REPUBLIQUE ALGERIENNE
DEMOCRATIQUE ET POPULAIRE
MINISTERE DE LŠENSEIGNEMENT
SUPERIEUR ET DE LA RECHERCHE
SCIENTIFIQUE

Université Mohamed Boudiaf de M'sila
Faculté des Mathématiques et de l'Informatique
Département des Mathématiques

Mémoire de Master

Domaine : Mathématiques et Informatique
Filière : Mathématiques
Option : Algèbre et Mathématiques Discrètes

Thème

Le nombre de points sur une courbe elliptique

Présentée par :
Noussieba Sekkai

Devant le jury composé de :

MIHOUBI Douadi	Prof	Université de M'sila	**Président**
GHADBANE Nacer	MCA	Université deM'sila	**Encadreur**
HEBOUB Lakhder	MAA	Université de M'sila	**Examinateur**

Année universitaire 2019/2020

Table des matières

Résumé

Ce mémoire s'inscrit dans le cadre de la théorie des courbes elliptiques.

Au premier chapitre, on rappelle des notions élémentaires sur les groupes, les anneaux et les corps finis.

À la suit, on étude Les courbes elliptiques définies sur $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$.

En fin, on s'intéresse au cardinal de points rationnels sur un corps fini.

Mots clés : Groupe, morphisme de groupe, corps fini, courbe elliptique, point rationnel.

Abstract

This memory is part of the theory of elliptic curves.

In the first chapter, we recall elementary notions on groups, rings and finite fields.

Next, we study the elliptical curves defined on $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

Finally, we are interested in the cardinality of rational points on a finite field.

Keywords : Group, group morphism, finite field, elliptic curve, rational point.

Introduction

Une courbe elliptique est un cas particulier de courbe algébrique, munie entre autres propriétés d'une addition géométrique sur ses points. Les courbes elliptiques ont de nombreuses applications dans des domaines très différents des mathématiques : en théorie des nombres dans la démonstration du dernier théorème de Fermat, en cryptologie dans le problème de la factorisation des entiers.

Les courbes elliptiques sont un sujet très à la mode ; Tout a commencé lorsque Lenstra a découvert un alghorithme de factorisation polynomial sur ces structures. Ensuite, en 1985, Koblitz et Miller ont proposé indépendamment d'adapter les protocoles de la cryptographie basés sur les courbe elliptiques.

Dans ce mémoire, nous allons étudier le cardinal de points rationnels de courbe elliptique définie sur un corps fini.

Ce travail et composé de trois chapitres :

Le premier chapitre, consiste à un rappel des notions élémentaires sur les groupes et les corps finis.

Dans le second chapitre, nous allons étudier les courbes elliptiques définies sur $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$, ainsi que certaines propriétés.

Dans le troisième chapitre, on fait une étude sur les points rationnels de courbe elliptique définie sur un corps fini.

Chapitre 1

Notions élémentaires sur les corps finis

1.1 Groupe

Definition 1 Un groupe est un couple formé d'un ensemble G et d'une loi de composition $(x, y) \mapsto xy$ sur l'ensemble G. Ces données doivent verifier les trois conditions :
(i) $\forall x, y, z \in G : (xy)\, z = x\,(yz)$ (l'associativité) ;
(ii) $\exists 1 \in G$ tel que $\forall x \in G : x1 = 1x = x$ (l'existence d'un élément neutre) ;
(iii) $\forall\ x \in G, \exists\ x^{-1} \in G$ tel que $x^{-1}x = xx^{-1} = 1$ (l'existence d'un élément inverse pour tout élément du groupe).
Si la loi de groupe et commutatif, nous utilisons l'écriture additive au lieu de l'ecriture multiplicative i.e la loi de composition est $(x, y) \mapsto x + y$.
Dans cette notation, l'élément neutre est habituellement noté 0 et l'inverse d'un élément x est noté $-x$.

Exemple 1.1 L'ensemble des entiers muni de l'addition usuelle noté $(\mathbb{Z}, +)$ forme un groupe commutatif.

Exemple 1.2 L'ensemble des réeles non nuls muni de la multiplication usuelle noté $(\mathbb{R}^*, \times)$ forme un groupe commutatif.

Exemple 1.3 Pour chaque ensemble X, on peut construire le groupe $Sym\,(X)$ de permutations de cet ensemble, appelé le groupe symétrique de l'ensemble X. Ce

groupe consiste en toutes les bijections de X dans X, et est muni de la composition naturelle.

1.1.1 Les sous groupes

Definition 2 Etant donné un groupe $(G, \cdot)$, un sous- groupe de G est un sous-ensemble $H \subset G$ tel que H, muni de la restriction de " $\cdot$ " sur H est un groupe. On note $H \leq G$.

Proposition 1.1 *Un ensemble $H \subseteq G$ est un sous-groupe de G si il vérifier les conditions suivantes :*
(i) H est non vide ;
(ii) H est un sous-enssemble stable de $(G, .)$;
(iii) $x^{-1} \in H$ pour tout $x \in H$.

Exemple 1.4 On a les chaines de sous- groupes suivantes :
$(n\mathbb{Z}, +) \leq (\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.
$(\mathbb{Q}^*, \times) \leq (\mathbb{R}^*, \times) \leq (\mathbb{C}, \times)$.
Si $(G, *)$ est un groupe, alors $(\{e_G\}, *)$ et $(G, *)$ sont 2 sous-groupes de $(G, *)$.
$(C^0(\mathbb{R}, \mathbb{R}), +)$ est un sous groupe de $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +)$.

Definition 3 Soit $(G, \cdot)$ un groupe et H un sous-groupe de G. Pour un élément $g \in G$, On dit que la classe latérale gauche de g selon H est l'ensemble $gH = \{gh : h \in H\}$. De la même façon, la classe latérale droite de g selon H est l'enssemble $Hg = \{hg : h \in H\}$. Un sous-groupe normal de G est un sous-groupe N tel que les classes latérales à gauches sont égales aux classses latérales droites -c'est-à-dire, $\forall g \in G, gN = Ng$. On dénote le fait que N est normal par $N \lhd G$.

Exemple 1.5 Soit $(G, \cdot, e)$ un groupe. Alors $\{e\}$ et G sont des sous-groupes de G, et sont même des sous-groupes normaux. On les appelle les sous-groupes triviaux. Tous les autres sous-groupes (s' ils existent) sont appellés sous-groupes propres de G. Soit G un groupe et $g \in G$.
Le centralisateur de g est l'ensenble $C_G(g) = \{x \in G \mid xg = gx\}$.

Le centre de G est l'ensemble $Z(G) = \{x \in G \mid xg = gx \text{ pour } g \in G\} = \cap_{g \in G} C_G(g)$. Alors, $C_G(g)$ et $Z(G)$ sont des sous-groupes de G. En outre, $Z(G)$ est un sous-groupe normal.
Dans un groupe commutatif, chaque sous-groupe est un sous-groupe normale.

Th■or■me 1.1 *(Lagrange) L'ordre $|H|$ d'un sous-groupe H d'un groupe fini G divise l'ordre $|G|$ de G. L'indice $[G : H]$ divise aussi $|G|$ et*
$[G : H] = |G| / |H|$.

Preuve. G est clairement la réunion disjointes des xH. D'où $|G| = \sum |xH|$. De plus $|xH| = |H|$, pour tout $x \in G$, d'où $|xH| = |yH|$, pour tous $x, y \in G$ et la somme ci-dessus est égale au nombre de classes fois $|H|$, ce qui est précisément la formule cherchée. ■

1.1.2 Groupe abeliens de type fini et les groupes cycliques

L'intérêt des groupes cycliques est qu'ils apparaissent souvent, par exemple comme le groupe additif d'un corps fini. Il nous permettent aussi des corps fini, qu'on va étuder plus tard.

Proposition 1.2 *Soient G un groupe et $A \subseteq G$ une partie de G. Il existe un plus petit sous-groupe H de G contenant A. On dit que H est le sous-groupe engendré par A, ou que les éléments de A sont des générateurs de H. On note $H = \langle A \rangle$.*

Preuve. L'existence de H peut se voir de deux manières :
a) On considère tous les sous-groupes de G contenant A (il ya au moins G tout entier) et leur intersection convient ;
b) On suppose A non vide (sinon on a $H = \{1\}$), on pose $A^{-1} = \{x \in G : x^{-1} \in A\}$, puis $H = \{a_1 ... a_n, n \in \mathbb{N}, a_i \in A \cup A^{-1}\}$. Alors H est un sous-groupe, contient A et est évidemment le plus petit possible. ■

Definition 4 Un groupe G engendré par un élément a, est dit monogène. Il est isomorphe à $(\mathbb{Z}, +)$ ou $(\mathbb{Z}/n\mathbb{Z}, +)$, pour $n \in \mathbb{N}$. Dans le second cas, G est dit cyclique.

Exemple 1.6 $G = (\mathbb{Z}/6\mathbb{Z}, +)$ est un groupe cyclique,1 et 5 sont deux générateurs de G.

Proposition 1.3 (*Sous- groupe des groupes cycliques*)
Chaque sous-groupe d'un groupe cyclique est un groupe cyclique.
Soit $G = \langle g \rangle$, *un groupe cyclique d'ordre* n *et soit* k *un nombre entier. Alors l'ordre du sous-groupe cyclique* $\langle g^k \rangle \subset G$ *est* $\frac{n}{PGCD(k,n)}$.
Soit G *un groupe cyclique engendré par* g, *alors* G *est aussi engendré par chaque* g^k *tel que* $PGCD\,(k,n) = 1$.
Soit G *un groupe cyclique d'ordre* n. *Si* d *un diviseur de* n. *Alors* G *a exactement un sous-groupe d'ordre* d, *c'est à dire* $\langle g^{n/d} \rangle$. *En outre, il ya exactement* d *solutions à l'équation* $x^d = 1$ *et celles-ci sont exactement les éléments de* $\langle g^{n/d} \rangle$.
deux groupes cycliques sont isomorphes si, et seulement s' ils ont le même ordre. Tous les groupe cycliques sont abéliens.

Proposition 1.4 (*Groupes cycliques et des morphismes*). *Soit* G *un groupe arbitraire et* $\phi : C_n \to G$ *un morphisme de groupes. Alors,* $\operatorname{Im}\phi$ *est un groupe cyclique isomorphe à* C_k, *avec* k *un diviseur de* n.

Definition 5 Soit G un groupe et $g \in G$. On dit que g est de torsion si l'ordre de g est fini. La torsion $T\,(G)$ de G est le sous-ensemble de tous les éléments de torsion.
On dit que G est sans torsion si la torsion de G ne contient que l'élément neutre.
Un groupe G est appelé un groupe de torsion si G est égal à sa torsion.

Exemple 1.7 $(\mathbb{Q}/\mathbb{Z}, +)$ est un groupe de torsion, et $(\mathbb{Z}, +)$ est un groupe sans torsion.

Proposition 1.5 *Soit* G *un groupe abélien, aloes la torsion* $T\,(G)$ *de* G *est un sous-groupe de* G.

Preuve. Clairement $1 \in T\,(G)$. Considérons deux éléments de $T\,(G)\,, g, h$ avec $O\,(g) = n$ et $O\,(h) = m$. Soit $k = ppcm\,(n,m)$. Alors $(gh^{-1})^k = g^k \left(h^k\right)^{-1} = 1$.
■

1.1.3 Théorèmes d'isomorphismes

Definition 6 Considérons deux groupes $(G, *, e_G)$ et $(H, \cdot, e_H)$. Soit $f : G \to H$ un morphisme de groupes, le noyau de f est l'ensemble $Ker f = \{g \in G : f\,(g) = e_H\} \subset G$. l'image de f est l'ensemble $\operatorname{Im} f = \{f\,(g) \mid g \in G\} \subset H$.

Proposition 1.6 *Soit* $f : (G, *, e_H) \to (H, \cdot, e_H)$ *un morphisme de groups. On a*
$Ker\ f$ *est un sous-groupe normal de* G *;*
Im f *est un sous- groupe de* H *;*
pour tout $x \in G$, $x* \ Kerf = f^{-1} \circ f(x) := \{y \in G \mid f(y) = f(x)\}$ *;*
f *est un monomorphisme si, et seulement si* $Kerf = \{e_G\}$ *;*
f *est un épimorphisme si, et seulement si* Im $f = H$.

Preuve. On sait que $e_G \in Kerf$, donc $Kerf$ non-vide. Alors si $a, b \in Kerf$, il suffit de démontrer que $a * b^{-1} \in Kerf$. On voit $f(a * b^{-1}) = f(a) \cdot f(b)^{-1} = e_H \cdot e_H^{-1} = e_H$. Donc, $a * b^{-1} \in Kerf$ et $Kerf$ est un sous-groupe. Pour voir que c'est un sous-groupe normal, il faut et il suffit de voir que $b * a * b^{-1} \in Kerf$,$\forall b \in G, \forall a \in Kerf$. En effet ,$f(b * a * b^{-1}) = f(b) \cdot f(a) \cdot f(b)^{-1} = f(b) \cdot e_H \cdot f(b)^{-1} = f(b) \cdot f(b)^{-1} = e_H$. De la même façon que pour Im f, on a que $e_H \in$ Im f et il suffit de montrer que si $x, y \in$ Im f, alors $x \cdot y^{-1} \in$ Im f. Comme $x, y \in$ Im f, il existe $a, b \in G$ tels que $x = f(a)$ et $y = f(b)$. Dès lors $x \cdot y^{-1} = f(a) \cdot f(b)^{-1} = f(a * b^{-1}) \in$ Im f. Supposons que $y \in f^{-1} \circ f(x)$. Alors $f(x) = f(y)$,où $e_H = f(x)^{-1} \cdot f(y) = f(x^{-1} * y)$. Donc $x^{-1} * y \in Kerf$. On déduit que $y = (x * x^{-1}) * y = x * (x^{-1} * y) \in x * Ker\ f$. D'autre part, si $y \in x * Kerf$, alors $y = x * a$ pour un élément $a \in Kerf$. Donc $f(y) = f(x * a) = f(x) \cdot f(a) = f(x) \cdot e_H = f(x)$. ■

Exemple 1.8 On les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}^*, .)$, alors l'application suivante est un homomorphisme de groupe $f : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$ $x \to \exp(x)$. On applique la définition $\forall\ x, y \in \mathbb{R}$, $f(x + y) = f(x) \cdot f(y)$, $\forall\ x, y \in \mathbb{R} \quad \exp(x + y) = \exp(x) \cdot \exp(y)$.

Definition 7 Un isomorphisme de groupe un morphisme de groupe qui est bijectif. Son inverse est alors un morphisme de groupe.

Th■or■me 1.2 *(Premier théorème d'isomorphisme). Considérent deux groupes* $(G, *, e_G)$ *et* $(H, \cdot, e_H)$. *Soit* $f : G \to H$ *un morphisme de groupes. Alors il existe un isomorphisme naturel de groupes* $G/K\,\mathrm{erf} \cong \mathrm{Im}\, f$.

Preuve. l'application $\psi : G/K\,\mathrm{erf} \longrightarrow \mathrm{Im}\, f$ définie par $\psi(gK\,\mathrm{erf}) = f(g)$ est un isomorphisme de groupes. ■

Exemple 1.9 Considérons le groupe général linéaire de degré n sur le corps $\mathbb{R}$,

$GL_n(\mathbb{R})$. Le déterminat est un morphisme de $GL_n(\mathbb{R})$ dans le groupe multiplicatif $(\mathbb{R}^*, \times)$. Le noyau est exactement le groupe spécial linéaire $SL_n(\mathbb{R})$, et on déduit que $\mathbb{R}^* \cong GL_n(\mathbb{R}) / SL_n(\mathbb{R})$.

Exemple 1.10 On considère le sous-groupe suivant du groupe multiplicatif $(\mathbb{C}^*, .)$: $E = \{x \in \mathbb{C} : |x| = 1\}$. L'ensemble E est le cercle unité complexe. On a un morphisme surjectif de groupes $\varphi : (\mathbb{R}, +) \longrightarrow (E, .), \varphi(x) = e^{2\pi x i}$. Puisque $Ker\varphi = \mathbb{Z}$, on obtient $E \cong \mathbb{R}/\mathbb{Z}$.

Th■or■me 1.3 *(Deuxième théorème d'isomorphisme). Soient H un-sous groupe et N un sous-groupe normal d'un groupe G. Alors,*
(i) N un sous- groupe normal de HN ;
(ii) $H \cap N$ est un sous-groupe normal de H ;
(iii) $H/(H \cap N) \cong HN/N$;
(iv) Si est en outre fini, alors $|HN| = \frac{|H||N|}{|H \cap N|}$.

Preuve. Voir (la réference). ■

Th■or■me 1.4 *(Troisième théorème d'isomorphisme). Soient H et N des sous-groupes normaux d'un groupe G et $N \subset H$, alors*
(i) H/N est un sous-groupe normal G/N ;
(ii) $(G/N)/(H/N) \cong G/N$.

Preuve. Voir (la réference). ■

1.2 Anneaux et corps

1.2.1 Anneaux

Definition 8 Un Anneaux est la donnée d' un ensemble A muni de deux opérations, une addition et une multiplication vérifant :
(i) $(A, +)$ est un groupe commutatif, d' élément neutre noté 0 ;
(ii) La multiplication est associative est possède un élément neutre noté 1, appelé élément unité ;
(iii) La multiplication est distrubitive par apport à l'addition c' est-à-dire :

$\forall (x,y,z) \in A^3 : x(y+z) = xy + xz$ et $(y+z)x = yx + zx$.
Si la multiplicaion est commutative, on dit que l' anneaux A est commutatif.

Exemple 1.11 (a) L'anneau nul, $0 = \{0\}$, avec l'addition $0+0=0$ et la multiplication $0 \cdot 0 = 0$.
(b) Les quaternions $\mathbb{H} = \{a + bi + cj + dk : a,b,c,d \in \mathbb{R}\}$, avec l'addition et la multiplication données par les formules suivantes :
$(a + bi + cj + dk) + (a' + b'i + c'j + d'k)$
$= (a+a') + (b+b')i + (c+c')j + (d+d')k$,
$i^2 = j^2 = k^2 = -1, ij = -ji = k$;
est un exemple d'anneau non-commutatif.

Definition 9 Soit A un anneau. On dit que A est intègre si la condition $ab = 0$ avec $a, b \in A$ implique que $a = 0$ ou $b = 0$.

Exemple 1.12 (1) $(\mathbb{Z}, +, \times)$ est un anneau intègre.
(2) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est intègre si, et seulement si n est premier.
(3) Si A est un anneau intègre, alors $A[x_1, ..., x_n]$ est intègre aussi.

Definition 10 Soit $(A, +, \times)$ un anneau d'unité 1.
Soit $\Phi : N \to A, n \longmapsto \underbrace{1+1+1...+1}_{(n \text{ fois})}$.

Le caractéristique de A qu' on note $Car(A)$ est le plus petit n, s'il existe, tel que $\Phi(n) = 0$. Sinon $Car(A) = 0$.

Exemple 1.13 $Car(\mathbb{Z}) = 0$.

Definition 11 Un sous- ensemble B d'un anneau A est appelé sous- anneau s' il est non vide, stable par soustraction, par multiplication, et contient 1.

Definition 12 Soient R, S et T des anneaux.
Un morphisme $f : R \to S$ d'anneaux est une application telle que :
$f(a+b) = f(a) + f(b)$;
$f(a \cdot b) = f(a) \cdot f(b)$;
$f(1_R) = 1_s$. pour tout $a, b \in R$.
Un morphisme d'anneaux $f : R \to S$ est appelé un monomorphisme si, et seulement

si pour tout deux morphismes d'anneaux $g, h : T \to R$, ona $f \circ g = f \circ h \Longrightarrow g = h$.
Si $R \to S$ est un monomorphisme, on dit que S est un extension d'anneau de R.
Un morphisme d'anneaux $f : R \to S$ est appelé épimorphisme si et seulement si pour tous deux morphisme d'anneaux $g, h : S \to T$, on a $g \circ h = h \circ f \Longrightarrow g = h$.
Un morphisme d'anneaux $f : R \to S$ est appelé un isomorphisme si et seulement s'il existe une application $f^{-1} : S \to R$ tel que $f^{-1} \circ f = id_r \quad f \circ f^{-1} = id_s$.
Un endomorphisme d'anneaux est un morphisme d'anneaux $f : R \to R$, un automorphisme d'anneaux est un isomorphisme d'anneaux $f : R \to R$.

Definition 13 Une partie $I \subset A$ est un idéal de A si I est un sous-groupe de A pour l'addition et si, pour tout $x \in I$ et tout $a \in A$, on a $ax \in I$.

Exemple 1.14 (a) $I = \{0\}, I = A$ sont deux idéaux pour tout anneau A.
(b) Pour $n \in \mathbb{Z}$ on définit $n\mathbb{Z} = \{x \in \mathbb{Z}, n \mid x\}$, qui est un idéal de $\mathbb{Z}$.

Definition 14 Soit R un anneau.
(1) Un idéal $P \subset R$ est applé un idéal premier si, et seulement si pour tous les idéaux I, $J \subset R$ tels que $IJ \subset P$, il suit que $I \subset P$ ou $J \subset P$.
(2) L'anneau R est appelé un anneau premier si, et seulement si $\{0\}$ est u n idéal premier.
(3) Un idéal $P \subset R$ est appelé un idéal maximal si, et seulement si pour tout idéal $M \subset R$ tel que $M \subset I$, il suit $M = I$ ou $M = R$.
(4) L'anneau R est appelé un anneau simple si, et seulement si $\{0\}$ et un idéal maximal, c'est -à-dire R ne contient pas d'idéaux propres.

1.2.2 Corps

Definition 15 Soit K un anneau. On dit que K est un corps si tout élément non nul de K est inversible.

Exemple 1.15 Les anneaux $\mathbb{Q}$ et $\mathbb{R}$ sont des corps, appelés respectivement corps des nombres rationneles et corps des nombres réeles.

Definition 16 Soient K un corps et $\varphi_k : \mathbb{Z} \to \Bbbk$,$n \to n \times 1$ un morphisme d'anneau,on a :

(a) Si $\ker \varphi_k = \{0\}$, on dit que le corps k est de caractéristique 0.

(b) Si $\ker \varphi_k = p\mathbb{Z}$, où p est un nombre premier, on dit que K est de caractéristique p.

Exemple 1.16 Les corps $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des caractéristique 0. Si p est un nombre premier, le corps $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p.

Definition 17 On appele corps fini un corps ayant un nombre fini d' éléments.

1. Tout corps fini (c'est-à-dire de cardinal fni) est nécessairement de caractéristique non nulle.
2. Pour tout nombre premier p, le corps $\mathbb{Z}/p\mathbb{Z}$ est de cardinal p de caractéristique p.
3. Si V est un espace vectoriel sur un corps K, alors $\dim_K v = n < \infty \Longleftrightarrow v \simeq K^n$.
4. Le cardinal d'un enssemble X sera noté $card\,(X)$ ou $|X|$.

Th■or■me 1.5 *Si K un corps fini de caractéristique p, il existe alors un entier $n \geq 1$ tel que $|K| = p^n$.*

Preuve. K un corps fini de caractéristique $p \neq 0$, donc K est extension de $\mathbb{F}_p$ (Ch.1) ; on peut supposer $\mathbb{F}_p \subseteq K$, alors, $(\mathbb{F}_p \subseteq K$ et $|K| < \infty) \Longrightarrow [K : \mathbb{F}_p] < \infty$ posons $n := [K : \mathbb{F}_p]$; ainsi K est un espace vectoriel de dimension fini, n, sur $\mathbb{F}_p$;d'oú $K \simeq \mathbb{F}_{p^n}$ (Rappel c,ci- dessus) ,ce qui implique $|K| = p^n$. ■

Th■or■me 1.6 *Soit un corps fini F. Alors le nombre q d'éléments de F est une puissance d'un nombre premier p, i.e. $q = p^m$.*

Preuve. Construisons la suite $\{u_i\}$ dans F comme suit :

$$\left\{ \begin{array}{c} u_0 = 0 \\ u_n = u_{n-1} + 1 \end{array} \right\}, \text{ pour } n \geqslant 1.$$

Comme F est fini , tous les éléments u_n ne sont pas distincts, soit $u_k = u_{k+c}$, la premier répétition rencontrée, c-à-d les éléments u_0 ,$u_1, ..., u_{k+c-1}$ sont tout distincts. Or $u_{k+c} = u_k + u_c$,et donc $u_c = 0$. Il s'ensuit que le premier élément répété est 0

et que les éléments de la suite $\{u_0, u_1, ..., u_{c-1}\}$ sont tous distinctes. Montrons que c est premier. Remarquons d'abord que $c \geq 2$ par définition d'un corps. Par l'absurde,

supposons que $c = ab$, avec $1 < a, b < c$. La relation $(II, 1)$ implique que $u_c = u_{ab} = u_a u_b$, ce qui est imposible car $u_c = 0, u_a \neq 0, u_b \neq 0$.E$'$tant donné que c est premier, nous allons le noter p.

Le sous -enssemble $F_q = \{u_0, u_1, ...u_{p-1}\}$ de F est un sous-corps de F car il est isomorphe au corps $\mathbb{F}_p = \{0, 1, ..., p-1\}$. en effet, il suffit de prendre l'application $f : F_p \to \mathbb{F}_p : u_i \to i$.

Construisons l'ensemble

$W_1 = \{u_0\omega_1, u_1\omega_1, ...u_{p-1}\omega_1\} = \{u_i\omega_1 / u_i \in F_p\}$

à partir d'un éléments $\omega_1 \in F \backslash F_p$. Cet ensemble possède p éléments

Si $q = p$, alors la thèse est démontrée. Sinon, nous construisons l'ensemble

$W_2 = \{u_i\omega_1 + u_j\omega_2 \mid u_i, u_j \in F_p \text{ et } u_i \neq u_j\}$

à partir d'un élément $\omega_2 \in F \setminus W_1$.

Si $q = p$, alors la thèse est démontrée. Sinon, nous construisons l'ensemble $W_2 = \{u_i\omega_1 + u_j\omega_2 \mid u_i, u_j \in F_p \text{ et } u_i \neq u_j\}$

à partir d'un élément $\omega_2 \in F \backslash W$.

L'enssemble W_2 comporte p^2éléments. Si $q = p^2$, alors la thèse démontrée. Sinon, nous recommençons de même jusqu'à la construction de l'ensemble

$W_m = \{u_i\omega_1 + u_j\omega_2 + ...u_l\omega_m \mid u_i, u_j, ...ut \in F_p \text{ et } u_i \neq u_j \neq ...u_t\}$

à partir d'un élément $\omega_m \in F \backslash W_{m-1}$.Cet ensemble comporte p^m éléments, ce qui termine la démonstration. ■

Exemple 1.17 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un corps fini pour p premier.

Proposition 1.7 *Soit $\mathbb{F}_{p^m}$ un corps à P^m éléments, si K est un sous-corps de $\mathbb{F}_{p^m}$, alors K à p^d éléments ou d divise m. Réciproquement pour tout diviseur d de m, il existe un unique sous -corps de $\mathbb{F}_{p^m}$ a p^d éléments.*

Exemple 1.18 Comme 2 divise 4, $\mathbb{F}_4 = \mathbb{F}_{2^2}$ est un sous-corps de $\mathbb{F}_{16} = \mathbb{F}_{2^4}$.

Proposition 1.8 *Soient i un entier naturel et p est un nombre premier. Soient x et y deux éléments d'un corps K, on a, $(x + y)^{p^i} = x^{p^i} + y^{p^i}$.*

Preuve. L'énoncé est vrai si $i = 0$. Soit k un entier tel que l'égalité annoncée est vérfiée. Pour tous $x, y \in K$, on a

$(x+y)^{p^{k+1}} = \left((x+y)^{p^k}\right)^p = \left(x^{p^k}+y^{p^k}\right)^p$. Pour tout entier $j = 1..., p-1$, le cofficient binômial C_p^j est divisibles par p. La formule du binômes de Newton entraîne alors l'égalité $(x+y)^{p^{k+1}} = x^{p^{k+1}} + y^{p^{k+1}}$. ■

Proposition 1.9 *Soit $(K,+,\times)$ un corp fini et p un nombre premier. On a,*
(1) *Le cardinal de K est une puissance de p.*
(2) *Pour tout $n \in \mathbb{N}^*$, il existe un corps K de cardinal p^n. De plus, K est unique à morphisme près.*

Preuve. Le sous-corps premier de K étant isomorphe à $\mathbb{Z}/p\mathbb{Z}$, K possède une structure naturelle de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. En notant $n = [K : \mathbb{Z}/p\mathbb{Z}]$.
Alors $|K| = |\mathbb{Z}/p\mathbb{Z}|^n = p^n$.
Soit $n \in \mathbb{N}^*$. Si K est un corps fini de cardinal p^n, alors K est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$:en effet, pour tout $x \in k$, x est racine de $X^{p^n} - X$ possède ses p^n racines dans k. Réciproquement, soit K le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$. Soit k l'ensemble des éléments de K qui sont racines de $X^{p^n} - X$, Vérifions que k est un sous-corps de K : d'une part,$1_K \in k$; d'autre part, si bien que $x+y \in k$, alors $x^{p^n} = x$ et $y^{p^n} = y$, donc $(x+y)^{p^n} = x^{p^n} + y^{p^n} = x+y$ et $(xy^{-1})^{p^n} = xy^{-1}$, si bien que $x+y$, $xy^{-1} \in k$. Par ailleurs, $\left(X^{p^n} - X\right)' = -1$ est premier avec $X^{p^n} - X$, donc les racines de $X^{p^n} - X$ sont simples, de sorte que $|k| = p^n$: par conséquent, $k = K$ est un corps à p^n éléments, et il est unique à isomorphe près, par unicité du corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$. On notera $\mathbb{F}_q$ le corps fini a $q = p^n$ éléments. ■

Th■or■me 1.7 *Le groupe multiplicatif $\mathbb{F}_q^*$ est un groupe cyclique, donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.*

Definition 18 Soit K une corps. Une extension de K est un corps L tel que K est un sous-corps de L (i.e $K \subset L$).

Remarque 1.1 (1) Si K est un sous-corps de L, L est un K-espace vectoriel.
(2) Si $\dim_K L$ est finie, on pose $[L : K] = \dim_K L$ et l'entier $[L : K]$ s'appelle le degré de L sur K.
(3) Si K et L sont des corps finis, on a $|L| = |K|^n$ avec $n = [L : K]$.

Remarque 1.2 (1) Si on a $f : K \to L$ un morphisme injectif de corps, on peut voir K comme un sous-corps de L en identifiant $f(K) \simeq K$.
(2) Si L est une extension de K, on dispose d'une structure de $K-$espace vectoriel sur L.

Definition 19 Un polynôme non constant $f(x)$ de $\mathbb{K}[x]$ est irréductible si et selement si n'est pas un constante multiplicative non nulle près, divisible que par lui même et par 1.

Exemple 1.19 (1) Les polynômes $x - \lambda$ sont irréductible ($\lambda \in \mathbb{R}$).
(2) Dans $\mathbb{R}[x]$, tout polynôme $ax^2 + bx + c$, tel que $\Delta = b^2 - 4ac < 0$ est irréductible.

Proposition 1.10 *Soit* $f(x) = a_d x^d + a_{d-1}x^{d-1} + ... + a_0 \in \mathbb{Z}[x]$. *Supposons qu' il existe* p *premier tel que*
· p *divise* a_i, $0 \leq i < d-1$, *mais* p *ne divise pas* a_d;
· p^2 *ne divise pas* a_0.
Alors $P(x)$ *est irréductible dans* $\mathbb{Q}[x]$.

Proposition 1.11 *Pour tout* $n \in \mathbb{N}^*$, *posons* $I(n,p)$ *l'esemble des polynômes de* $\mathbb{F}_p[x]$ *unitaires irréductibles de degré* n. *Alors pour tout* $n \in \mathbb{N}^*$, *dans* $\mathbb{F}_p[x]$,

$$X^{p^n} - X = \prod_{d \backslash n} \prod_{P \in I(d,p)} P.$$

Preuve. Soit p un facteur irréductible de $X^{p^n} - X$ sur $\mathbb{F}_p$ de degré d. Le corps rupture de P sur $\mathbb{F}_p$ est un sous-corps de cardinal p^d du corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$, c'est-à-dire $\mathbb{F}_{p^n}$, donc d/n.
Réciproquement, soient $d \backslash n$, et $P \in I(d,p)$. Soit α une racine de P dans le corps de rupture de P sur $\mathbb{F}_p$; alors $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^d}$. On en déduit que α est racine de $X^{p^n} - X$. Or Comme P est irréductible, alors P est le polynôme minimal de α est $\mathbb{F}_p$,donc $p \mid X^{p^n} - X$. Pour conclure, il suffit de remarquer que les facteurs irréductibles de $X^{p^n} - X$ sur $\mathbb{F}_p$ sont simples (par le même argument que précédemment), d'où la formule annoncée. ■

Chapitre 2

Les courpes elliptiques définies sur $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$

La lettre $\Bbbk$ désigne le corps commutatif $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ou $\mathbb{F}_q$.

2.1 Définitions et invariants

Definition 20 Une courbe elliptique est une cubique plane E non singulière (lisse) (les points singuliers sont les sont : les noeuds, les point de rebourssements), d'équation de la forme : $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, les cinq coefficients a_i sont des éléments d'un corps commutatif quelconque $\Bbbk$. Les deux variables x et y sont des zéros de cette équation. L'équation ci-dessus est dite l'équation de Weierstrass.

Proposition 2.1 *Soit E une cubique plane définie par l'équation $E : y^2+a_1xy+a_3y = x^3 + a_2x^2 + a_4x + a_6$, les cinq coefficients a_i sont des éléments d'un corps commutatif quelconque $\Bbbk$. On pose $P(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$. On a, la courbe E est elliptique si, et seulement si, le vecteur $\left(\frac{\partial P}{\partial x}(x, y), \frac{\partial P}{\partial y}(x, y)\right)$ n'est pas le vecteur nul. En d'autres termes, on peut définir une tangente à la courbe au point (x, y).*

Exemple 2.1 On prend $\Bbbk = \mathbb{R}$, on pose :
$E_1 : y^2 = x^3 + x$ et $E_2 : y^2 = x^3 + x^2$.
Les courbes E_1 et E_2 sont bien définies sur $\mathbb{R}$ puisque tous les coefficients sont réels.

La courbe E_1 est lisse, en effet :

$\left(\frac{\partial P}{\partial x}(x,y), \frac{\partial P}{\partial y}(x,y)\right) = (0,0) \Longleftrightarrow \begin{cases} x = i/\sqrt{3} \text{ ou } -i/\sqrt{3} \\ y = 0 \end{cases}$.

Or les points $\left(i/\sqrt{3}, 0\right), \left(-i/\sqrt{3}, 0\right)$ ne sont pas sur la courbe E_1 et E_1 est donc une courbe elliptique.

Pour E_2, le point $(0,0)$ est un point sur la courbe et on vérifie aisément que $\frac{\partial P}{\partial x}(0,0) = \frac{\partial P}{\partial y}(0,0) = 0$. On dit alors que le point $(0,0)$ est un point singulier. La courbe E_2 n'est pas lisse et n'est pas une courbe elliptique.

Definition 21 Toute courbe elliptique E possède plusieurs invariants : un discriminat, un invariant modulaire, un invariant différentiel, un conducteur, un régulateur,...

Proposition 2.2 *Soit $\mathbb{k}$ un corps de caractéristique $\neq 2$ et E une courbe définie sur $\mathbb{k}$ par $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ alors la courbe E est lisse si, et seulement si le polynôme $x^3 + a_2x^2 + a_4x + a_6$ n'a pas de racine multiple dans $\overline{\mathbb{k}}$. On rappelle qu' un polynôme p possède une racine multiple si et seulement si son discriminant, $disc(P)$, est nul , or : $disc(x^3 + a_2x^2 + a_4x + a_6) = -4a_6a_2^2 + (a_4a_2)^2 + 18a_6a_4a_2 - 4a_4^3 - 27a_6$.*

On pose $\Delta(E) = 16 disc(P)$ et ainsi $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ est une courbe elliptique si, et seulement si $\Delta(E) \neq 0$.

1. $E_1/\mathbb{R} : y^2 = x^3 + x$,on a $\Delta(E_1) = -64 \neq 0$.
2. $E_2/\mathbb{R} : y^2 = x^3 + x^2$,on a $\Delta(E_2) = 0$.
3. $E_3/\mathbb{R} : y^2 = x^3 + a$,on a $\Delta(E_3) = -2^4 \times 3^3 \times a$. On verifie directement que E_3 est une courbe elliptique si, et seulement si car $k \nmid 2 \times 3 \times a$.

Definition 22 E une courbe définie sur $\mathbb{k}$ par $E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$. On pose : $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$, $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

La courbe E est une courbe elliptique si, et seulement si $\Delta(E) \neq 0$. Dans ce cas, on pose $j(E) = \frac{\left(b_2^2 - 24b_4\right)^3}{\Delta(E)}$, on dit que $j(E)$ est le j-invariant de E.

Definition 23 L'invariant différentiel d'une courbe elliptique E d'équation de Weierstrass :

$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$

Est l'élément différentiel $\omega(E) = \frac{dx}{2y+a_1x+a_3} = \frac{-dy}{3x^2+2a_2+a_4-a_1y}$.

Exemple 2.2 Pour l'équation de Weierstrass E :

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

l'invariant différentiel est égal à :

$\omega(E) = \frac{dx}{2y} = \frac{-dy}{3x^2-a1}$.

Definition 24 On considère une courbe elliptique E définie sur $\Bbbk$ d'équation de Weierstrass :

$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$

L'ensemble des point $\Bbbk$-ratinnels de E, noté $E(\Bbbk)$ est :

$E(\Bbbk) = \{(x, y) \in \Bbbk^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$.

Le point O est appelé point à l'infini.

Exemple 2.3 Soit E une courbe elliptique définie sur $\mathbb{Q}$ par $E : Y^2 = X^3 - 6X + 4$.

L'enssemble des points $\mathbb{Q}$ rationnels de E

$E(\Bbbk) = \{O_E, (-1, 3), (-1, -3), (2, -3), (2, 0), (1, -1), ...\}$.

Definition 25 Soient E une courbe elliptique et $E(\Bbbk)$ les point $\Bbbk$-ratinnels de E. On définit sur $E(\Bbbk)$ une loi de composition, on prend le point à l'infini comme élément neutre. cette loi est rendue possible par la porpriètè suivante, qui est la règle géométrique suivante "trois points colineaires de $E(\Bbbk)$ ont une somme nulle". Prenons deux points P et Q de $E(\Bbbk)$, en général, la ligne passant par P et Q recoupe la courbe E en un troisième point de cordonnées (x, y). Son symétrique $(x, -y)$ est lui aussi sur la courbe E et on le désigne $P + Q$. $(E(\Bbbk), +)$ forme un groupe abélien.

Th■or■me 2.1 *Soit E une courbe elliptique définie sur $\Bbbk$ par $E : y^2 = x^3 + ax + b$. Considèrons deux points $P_1(x_1, y_1), P_2(x_2, y_2)$ de $E(\Bbbk)$. On a,*

Si $P_1 = O$, alors $P_1 + P_2 = P_2$;

Si $P_2 = O$, alors $P_1 + P_2 = P_1$;

Si $x_1 = x_2$ et $y_1 = -y_2$, alors $P_1 + P_2 = 0$;

Sinon, définir λ par :

$$\begin{cases} \lambda = \frac{y_2 - y_1}{x_2 - x_1} \ si \ P_1 \neq P_2 \\ \lambda = \frac{3x_1^2 + a}{2y_1} \ si \ P_1 = P_2 \end{cases}$$

Et soit $x_3 = \lambda^2 - x_1 - x_2$ *et* $y_3 = \lambda(x_1 - x_3) - y_1$.

Alors $P_1 + P_2 = (x_3, y_3)$.

Definition 26 Soit $n \in \mathbb{N} - \{0\}$. Le $n-$espace projectif sur le corps $\Bbbk$ qu'on note $P^n(\Bbbk)$ est défini comme l'ensemble des classes d'équivalence des $(n+1)$-uplets suivants :

$P^n(\Bbbk) = \frac{\{(a_0,...,a_n) \in \Bbbk : a_0,...,a_n \text{ non tous nuls}\}}{\sim}$,

où $(a_0, ..., a_n) \sim (b_0, ..., b_n)$ s'il existe $t \in \Bbbk^*$ tel que

$(b_0, ..., b_n) = t(a_0, ..., a_n)$

Th■or■me 2.2 *Si* E *est une courbe elliptique définie sur un corps* $\Bbbk$*, alors il existe une application* $\phi : E(\Bbbk) \to P^2(\Bbbk)$ *qui fournit un isomorphisme de* $E(\Bbbk)$ *sur une courbe* $C(\Bbbk)$ *donnée par l'équation de Weierstrass* $C : F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0$,

où $a_1...a_6 \in K$ *; et tel que* $\phi(\mathcal{O}) = (0,1,0)$.

Preuve. *Voir* [8] ■

2.1.1 Courbe elliptique sur $\mathbb{Q}$

On va maintenant s'occuper à des aspacts diophantiens des courbes elliptiques. Une des questions que on peut se poser à ce sujet c'est l'existence et la structure des point rationnels sur la courbe. A ce propos on sait, grace au théorème de Fermat, que $E(\mathbb{Q})$ a une structure de groupe Abelien, et ona un autre resulta trés important du à Mordell :

Th■or■me 2.3 (*Mordell*) *Soit* E *une courbe elliptique sur* $\mathbb{Q}$*. Alors* $E(\mathbb{Q})$ *est un groupe Abelien de type fini. Plus précisement, on a :*

$E(\mathbb{Q}) = E_t(\mathbb{Q}) \oplus G$,

où $E_t(\mathbb{Q})$ *est le sous groupe de torsion de* $E(\mathbb{Q})$ *c'est-à-dire l'ensemble des points* $T \in E(\mathbb{Q})$ *tels que il existe* $k \in \mathbb{Z} - \{0\}$*, avsc* $kT = \mathcal{O}$ *et* G *est engendré par un nombre fini* r *des points* P_i *d'ordre infini . Donc* $G \simeq \mathbb{Z}$ *et tout point* $P \in E(\mathbb{Q})$ *peut s'écrire comme* $P = T + \sum_{i=1}^{r} a_i P_i$*, avec* $T \in E_t(\mathbb{Q})$, $a_i \in \mathbb{Z}$*. L'ordre* r *est appelé*

rang algébrique de la courbe E.

Proposition 2.3 (*Forme Normale de Weierstrass*). *Toute courbe cubique C ayant coefficients dans $\mathbb{Q}$ et possédant au moins un point rationnel peut s'écrire la forme normale de Weierstrass.*

$y^2 = x^3 + ax^2 + bx + c$ ou $y^2 = 4x^2 - g_1x - g_2$ ou $y^2 = x^3 + Ax + B$

avec $a, b, c, g_1, g_2, A, B \in \mathbb{Q}$. Cette proposition est aussi vraie pour tout corps $\mathbb{K}$ ayant caractéristique différente 2 et 3.

Preuve. La preuve consiste un transformation projective. E$'$tant donné $\mathcal{O}$ un point rationnel sur C n étant pas un point d'inflexion, considérons les axes suivantes :

-L'axe Z donné par la tangente au point $\mathcal{O}$;

-L'axe X donné par la tangent au point d'interseciant centre C et l'axe Z ;

-L'axe Y donné par tout axe différent de Z intersection l'axe X .

La transformation projective $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ ainsi q'un complétion du carré permet d'obtenir le premier resultat . Un translation selon l'axe des x permet d'obtenir le second. Le troisième est déduit du second.

Nous ne discuterons que des courbes sous la forme 1.1. Chaque courbe cubique C ayant coefficients rationneles peut être décrire avec $f \in \mathbb{Q}[x]$ comme $Z(y^2 - f(x))$ et f ayant la forme $f(x) = x^3 + ax^2 + bx + c$ ou

$f(x) = 4x^3 - g_1x - g_2$ ou $f(x) = x^3 + Ax + B$. ■

2.1.2 Courbe elliptique sur $\mathbb{R}$

Definition 27 (Courbe elliptique sur réelle). On appelle courbe elliptique sur $\mathbb{R}$ la réunion de tout courbe plane l'équation $y^2 = x^3 + ax + b$. (avec a et b deux réelles vérifant $4a^3 + 27b^2 \neq 0$) et de $\{\mathrm{Q}_\infty\}$ soit ε une courbe illéptique réelle $\exists\,(a,b) \in \mathbb{R}^2 \left\{ \begin{array}{c} \varepsilon = \{Q_\infty\} \cup \{x,y\} \in \rho / y^2 = x^3 + ax + b \\ 4a^3 + 27b^2 \neq 0 \end{array} \right\}$

Proposition 2.4 *La courbe plane réelle $\varepsilon \setminus \{Q_\infty\}$ admet en tout point une tangente.*

Preuve. *Ce resultat de courbe directement du fait que l'apllication $x \mapsto \sqrt{x^3 + ax + b}$ et $x \mapsto -\sqrt{x^3 + ax + b}$sont dérivable sur leur ensemble définition privé des racines de $X^3 + aX + b$ et que soit $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux point ε.*

si $P_1 = \ Q_\infty$ *on pose* $A(P_1, P_2) = P_2$;

si $P_2 = \ Q_\infty$ *on pose* $A(P_1, P_2) = P_1$;

si $P_1 = p_2 \neq Q_\infty$ *et* $y_1 \neq 0$, *la tangente a* $\varepsilon \setminus \{Q_\infty\}$ *coupe* ε *en deuxième point* $p_3^{'}$ *,et on note* $A(P_1, P_2)$ *le symétrique otthogonal de* $P_3^{'}$ *par apport à l'axe des abscisses*

si $P_1 = p_2 \neq Q_\infty$ *et* $y_1 = 0$, *on pose* $A(P_1, P_2) = Q_\infty$

si $x_1 = x_2 \neq \infty$ *et* $y_1 \neq y_2$,*on pose* $A(P_1, P_2) = Q_\infty$

si $x_1 \neq x_2$, *la droite affine* (P_1, P_2) *coupe* ε *en troisième point et on note* $A(P_1, P_2)$ *le symétrique orthogonale de le troisième point par apport á l'axe abscisses.* ■

Definition 28 Le discriminant Δ de l'équation de Weierstrass et la quantité $\Delta = -b_2^2 b_8 - \ b_4^3 - 27b_6^2 + ab_2b_4b_6$

et le $j - invariant$ de la courbe élliptique E est la quantité

$J(E) = \frac{C_4^3}{\Delta}$.

1. $E_1/\mathbb{R} : y^2 = x^3 + x$. On a $(E_1) = -4 \times 16 \neq 0$, est une courbe elliptique ;
2. $E_2/\mathbb{R} : y^2 = x^3 + x^2$.On a $\Delta(E_1) = 0 \times 16 = 0$, n'est pas courbe elliptique.

2.1.3 Courbes elliptiques sur $\mathbb{C}$

Definition 29 Soient $\mathbb{K}$ un corps et V un $\mathbb{K}$-espace vectoriel de dimenssion n. Une partie L de V est un sous réseau s'il existe une famille libre $B = (v_1, ..., v_r), 1 \leq r \leq n$ de V telle que $L = \mathbb{Z}v_1 + ... + \mathbb{Z}v_r$. On dit que B est une $\mathbb{Z}$-base de L et r est son range. On dit que L est un réseau si $r = n$.

Exemple 2.4 1. On sait que $\mathbb{C}$ est $\mathbb{R}$-espace vectoriel de dimenssion 2. La partie $L = \mathbb{Z} + \mathbb{Z}i$, avec $i^2 = -1$ est un réseau de range 2.
2. $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ n'est pas un sous réseau de $\mathbb{R}$.

Proposition 2.5 *Soient* L *un réseau de* V *et* $B = (v_1, ..., v_n)$ *une base de* V. *Alors* $B = (l_1, ..., l_n)$ *est une* $\mathbb{Z}$*-base de* L *si et seulement s'il existe une matrice* $A \in GL_n(\mathbb{Z})$ *tel que* $\begin{pmatrix} v_1 \\ . \\ . \\ . \\ v_n \end{pmatrix} = A \begin{pmatrix} l_1 \\ . \\ . \\ . \\ l_n \end{pmatrix}$.

Definition 30 Un réseau L de $\mathbb{C}$ est un sous groupe discret de range 2 de $\mathbb{C}$. Si $\{\omega_1, \omega_2\}$ est une base de L, on écrit $L = [\omega_1, \omega_2]$.

Definition 31 Une courbe elliptique E_L est le quotient de $\mathbb{C}$ par l'action d'un réseau L.

Definition 32 Soient E_{L_1} et E_{L_2} deux courbes elliptiques. On appelle isogénie une application non constante $f : E_{L_1} \longrightarrow E_{L_2}$ qui est à la fois une application holomorphe et un morphisme de groupes.

Notation 2.4 *Si $\alpha \in \mathbb{C}$, on note $m_\alpha : \mathbb{C} \longrightarrow \mathbb{C}$ la multiplication par α, $z \longmapsto \alpha z$.*

Proposition 2.6 *Soit $f : E_{L_1} \longrightarrow E_{L_2}$ une isogénie entre deux courbes elliptiques. Alors il existe $\alpha_f \in \mathbb{C}$ tel que $f \circ p_{L_1} = p_{L_2} \circ m_{\alpha_f}$. où $p_{L_1} : \mathbb{C} \longrightarrow E_{L_1}$ et $p_{L_1} : \mathbb{C} \longrightarrow E_{L_1}$ sont les projections canoniques.*

Proposition 2.7 *Soient L_1 et L_2 deux réseaux de $\mathbb{C}$. Alors les courbes elliptiques E_{L_1} et E_{L_2} sont isomorphes si et seulement si il existe $m_\alpha : \mathbb{C} \longrightarrow \mathbb{C}$ tel que $m_\alpha(L_1) = L_2$. Les classes d'isomorphisme des courbes elliptiques correspondent donc aux classes d'homothétite des réseux de $\mathbb{C}$.*

Corollaire 2.1 *L'étude des classes d'isomorphisme des courbes elliptiques est donc équivalante à l'étude des réseux complexes à homothétie prés. Soit $L = [\omega_1, \omega_2]$ un tel réseau. L'homothétie de rapport $\frac{1}{\omega_1}$ l'envoi sur le réseau $\left[1, \frac{\omega_2}{\omega_1}\right]$. On a $[\omega_1, \omega_2] \cong \left[1, \frac{\omega_2}{\omega_1}\right]$.*

Proposition 2.8 *On considère $H = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. On a,*
1. l'application $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) \longmapsto \frac{az+b}{cz+d}$, définit une action de $SL_2(\mathbb{Z})$ sur H.
2. Les réseaux $L_1 = [1, \tau_1]$ et $L_2 = [1, \tau_2]$ sont homothétiques si et seulement si τ_1 et τ_2 sont dans la même orbite sous cette action.

Preuve. Voir [1]. ■

Definition 33 Soit $\Omega := Z_{w_1} \oplus Z_{w_2}$ un réseau dans C, on définit la fonction de Weierstrass associeé à Ω par la formule :

$\wp(z) = \wp(z;\Omega) = \frac{1}{z^2} + \sum'_{\omega\in\Omega}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$,

où le signe $\sum'$ signifie qu'ou omet $\omega = 0$.

La fonction de Weierstrass permet de donner une description complète des fonctions elliptiques et d'établir le lien avec les courbes elliptiques.

Proposition 2.9 *Soit $E = C/\Omega$ une courbe elliptique, on alors*

$Ker\,[N]_E = \frac{1}{N}\Omega\ /\Omega \cong (Z/NZ)^2$.

Preuve. En effet l'application $[N]_E : C/\Omega \to C/\Omega$ est induite par la multiplication par N sur C donc $Ker\,[N]_E = \{z \in C \mid N\ z \in \Omega\}$ et comme $\Omega \cong Z^2$ le résultat est clair. ■

Th■or■me 2.5 (*Liouville*) *Une fonction entière* (*i.e. holomorphe sur C tout entier*) *est bornée et constante .*

Preuve. Considérons maintenant $\Omega := \mathbb{Z}_{\omega 1} \oplus \mathbb{Z}_{\omega 2}$ un réseau dans $\mathbb{C}$ et étudions les fonctions $\Omega-$ périodique, i.e, tells que $f(z+\omega) = f(z)$ pour $\omega \in \Omega$. Le théorème de Liouville indique que les seules fonctions entières et $\Omega-$périodiques sont les constantes, ce qui justifie la définition suivante. ■

Definition 34 Une fonction elliptique est une fonction méromorphe sur C et $\Omega-$ périodique pour un réseau Ω.

Remarquons que l'ensemble des fonctions $\Omega-$elliptiques forme en corps qu' on notera $\mathcal{M}(\Omega)$, qui contient les constantes, i.e. le corps C, et est stable par dérivation. Voyons tout de suite que cette définition n'est pas reduite aux constante.

Chapitre 3

Cardinal de point rationnels sur un corps fini

3.1 Les points rationnelles

Dans cette partie, on considère une courbe elliptique E defini sur k par :

$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$

Definition 35 L'ensemble des points $k-$rationneles de E, noté $E(k)$ est :

$E(k) = \{(x, y) \in k^2 \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$

Le point $\mathcal{O}$ est appelé "point à l'infinit".

Exemple 3.1 Soit E la courbe elliptique définie sur $\mathbb{Q}$ par

$E : Y^2 = X^3 - 6X + 4$

L'enssemble des points $\mathbb{Q}$ rationnels de E

$E(\Bbbk) = \{O_E, (-1, 3), (-1, -3), (2, -3), (2, 0), (1, -1), ...\}$.

Proposition 3.1 *Soit R un anneau principal, avec corps des fonction K, soit E une courbe elliptique donnée par une équation générale de Weierstrass :*

$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$, avec les $a_i \in R$, et soit $P = (X, Y) \in E(K)$ un point affine sur K

$X = \frac{M}{D^2}$ et $Y = \frac{N}{D^2}$, avec $\gcd(M, D) = \gcd(N, D) = 1$

Evidement cette proprieté est valable pour les cas $R = \mathbb{Z}$ et $K = \mathbb{Q}$ et elle est trés utile en pratique (comme on verra plus tard, dans la méthode des point de Heegner) .

Proposition 3.2 *Si P_1, P_2 et $\mathcal{O}$ sont des points rationnels, alors $P_1 + P_2$ est un point rationnele.*

Preuve. La proposition est évidente puisque les formules explicites ne contiennent que des constantes rationnelles.

Et ainsi, si nous admettons l'associativité de ‹‹+››, nous abtenons le résulta suivant. ■

Th■or■me 3.1 *Les points sur une courbe cubique non-singulière avec un point fixé $\mathcal{O}$ formet un groupe abélien sous l'opération ‹‹+››. De plus , si la courbe cubique est définie sur $\mathbb{Q}$ et si $\mathcal{O}$ est rationnel, $C(\mathbb{Q})$ est fermé sous l'opération*

Cette section est nécessaire pour introduire ce que sera une courbe elliptique et son lien avec les courbe cubique. L'objectif est simplement de pouvoir comprendre l'énoncé du théorème de Riemann-Roch et non de pouvoir le prouver. Soit un courbe C.

Definition 36 (Application rationnelle) .Pour deux variétés X, Y , une application

$\varphi : X \longrightarrow Y \quad \varphi = (f_1, ..., f_n)$

où $f_1, ...f_n \in \overline{K}(X)$, est dite rationnelle si pour tout point p de X où les f_i sont définies $\forall\ i$,

$\varphi(p) = (f_1(p), ...f_n(p)) \in Y$.

Finalement, nous abtenons un concept de morphisemes entre les variétés algébriques.

Definition 37 (Corps des fonctions rationnelles) . Soit $\overline{K}(V)$, appelé de corps des fonctions rationnelles, le corps des fraction de $\overline{K}[V]$.

Nous souhaitons pouvoir représenter les fonctions localement comme les fonctions de$\overline{K}$ (V) .

Th■or■me 3.2 *Le groupe* $E(\mathbb{F}_q)$ *est soit un groupe cyclique soit le produit de deux groupe cycliques. Dans le premier cas on a :*
$E(\mathbb{F}_q) \simeq \mathbb{Z}/d_2\mathbb{Z}$ *où* $d_2 = |E(\mathbb{F}_q)|$. *Dans le second cas, on a :* $E(\mathbb{F}_q) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ *où* $d_1 \mid d_2$ *et* $d_1 \mid q-1$.

Remarque 3.1 Il existe également des résultats sur la structure de points rationnels lorsque le corps $\mathbb{k}$ n'est pas un corps fini.
Soit $n \in \mathbb{Z}$, on dira qu'un point $P \in E\left(\overline{\mathbb{k}}\right)$ est un point de $n-torsion$ si l'on a $nP = \mathcal{O}$. Le sous-groupe de $E\left(\overline{\mathbb{k}}\right)$ des points de $n-$torsion est noté $E[n]$ i.e. :
$E[n] = \left\{P \in E\left(\overline{k}\right) \mid nP = \mathcal{O}\right\}$.

La structure des points de $n-torsion$ est donnée par le théorème suivant :

Th■or■me 3.3 *Si* $car\,\mathbb{k} = 0$ *ou si* $(n, car(\mathbb{k})) = 1$ *on a :*
$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
Si $car(\mathbb{k}) = p$ *et* $n = p^n$ *on a soit :*
$E[P^r] = \{\mathcal{O}\}$ *pour tout* $r \geq 1$
soit :
$E[P^r] \simeq \mathbb{Z}/P^r\mathbb{Z}$ *pour tout* $r \geq 1$.

Definition 38 Soit $p = car(\mathbb{k}) \neq 0$, si $E[P^r] = \{\mathcal{O}\}$ pour un (et donc pour tout) $r \geq 1$, la courbe elliptique E est dite supersingulière. Sinon , E est dite ordinaire.

Exemple 3.2 Sur $\mathbb{k} = \mathbb{F}_5$ on définit E par :
$E : y^2 = x^3 + 4x + 1$
On peut facilement énumérer tous les points de $E(\mathbb{F}_5)$:
$E(\mathbb{F}_5) = \{\mathcal{O}, (0,1), (0,4), (1,1), (1,4), (3,0), (4,1), (4,4)\}$.
Par exemple, le point $(0,1)$ est d'ordre 8 et le groupe $E(\mathbb{F}_5)$ est cyclique engendré par $(0,1)$ (ou par $(0,4), (1,1)$ et $(4,4)$). Le groupe $E(\mathbb{F}_5)$ ne possède pas de point de $5-torsion$ non-trivial. Cependant, cette courbe n'est pas supersingulière car on a bien $E[5] \simeq \mathbb{Z}/5\mathbb{Z}$; pour montrer cela il suffit juste et trouver un point de $5-torsion \neq \mathcal{O}$ dans $E\left(\overline{\mathbb{F}_5}\right)$. Considérons le corps $\mathbb{F}_{5^8} \simeq \mathbb{F}_5[\theta]$ où $\theta^8 + 2 = 0$, on peut vérifier que le point :
$P = \left(2\theta^4 + 1, 2\theta^6 + \theta^2\right)$

est bien un point de $5-torsion$; P ne peut pas être défini sur une extension plus petite de $\mathbb{F}_5$.

Remarque 3.2 L'utilisation des courbe elliptique pour le problème du logarithme discret demonde que l'on cnnaisse l'ordre du groupe. $E(\mathbb{F}_5)$, (ou du moins l'ordre du point de base G dans $E(\mathbb{F}_q)$).

Une estimation de cet ordre est donné par le théorème de Hasse-Weil :

Th■or■me 3.4 (*Hasse-Weil*)
Soit E une courbe elliptique définie sur $\mathbb{F}_q$, on a :
$|E(\mathbb{F}_q)| = q+1-t$ *où* $|t| \leq 2\sqrt{q}$
De plus, si p est un nombre premier, alors pour toute valeur entière de t dans l'intervalle $\left[-2\sqrt{P}, 2\sqrt{P}\right]$, il existe une courbe elliptique E définie sur $\mathbb{F}_p$ telle que $|E(\mathbb{F}_p)| = p+1-t$. Supposons que nous comaissons un point $G \in E(\mathbb{F}_q)$ ainsi que son ordre $l \in \mathbb{N}$, alors si $l \succ \frac{q+1}{2} + \sqrt{q}$, le thérème de Hasse-Weil montre que le groupe $E(\mathbb{F}_q)$ est cyclique engendré par G et que ce groupe est d'ordre l.

Remarque 3.3 L'utilisation directe de ce pocédé est cependant assez rare car, en principe, on calcule d'abord l'ordre du groupe $E(\mathbb{F}_q)$ et on l'utilise pour trouver l'ordre du point G. La détermination du nombre de points $\mathbb{F}_q$-rationnels sur E est une problème important pour le logarithme discret et pour d'autre application (test de primalité, factorisation,etc).

Exemple 3.3 On considère la courbe E donneé par une équation de Weierstrass courte :
$y^2 = x^3 + ax^2 + bx + c$ sur $\mathbb{F}_q$ (donc implicitement on a *car* $k \neq 2$), la formule : $|E(\mathbb{F}_q)| = p + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3+ax^2+bx+c}{q}\right)$
permet de calculer $|E(\mathbb{F}_q)|$ avec une complexité $O(q^{1+\varepsilon})$ (le "ε" prenant en compte la complexité des opérations élémentaires dans $\mathbb{F}_q$ ainsi que celle du calcul du symbole de Lengendre). Une adaptation finie de la méthode "Baby steps-Giant steps" permet de calculer $|E(\mathbb{F}_q)|$ avec une complexité $O\left(q^{1/2+\varepsilon}\right)$. Des méthodes récentes trés sophitiquées permettent d'obtenir $|E(\mathbb{F}_q)|$ avec une complexité on $O\left(\log(q)^{2+\mu}\right)$ où μ est donnée par la complexité multiplication dans $\mathbb{F}_q$.

3.2 Courbes elliptiques sur le corps $\mathbb{F}_{2^n}, n \geq 1$

Definition 39 Il existe deux formes simpliées de l'équation de Weierstrass de les courbes élliptiques définies sur $\mathbb{F}_{2^n}, n \geq 1$:
$y^2 + xy = x^3 + a_2x^2 + a_6 \mod(2^n)$
$y^2 + a_3y = x^3 + a_4x + a_6 \mod(2^n)$
où a_2, a_3, a_4 et $a_6 \in \mathbb{F}_{2^n}$.

Proposition 3.3 *Soit $E(\mathbb{F}_{2^n})$ une courbe elliptique définie sur le corps $\mathbb{F}_{2^n}$. On a,*

1. Si $P(x_P, y_P) \in E(\mathbb{F}_{2^n})$, alors son opposé $Q(x_Q, y_Q)$ où $\begin{cases} x_Q = x_P \\ y_Q = x_P + y_P \end{cases}$.

2. Si $P(x_P, y_P), Q(x_Q, y_Q) \in E(\mathbb{F}_{2^n})$, alors $P + Q = R(x_R, y_R)$, avec

$$\begin{cases} x_R = \lambda^2 + \lambda + a_2 + x_P + x_Q \\ y_R = (\lambda + 1)\, x_R + \lambda x_P + y_P \end{cases}$$

$$où \begin{cases} \lambda = \frac{y_P + y_Q}{x_P + x_Q} \ si\ x_P \neq x_Q \\ \lambda = \frac{x_P^2 + y_P}{x_P} \ si\ x_P = x_Q \end{cases}$$

Exemple 3.4 Soit le corps $\mathbb{F}_{2^4} = \frac{\mathbb{F}_2[x]}{\langle x^4+x+1\rangle} = \{x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3, (x_0, x_1, x_2, x_3) \in \mathbb{F}_2^4\}$, où α est une racine du polynôme $x^4 + x + 1$ irréductible sur $\mathbb{F}_{2^4}$. On considère l'équation de Weierstrass $y^2 + xy = x^3 + (\alpha + 1)x^2 + 1 \mod(2^4)$.
Le point $P(1, \alpha^3 + \alpha^2) \in E(\mathbb{F}_{2^4})$, on a ,
$2P(0, 1)$ et $3P(1, \alpha^3 + \alpha^2 + 1)$.

3.3 Recherche des points rationnels

Pour donner un problème de logarithme discret à base d'une courbe elliptique $E/\mathbb{F}_q$, il faut avoir un point $\mathbb{F}_q$-rationnele sur E possédant, si possible, un grand ordre premier. Supposons, pour simplifier l'exposer, que *car* $\mathbb{F}_q \geq 3$ et que la courbe E est définie par $y^2 = x^3 + ax^2 + bx + c$

Pour trouver un point $P \in E(\mathbb{F}_q)$, on choisit un élément x dans $\mathbb{F}_q$ tel que $A = x^3 + ax^2 + bx + c$ est un carré dans $\mathbb{F}_q$. Alors, le point $P = (x, y)$, où y est une racine carré de A dans $\mathbb{F}_q$, est une racine carrée de A dans $\mathbb{F}_q$, est bien un point de $E(\mathbb{F}_q)$.

Toute le problème consiste donc à pouvoir extraire une racine carrée dans un corps fini. Remarquons que si le corps est $\mathbb{F}_{2^r}$ alors tout élément $x \in \mathbb{F}_{2^r}$ est trivialement le carré de $x^{2^{m-1}}$.

Algorithme

1. Entreés : un corps $\mathbb{F}_q$ de caracteristique $P \geq 3$, un élément $A \in \mathbb{F}_q$.
2. Sortie : $r \in \mathbb{F}_q$ tel que $r^2 = A$ (s' il existe).

E′tap 1 : faire $\varepsilon \leftarrow \left(\frac{A}{q}\right)$.

Si $\varepsilon = -1$ alors A n'est pas un carré dans $\mathbb{F}_q$: fini .

Si $\varepsilon = 0$, sortir $r = 0$: fini .

E′tap 2 : Choisir un élément $B \in \mathbb{F}_q$ tel que $\left(\frac{B^{2-}-4A}{q}\right) = -1$.

E′tap 3 : Dans le corps $\mathbb{F}_q[\theta]$ $(\simeq \mathbb{F}_{q^2})$ où θ vérifie $\theta^2 - B\theta + A = 0$, faire $r \leftarrow \theta^{(q+1)/2}$.

Retourner r (ou $-r$).

Le choix de B dans l'étape 2 est probabiliste. Cependant, pour chaque élément $B \in \mathbb{F}_q$, on peut espérer qu'il ya, à peu près, une chance sur deux pour qu'un B pris au hasard convienne .Cette algorithme nécessite alors $O(\log\ q)$ multiplication dans $\mathbb{F}_q$ (essentiellment, des élevations à la puissance $\approx q/2$): autant que nécessaires pour trouver B et une pour calculer r. Pour montrer la validité l'algorithme, il suffit juste de vérifier que $r^2 = A$. On a

$r^2 = \theta^{q+1}$ et on peut écrire :

$\theta = \frac{b+\delta}{2}$

où $\delta^2 = B^2 - 4A \in \mathbb{F}_q[\theta]$ .Si σ_q désigne l'automorphisne de Frobenius, o na $\sigma_q\delta = -\delta$ car $\sigma_q\delta$ est aussi une racine carée de $B^2 - 4A$ et $\delta \neq \sigma_q\delta$ (sinon $B^2 - 4A$ serait un carré dans $\mathbb{F}_q$) .

On peut aussi voir cela en utilisant directement l'experesion du symbole de lengendre :

$-1 = \left(\frac{B^2-4A}{q}\right) = (B^2 - 4A)^{\frac{q-1}{2}} = \delta^{q-1}$ donc $\delta^q = -\delta$

Ceci étant, on a alors :

$\theta^{q+1} = \left(\frac{b+\delta}{2}\right)^{q+1} = \left(\frac{b+\delta}{2}\right)^q \left(\frac{b+\delta}{2}\right) = \left(\frac{b^q+\delta^q}{2^q}\right) \left(\frac{b+\delta}{2}\right) = \left(\frac{b-\delta}{2}\right) \left(\frac{b+\delta}{2}\right) = \left(\frac{b^{2--}\delta^2}{4}\right) = A.$

Exemple 3.5 On pose $p = 100003$, et on cherche la racine carréE de 69. Tout d'abord,

$\left(\frac{69}{p}\right) = 69^{500016} = 1$

et 69 est bien carrée dans $\mathbb{F}_p$. Ensuite, on essaie $B = 0, 1, 2, ...$jusqu'à ce que $B^2 - 4A$ ne soit pas un carrée dans $\mathbb{F}_p$: la valeur $B = 6$ convient . Dans le corps $\mathbb{F}_p[\theta]$,

où $\theta^2 - 6\theta + 69 = 0$, on calcule $\theta^{(p+1)/2}$ est on trouver 736476, qui est bien une racine carrée de 69 dans $\mathbb{F}_p$.

Lorsque $q \equiv 3$, 5 ou $7 \pmod 8$, on peut éviter d'avoir recours à l'extension quadratique $\mathbb{F}_{q^2}/\mathbb{F}_p$, en efet :

Proposition 3.4 *On a : Si* $q \equiv 3 \pmod 4$ *et si* A *est une carrée dans* $\mathbb{F}_q$ *alors* $A^{(q+1)/4}$ *est une racins carrée de* A.

Si $q \equiv 5 \pmod 8$ et si A est un carrée dans $\mathbb{F}_q$, on pose $d = A^{(p-1)/4}$. Si $d = 1$ alors $r = A^{(q+3)/8}$ est une racine de A dans $\mathbb{F}_q$.Si $d = -1$ alors $r = 2A(4A)^{(p-5)/8}$ est une racine de A dans $\mathbb{F}_q$.

Th■or■me 3.5 (*Nagell -lutz*) .*Si un point* $(x, y) \in E(\mathbb{Q})$ *et de torsion, alors celui-ci possède de coordonnées entières. De plus, soit* $y = 0$, *ou soit* y *divise le discriminant* Δ *de la courbe.*

Nous allons prouver partiellement le théorème à l'aide de quelques lemmes pour donner une idée du processus et nous indiquerons commment terminer la preuve. Tout d'abord, rappelons que pour un point P rationnel sur une courbe de la forme

$E : y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Z}$

nous avons que si $\mathbb{Q} = 2P$,alors,

$x(Q) = \frac{4x(P)y(P)^2 - \left(3x(P)^4 + 6Ax(P)^2 + 12Bx(P) - A^2\right)}{4y(P)^2}$

$y(Q) = \frac{x(P)^6 + 5Ax(P)^4 + 20Bx(P)^3 - 5A^2x(P)^2 - 4ABx(P) - ()B^2 - A^3}{()y(P)^3}$

par les formules d'addition explicites [Cas91] .Les lemmes suivant s'imposent.

Lemme 3.1 ([*Si109*]) .*Si* $2P = \mathcal{O}$, *alors* $x(P), y(P) \in \mathbb{Z}$.

Preuve. Par les formules ci-dessus, nous voyans que $y(P) = 0$.Ainssi, par substitituon directe. $x(P)^3 + Ax(P) + B = 0$.

Puisque le polynôme et unitaire de $\mathbb{Z}[x]$, $x(P) \in \mathbb{Z}$. ■

Lemme 3.2 ([*Cas91*]). *E'tant donné un point* P *d'ordre fini* ≥ 3, *si* $x(P)$, $y(P)$, $x(2P) \in \mathbb{Z}$.

Preuve. Comme montré par cassels , nous avons que

$x(2P) = \frac{\left(3x(P)^2+A\right)}{4y(P)^2} - 2x(P)$.

De plus, puisque $x(2P)$ entntier, $y(P) = x(P)^3 + Ax(P) + B$ divise $\left(3x(P)^2 + A\right)^2$. Mais,

$4A^3 + 27 = \left(6Ax(P)^2 - 9Bx(P) + 4A^2\right)$
$\left(3x(P)^2 + A\right)^2 - (18Ax(P) - 27b)(x(P) + Ax(P) + B)$

et donc , $y(P)$ divise les deux côtés de l'égalité. Ceci montre ainsi que $y(P) \mid \Delta$.

Pour terminer la preuve du théorème de Nagell-Lutz, il ssuffit donc de montrer que $x(P)$ et $y(P)$ sont entiers. Dans son livre, Cassels procède en utilisant le principe local global. Nous

n'effectuerons pas ceci ici puisque nous devrions introduire les nombres $P-$adics pour présenter une preuve. Nous référons à son couvrage [Cas91] contenant tout le matériel nécessaire.

De plus, il existe une caractérisation non triviale des sous-groupes de torsion pour certaines formes de courbe particulièrs. ■

Conclusion

Dans ce mémoire, on a fait une étude sur les courbes elliptiques.

Nous avons présenté dans le premier chapitre les définitions et quelques propriétés sur les groupes, les anneaux et les corps finis.

Ensuite nous avons fait une étude sur les courbes elliptiques définies sur $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$.

Finalement nous avons étudé le cardinal de points rationnels sur un corp fini.

Bibliographie

[1] C. Berenfeld, L. Lerer, M. Tamiozzo, Multiplication Complexe, (2015)

[2] A. DAOUI, "Courbe elliptique de rang 1", Université de constantine, (2010).

[3] A.KRAUSS, "Cours des cryptographie", Université Pierre et Marie Curne, (2009).

[4] A. MORRA, "Théorie et Pratique de la méthode des pointsde Heegner", Université Bordeaux (2006).

[5] A. TROESCH, "Cours de mathématique Partie III algèbre", Lycie Louis -Le-Gand, (2017).

[6] B. AMINA et M. LEYLA, "Etude sur les automorphismes de groupe : Application sur les code", Université de M'sila, (2017).

[7] B. SOUAD, "Introduction aux courbe elliptique", Université de Djilali - Bounaâma, (2016).

[8] CH. M. MARLE et PH. PILIBOSSIAN, "Extension de Corps- Théories de Galois", Université de Remies-Champagne-Arderne, (2006).

[9] D. ARNOLD MOLDOVAN, "Cryptographie et courbes elliptiques", E'cole Polytechnique Fédérale de Laussane, (2011).

[10] E. PEYRE , "Corps fini et courbe elliptique", (2014).

[11] E. WEGRZ YNOWSKI, "Corps fini, Licence et Master mension informatique", (2000).

[12] J. FRANÇOIS-DAT, "Algèbre II, Anneaux -module, Théorie de Galois", E'cole Normale Séperieure, (2018).

[13] H.RANDRIAM, "Resumé de cours sur les courbe elliptique", (2015).

[14] T.HAMAIZIA, "Groupe de torsion de courbe elliptique sur une Extension quadratique du corps ∞ ", Université de constantine, (2011).