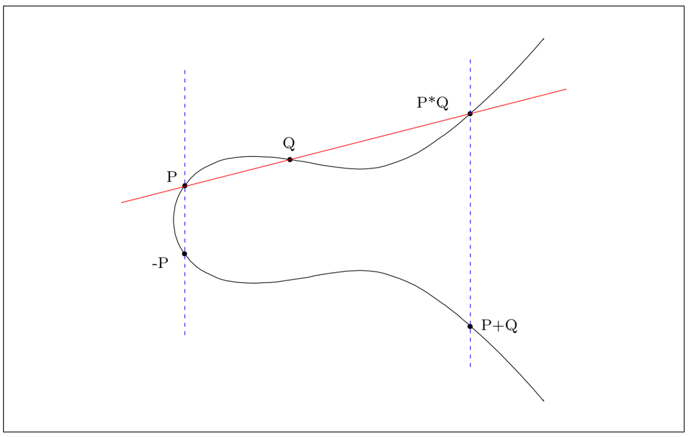

FIGURE 4.4 – La loi de groupe $+$ sur l'ensemble des points rationnels d'une courbe elliptique

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

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

Théorème 4.10. 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 $y_P \neq y_Q$.
D'après la proposition 4.1 (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 4.1 , 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

Applications

Le groupe abélien $(E, +)$ des points rationnels d'une 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.

5.1 Cryptosystèmes elliptiques

Aujourd'hui, le groupe E des points rationnels d'une courbe elliptique intervient notamment pour l'échange de clé et les signatures numériques.

Nous allons, nous intéressé à deux cryptosystème asymétrique, à savoir le protocol d'échange de clés Diffie-Hellman, ainsi que l'algorithme d'El-Gamal, basé sur le principe du protocol de Diffie-Hellman, qui permet d'échanger des messages messages chiffré à l'aide d'une clé publique et de déchiffrer les messages avec la clé secrète de chaque utilisateur.

La force des cryptosytèmes asymétrique réside dans la difficulté, voir l'impossibilité actuel dans le cas elliptique, de résoudre le problème du logarithme discret que nous énoncerons par la suite.

Dans le cas des cryptosystèmes à clé publique classique, on s'appuie sur le groupe multiplicatif d'un corps fini et de son groupe des inversibles. Ce qui réduit grandement notre choix comparé aux versions elliptique des algorithmes équivalent.

En effet, dans le cas elliptique, on remplace le groupe multiplicatif sur un corps fini par le groupe des points rationnels d'une courbe elliptique. L'avantage de cette méthode est que pour un corps fini K donné, on dispose généralement de nombreux choix de courbes elliptiques E sur K. Autrement dit, on a de nombreux groupes $E(K)$, pour utiliser efficacement un cryptosystème asymétrique élliptique contrairement aux versions classique comme énoncé plus haut où l'on ne dispose que du groupe des inversible K^*.

Dans ce qui suit Alice et Bob sont deux personnes qui souhaite s'échanger soit un message, soit une clef secrète. Cependant, il faut bien comprendre qu'il peuvent également représenter deux entité qui souhaitent communiqué via des messages chiffrés ou bien s'échanger une clef secréte via cannaux publique. Par entité, j'entends soit des banques, des entreprises ou tout ce qui serait suceptible de vouloir communiqué secretement entre eux.

De plus le choix des clés secret s'effectue de façon aléatoire dans le respect des conditions de chaque cas.

5.1.1 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.

Problème (Diffie-Hellman)**.**

5.1.2 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 :

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

Perspectives

Qu'est ce qui peut être intéressant d'étudier à la suite de ce que l'on a vu