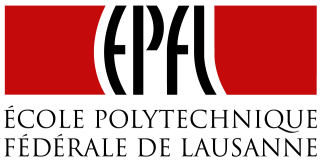

SMA

Projet de semestre

Cryptographie et courbes elliptiques

Thierry Favre

Sous la direction de la Prof. Eva Bayer Fluckiger

Assistant : Daniel Arnold Moldovan

Lausanne, le 31 mai 2011

Table des matières

1 Introduction

Le but de ce projet est d'introduire les notions de bases des courbes elliptiques puis de présenter l'article de Menezes, Okamoto et Vanstone concernant la réduction du problème du logarithme discret sur le groupe d'un certain type de courbes elliptiques définies sur un corps fini au problème du logarithme discret sur le groupe multiplicatif d'un certain corps fini. Les courbes elliptiques sont des courbes algébriques de genre 1. Nous allons donc, dans le premier chapitre, définir et étudier les notions de courbe et de genre d'une courbe. Le premier chapitre se termine par le théorème de Riemann-Roch qui permet de définir (et de calculer) le genre d'une courbe algébrique.

Le deuxième chapitre traite des courbes elliptiques. Nous allons commencer par montrer qu'une courbe elliptique est définie par les solutions d'une équation cubique à deux variables, puis nous nous servirons de cette correspondance pour mettre une structure de groupe sur les courbes elliptiques. Nous parlerons ensuite des isogénies entre courbes elliptiques. Puis, nous définirons le couplage de Weil qui servira pour la réduction décrite dans l'article de Menezes, Okamoto et Vanstone. Nous terminerons par donner quelques résultats sur les corps finis, par exemple une borne sur le nombre d'élément d'une courbe elliptique sur un corps fini et une classification des courbes dites supersingulières.

Dans le troisième chapitre, nous parlerons des applications des courbes elliptique à la cryptographie et nous expliquerons comment certaines méthodes classiques de cryptographie peuvent être adaptées pour fonctionner sur des courbes elliptiques, par exemple le protocole d'échange de clé de Diffie-Hellman.

Le dernier chapitre parlera de l'article de Menezes, Okamoto et Vanstone et donnera un algorithme probabiliste en temps polynomial pour la réduction du problème du logarithme discret sur des courbes elliptiques au problème du logarithme discret sur le groupe multiplicatif d'un corps fini.

2 Courbes algébriques

Comme une courbe elliptique est une variété projective de dimension et de genre 1, nous allons définir et donner des exemples de ces notions de géométrie algébrique classique. Nous parlerons d'abord des variétés affines et projectives puis des courbes algébriques (qui sont des variétés projectives de dimension 1). Nous terminerons ce chapitre en énonçant le théorème de Riemann-Roch qui définit la notion de genre d'une courbe lisse.
Soit K un corps. Pour un corps F, on fixe $\bar{F}$ une de ses clôtures algébriques.

2.1 Variétés affines

Définition 2.1 (L'espace affine de dimension n sur K)
L'espace affine de dimension n sur K est l'ensemble des n-tuples

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{(x_1, \ldots, x_n) : x_i \in \bar{K}\}.$$

Les points K-rationnels de $\mathbb{A}^n$ sont les points de l'ensemble

$$\mathbb{A}^n(K) = \{(x_1, \ldots, x_n) \in \mathbb{A}^n : x_i \in K\}.$$

Soit $\bar{K}[X] = \bar{K}[X_1, \ldots, X_n]$ l'anneau des polynômes à n variables et à coefficients dans $\bar{K}$ et $I \subset \bar{K}[X]$ un idéal. On associe à I un sous-ensemble de $\mathbb{A}^n$ en posant

$$V(I) = \{P \in \mathbb{A}^n : f(P) = 0 \text{ pour tout } P \in I\}.$$

Définition 2.2 (Ensemble algébrique affine)
Un ensemble algébrique affine est un ensemble de la forme $V(I)$, où I est un idéal de $\bar{K}[X]$.

Exemples 2.3 (i) Soient $f(X) = X^2 - 1 \in \mathbb{C}[X]$ et $I = \langle f \rangle$. Alors, $V(I) = \{-1, 1\}$.

(ii) Soient $K = \mathbb{F}_7, f(X) = X^2 - 1 \in K[X]$ et $I = \langle f \rangle$. Alors, $V(I) = \{1, 6\}$.

(iii) Soient $K = \mathbb{F}_p$, où p est un premier, $d \in \mathbb{N}, f(X) = X^{p^d} - X \in K[X]$ et $I = \langle f \rangle$. Alors, $V(I) = \mathbb{F}_{p^d}$.

Soit $V \subset \mathbb{A}^n$ un ensemble algébrique affine.

Définition 2.4 (Idéal d'un ensemble algébrique affine)
L'idéal d'un ensemble algébrique affine V est l'ensemble

$$I(V) = \{f \in \bar{K}[X] : f(P) = 0 \text{ pour tout } P \in V\}.$$

On vérifie qu'il s'agit bien d'un idéal. On défini de plus l'idéal $I(V/K)$ par

$$I(V/K) = \{f \in K[X] : f(P) = 0 \text{ pour tout } P \in V\} = I(V) \cap K[X].$$

Exemples 2.5 (i) Soit $V = \{-1, 1\} \subset \mathbb{C} = \mathbb{A}^1$. Alors, $I(V) = \langle X^2 - 1 \rangle \subset \mathbb{C}[X]$.

(ii) Soit $V = \{1, 6\} \subset \mathbb{F}_7$. Alors, $I(V) = \langle X^2 - 1 \rangle \subset \bar{\mathbb{F}}_7[X]$ et $I(V/\mathbb{F}_7) = \langle X^2 - 1 \rangle \subset \mathbb{F}_7[X]$.

(iii) Soient p un nombre premier, $d \in \mathbb{N}$ et $V = \mathbb{F}_{p^d} \subset \bar{\mathbb{F}}_p$. Alors, $I(V) = \langle X^{p^d} - X \rangle \subset \bar{\mathbb{F}}_p[X]$.

Définition 2.6
On dit qu'un ensemble algébrique V est *défini sur K* si $I(V)$ peut être généré par des polynômes à coefficients dans K. On le note alors V/K. Soit V un ensemble algébrique défini sur K. On définit les *points K-rationnels* de V par $K(V) = V \cap \mathbb{A}^n(K)$.

Définition 2.7 (Variété affine)
Une variété affine est un ensemble algébrique affine tel que $I(V)$ est un idéal premier de $\bar{K}[X]$.

Exemples 2.8 (i) Aucun des ensembles algébriques définis dans l'exemple 2.3 ne sont des variétés affines. En effet, leurs idéaux ne sont pas premiers.

(ii) Soit $I = \langle X-1, Y-1\rangle \subset \mathbb{C}[X,Y]$. Alors, $V(I) = \{(1,1)\} \subset \mathbb{A}^2$, et donc $I(V) = I$ qui est premier. Ainsi, $V = \{(1,1)\}$ est une variété affine.

(iii) Soient $f(X) = X^2 + X + 1 \subset \mathbb{F}_2[X]$ et $\alpha \in \bar{\mathbb{F}}_2$ tel que $\alpha^2 = \alpha + 1$. Alors,

$$\mathbb{F}_2[X]/\langle f\rangle \cong \mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$$

car f est irréductible dans $\mathbb{F}_2[X]$. Posons $I = \langle f\rangle$. Alors $V = V(I) = \{\alpha, \alpha+1\} \subset \bar{\mathbb{F}}_2, I(V) = I$ et $I(V/\mathbb{F}_2) = \langle f\rangle \subset \mathbb{F}_2[X]$. Puisque f est irréductible, V est une variété affine.

Définition 2.9 (Anneau de coordonnée affine de V/K)
Soit V/K une variété affine définie sur K. L'anneau de coordonnée affine de V/K est alors $K[V] = K[X]/I(V/K)$. Comme $I(V/K)$ est un idéal premier, $K[V]$ est un anneau intègre. Le corps des fractions de $K[V]$, noté $K(V)$, est appelé *corps des fonctions de* V/K. On définit $\bar{K}[V]$ et $\bar{K}(V)$ de manière similaire, en remplaçant K par $\bar{K}$.

Exemples 2.10 (i) Soit V la variété affine $V = \{(1,1)\} \subset \mathbb{A}^2(\mathbb{C})$. Alors,

$$\mathbb{C}[V] = \mathbb{C}[X,Y]/\langle X-1, Y-1\rangle \cong \mathbb{C}.$$

(ii) Soit $V = \{\alpha, \alpha+1\} \subset \bar{\mathbb{F}}_2$ l'ensemble défini au point (*iii*) de l'exemple 2.8. Alors,

$$I(V/\mathbb{F}_2) = \langle X^2 + X + 1\rangle \subset \mathbb{F}_2[X].$$

Ainsi, on a $\mathbb{F}_2[V] = \mathbb{F}_2[X]/\langle X^2 + X + 1\rangle \cong \mathbb{F}_4$.

Définition 2.11 (Dimension d'une variété affine)
Soit V une variété affine. La *dimension de* V, notée $\dim(V)$, est le degré de transcendance de $\bar{K}(V)$ sur $\bar{K}$.

Exemple 2.12
La dimension de $\mathbb{A}^n$ est n, puisque $\bar{K}[\mathbb{A}^n] = \bar{K}[X_1, \ldots, X_n]$. Si $V \subset \mathbb{A}^n$ est engendré par un seul polynôme non-constant, alors $\dim(V) = n-1$.

Comme $\bar{K}[X]$ est noethérien, l'idéal $I(V)$ est de génération finie.

Définition 2.13 (Variété affine lisse)
Soient $V \subset \mathbb{A}^n$ une variété affine, $P \in V$ et $f_1, \ldots, f_m \in \bar{K}[X]$ des polynômes tels que $I(V) = \langle f_1, \ldots, f_m\rangle$. On dit que V est *lisse* ou *non-singulière en* P ou encore que P *est un point lisse de* V si la matrice

$$\left(\left(\frac{\partial f_i}{\partial X_j}\right)(P)\right)_{1\le i\le m, 1\le j\le n}$$

est de rang $n - \dim(V)$. On dit que V est *lisse* ou *non-singulière* si tous ses points sont lisses.

Exemples 2.14
Soit $V \subset \mathbb{A}^n$ engendré par un seul polynôme non constant f. Comme $\dim(V) = n-1$, on a que $P \in V$ est singulier si et seulement si

$$\frac{\partial f}{\partial X_i}(P) = 0$$

pour tout $i = 1, \ldots, n$. On va utiliser cette caractérisation dans les deux exemples suivants :

(i) Soit $V_1 = V_1(I) \subset \mathbb{A}^2(\mathbb{R})$, où $I = \langle Y^2 - X^3 - X \rangle \subset \mathbb{C}[X, Y]$. Alors, un point singulier de V_1 doit satisfaire $3X^2 + 1 = 2Y = 0$ qui n'as pas de solutions dans $\mathbb{R}$ et donc V_1 est lisse.

(ii) Soit $V_2 = V_2(I) \subset \mathbb{A}^2(\mathbb{R})$, où $I = \langle Y^2 - X^3 - X^2 \rangle \subset \mathbb{C}[X, Y]$. Alors, un point singulier de V_2 doit satisfaire $3X^2 + 2X = 2Y = 0$ qui ne possède que $x = 0, y = 0$ comme racine réelle et donc V_2 possède un unique point singulier, à savoir $(0, 0)$.

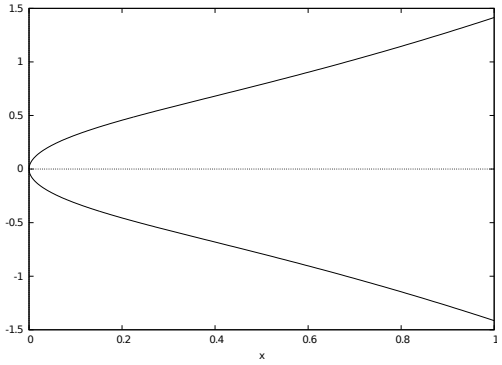

FIGURE 1 – La courbe lisse $Y^2 = X^3 + X$

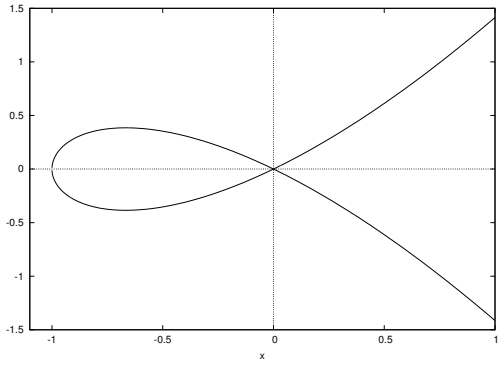

FIGURE 2 – La courbe $Y^2 = X^3 + X^2$

Soit V une variété affine et $P \in V$. Définissons $M_P = \{f \in \bar{K}[V] : f(P) = 0\}$. C'est un idéal maximal de $\bar{K}[V]$ puisqu'on a l'isomorphisme suivant

$$\begin{aligned} \theta : \bar{K}[V]/_{M_P} &\longrightarrow \bar{K} \\ f + M_P &\longmapsto f(P). \end{aligned}$$

Définition 2.15 (Anneau local)
Soient V une variété affine et $P \in V$. *L'anneau local de V en P*, noté $\bar{K}[V]_P$, est la localisation de $\bar{K}[V]$ en M_P, autrement dit,

$$\bar{K}[V]_P = \left\{ \frac{f}{g} : f, g \in \bar{K}[V], g(P) \neq 0 \right\}.$$

Les fonctions de $\bar{K}[V]_P$ sont dites *régulières en P* ou *définies en P*. En effet, si on considère $F = \dfrac{f}{g} \in \bar{K}[V]_P$, alors $F(P) = \dfrac{f(P)}{g(P)}$ est bien défini.

2.2 Variétés projectives

Définition 2.16 (Espace projectif de dimension n sur K)
L'espace projectif de dimension n sur K, noté $\mathbb{P}^n(\bar{K})$ ou juste $\mathbb{P}^n$ si cela n'est pas ambigu, est l'ensemble $(\mathbb{A}^{n+1} \backslash \{(0, \ldots, 0)\})/_\sim$, où $\sim$ est la relation d'équivalence définie par $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ si et seulement s'il existe $\lambda \in \bar{K}^*$ tel que $(y_0, \ldots, y_n) = \lambda(x_0, \ldots, x_n)$. Une classe d'équivalence de cette relation $\{(\lambda x_0, \ldots, \lambda x_n) : \lambda \in \bar{K}^*\}$ se note $[x_0, \ldots, x_n]$. *Les points K-rationnels* de $\mathbb{P}^n$ sont les points de l'ensemble $\mathbb{P}^n(K)$ qui contient tout les points dont il existe un représentant $[x_0, \ldots, x_n] \in \mathbb{P}^n$ tel que $x_i \in K$ pour tout $i = 1, \ldots, n$.

Définition 2.17 (polynôme homogène)
Soit $d \in \mathbb{N}$. Un polynôme $f \in \bar{K}[X] = \bar{K}[X_0, \ldots, X_n]$ est dit *homogène de degré d* si

$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n)$$

pour tout $\lambda \in \bar{K}$. Un idéal de $\bar{K}[X]$ est dit *homogène* s'il est généré par des polynômes homogènes.

Soit I un idéal homogène de $\bar{K}[X]$. Notons $V(I)$ l'ensemble

$$V(I) = \{P \in \mathbb{P}^n : f(P) = 0 \text{ pour tout polynôme homogène } f \in I\} \subset \mathbb{P}^n.$$

Remarquons qu'il est pertinent de parler de $f(P) = 0$ puisque f est homogène et donc si $P \sim P'$, alors $f(P) = 0$ si et seulement si $f(P') = 0$.

Définition 2.18 (Ensemble algébrique projectif)
Un ensemble algébrique projectif est un ensemble de la forme $V(I)$, où I est un idéal homogène.

Exemple 2.19
Soit $I = \langle XY^2 - X^3 \rangle \subset \mathbb{C}[X, Y]$. Alors, $V(I) = \{[0, 1], [1, 1], [1, -1]\} \subset \mathbb{P}^1(\mathbb{C})$.

Soit $V \subset \mathbb{A}^n$ un ensemble algébrique projectif.

Définition 2.20 (Idéal d'un ensemble algébrique (projectif))
L'idéal homogène d'un ensemble algébrique (projectif) V est l'ensemble

$$I(V) = \{f \in \bar{K}[X] : f \text{ homogène et } f(P) = 0 \text{ pour tout } P \in V\}.$$

Exemple 2.21
Soit $V = \{[0, 1], [1, 1]\} \subset \mathbb{P}^1(\mathbb{C})$. Alors, $I(V) = \langle XY - X^2 \rangle \subset \mathbb{C}[X, Y]$.

Définition 2.22
Un ensemble algébrique V est dit *défini sur* K si $I(V)$ peut être généré par des polynômes homogènes à coefficients dans K. On le note alors V/K. Soit V un ensemble algébrique défini sur K. On définit les *points K-rationnels* de V par $K(V) = V \cap \mathbb{P}^n(K)$.

Définition 2.23 (Variété projective)
Une variété projective est un ensemble algébrique projectif tel que $I(V)$ soit un idéal homogène premier de $\bar{K}[X]$.

Exemple 2.24
Soit $V_1 = \{[0, 1], [1, 1]\} \subset \mathbb{P}^1(\mathbb{C})$. Alors, $I(V_1) = \langle XY - X^2 \rangle \subset \mathbb{C}[X, Y]$ n'est pas premier et donc V_1 n'est pas une variété projectif. Par contre, si $V_2 = \{[1, 1]\} \subset \mathbb{P}^1(\mathbb{C})$, alors

$$I(V_2) = \langle X - Y \rangle \subset \mathbb{C}[X, Y]$$

est premier et donc V_2 est une variété projective.

Définition 2.25 (Hyperplan)
Un hyperplan de $\mathbb{P}^n$ est un ensemble algébrique H défini par l'équation $a_0X_0 + \ldots + a_nX_n = 0$, où les $a_0, \ldots, a_n$ appartiennent à $\bar{K}$ et ne sont pas tous nuls. Si $n = 2$, on appelle H une *droite*.

Remarquons maintenant que $\mathbb{A}^n$ peut être plongé dans $\mathbb{P}^n$ de plusieurs manières différentes. En effet, pour $i = 0, \ldots, n$ on définit le plongement

$$\begin{aligned} \varphi_i : \mathbb{A}^n &\longrightarrow \mathbb{P}^n \\ (x_1, \ldots, x_n) &\longmapsto [x_1, \ldots, x_{i-1}, 1, x_i, \ldots, x_n]. \end{aligned}$$

Soient $H_i = \{[x_0, \ldots, x_n] \in \mathbb{P}^n : x_i = 0\}$ l'hyperplan défini par $X_i = 0$ et $U_i = \mathbb{P}^n \setminus H_i$. On définit encore

$$\begin{aligned} \psi_i : U_i &\longrightarrow \mathbb{A}^n \\ [x_0, \ldots, x_n] &\longmapsto \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i} \right). \end{aligned}$$

Remarquons que pour $[x_0, \ldots, x_n] \in U_i$, la fraction $\dfrac{x_j}{x_i}$ est bien définie et que $\psi_i = \varphi_i^{-1}$ si on corestreint φ_i à $\operatorname{im} \varphi_i = U_i$. Fixons un $i \in \{0, \ldots, n\}$. Ainsi, nous pouvons identifier $\mathbb{A}^n$ avec $U_i \subset \mathbb{P}^n$ par l'application φ_i.
Soient V un ensemble algébrique projectif et $I(V)$ son idéal homogène. Alors, l'ensemble $\varphi_i^{-1}(V \cap U_i)$, que l'on note aussi $V \cap \mathbb{A}^n$, est un ensemble algébrique affine et son idéal $I(V \cap \mathbb{A}^n)$ est donné par

$$I(V \cap \mathbb{A}^n) = \{f(Y_0, \ldots, Y_{i-1}, 1, Y_{i+1}, \ldots, Y_n) : f(X_0, \ldots, X_n) \in I(V)\}.$$

Le fait de remplacer le polynôme $f(X_0, \ldots, X_n)$ par $f(Y_0, \ldots, Y_{i-1}, 1, Y_{i+1}, \ldots, Y_n)$ est appelé *déshomogénéisation par rapport à X_i*. Ce procédé possède un inverse appelé *homogénéisation de f par rapport à X_i* : pour tout $f(X) \in \bar{K}[X]$, on définit

$$f^*(X_0, \ldots, X_n) = X_i^{\deg f} f\left(\frac{X_0}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \ldots, \frac{X_n}{X_i}\right),$$

qui est homogène. En effet,

$$\begin{aligned} f^*(\lambda X_0, \ldots, \lambda X_n) &= \lambda^{\deg f} X_i^{\deg f} f\left(\frac{\lambda X_0}{\lambda X_i}, \ldots, \frac{\lambda X_{i-1}}{\lambda X_i}, \frac{\lambda X_{i+1}}{\lambda X_i}, \ldots, \frac{\lambda X_n}{\lambda X_i}\right) \\ &= \lambda^{\deg f} f^*(X_0, \ldots, X_n). \end{aligned}$$

Définition 2.26 (Clôture projective)
Soient V un ensemble algébrique affine et $I(V)$ son idéal. On peut considérer V comme sous-ensemble de $\mathbb{P}^n$ en identifiant V avec son image $\varphi_i(V)$ pour un i fixé. *La clôture projective* de V, notée $\bar{V}$, est l'ensemble algébrique projectif dont l'idéal homogène est généré par

$$\{f^*(X) : f \in I(V)\}.$$

Remarque 2.27
Notons que $V(I(V)) = V$ pour tout ensemble algébrique affine ou projectif et donc la clôture projective d'un ensemble algébrique affine est bien définie.

Proposition 2.28
Soient V une variété affine et W une variété projective. Alors,

(*i*) *$\bar{V}$ est une variété projective et $V = \bar{V} \cap \mathbb{A}^n$.*

(*ii*) *$W \cap \mathbb{A}^n$ est une variété affine et on a soit $W \cap \mathbb{A}^n = \emptyset$, soit $\overline{W \cap \mathbb{A}^n} = W$.*

(*iii*) *Si V, respectivement W, est défini sur K, alors $\bar{V}$, respectivement $W \cap \mathbb{A}^n$ est défini sur K.*

Démonstration. Pour les deux premiers points, voir [Har77] pages 9-12. Le dernier point est clair. □

Une variété affine peut ainsi être identifiée de manière unique avec une variété projective. Par abus de langage, la variété projective V définie par un polynôme f, pas nécessairement homogène, sera la clôture projective de la variété affine W définie par f. Considérons maintenant W comme sous-ensemble de $\mathbb{P}^n$. On appelle alors *points à l'infini sur V* les éléments de $V \setminus W$.

Exemple 2.29
Soit V la variété projective de $\mathbb{P}^2$ donnée par l'équation $Y^2 = X^3 + 17$. En effectuant le changement de variable $X' = \dfrac{X}{Z}$ et $Y' = \dfrac{Y}{Z}$, on trouve l'équation homogène $ZY'^2 = X'^3 + 17Z^3$. On trouve que $[0, 1, 0]$ est le seul point à l'infini de V. Cette variété est appelé *courbe elliptique*, c'est le premier exemple des objets dont nous allons parler plus loin.

Définition 2.30 (Dimension d'une variété projective)
Soit V/K une variété projective non vide et fixons i tel que $V \cap \mathbb{A}^n = \varphi_i^{-1}(V \cap U_i) \neq \emptyset$. *La dimension* de V est la dimension de $V \cap \mathbb{A}^n$.

Remarquons qu'un tel i doit exister car V est non vide. De plus, la définition est indépendante du choix de i. En effet, si $j \neq i$ est tel que $\varphi_j^{-1}(V \cap U_j) \neq \emptyset$, alors

$$\overline{\varphi_j^{-1}(V \cap U_j)} = V = \overline{\varphi_i^{-1}(V \cap U_i)},$$

par la proposition 2.28 et donc $\varphi_j^{-1}(V \cap U_j) = \varphi_i^{-1}(V \cap U_i)$.

Définition 2.31 (Variété projective lisse)
Soient V une variété projective, $P \in V$ et on fixe i tel que $P \in \mathbb{A}^n$. On dit que V est *lisse* ou *non-singulière en* P ou encore que P *est un point lisse de* V si $V \cap \mathbb{A}^n$ est non-singulière en P. On dit que V est *lisse* ou *non-singulière* si tous ses points sont lisses. *L'anneau local de* V *en* P, noté $\bar{K}[V]_P$, est l'anneau local de $V \cap \mathbb{A}^n$ en P. Une fonction $f \in K(V)$ est dite *régulière* ou *définie en* P si elle est dans $\bar{K}[V]_P$.

Exemple 2.32
Soit $V \subset \mathbb{P}^2(\mathbb{R})$ la variété projective définie par le polynôme $Y^2Z - X^3 - XZ^2$. Alors, V est la clôture projective de la variété lisse définie dans le point (ii) de l'exemple 2.14. Ainsi V est une variété projective lisse.

Remarquons que si f est régulière, alors $f(P)$ est bien définie.

Définition 2.33 (Application rationnelle)
Soient $V_1, V_2 \subset \mathbb{P}^n$ deux variétés projectives. Une application $\varphi : V_1 \to V_2$ est dite *rationnelle* s'il existe $f_0, \ldots, f_n \in \bar{K}(V_1)$ tels que φ soit de la forme $\varphi = [f_0, \ldots, f_n]$, où

$$[f_0, \ldots, f_n](P) = [f_0(P), \ldots, f_n(P)] \in V_2$$

pour tout point $P \in V_1$ tel que $f_i(P)$ soit défini pour tout $i \in \{0 \ldots, n\}$. S'il existe un $\lambda \in \bar{K}^*$ tel que $\lambda f_0, \ldots, \lambda f_n \in K(V)$, on dit que φ *est définie sur* K.

Exemple 2.34
Soient V_1 et V_2 les variétés projectives engendrées par $X-Y$, respectivement $X+Y \in \mathbb{C}[X, Y]$. Alors, $V_1 = \{[1, 1]\}$ et $V_2 = \{[1, -1]\}$. On définit $[f_0, f_1] : V_1 \to V_2$ en posant $f_0([x, y]) = 1$ pour tout $[x, y] \in V_1$ et $f_1([x, y]) = -1$ pour tout $[x, y] \in V_1$. Alors, $f_0, f_1 \in \mathbb{C}(V_1)$ et donc $[f_0, f_1]$ est une application rationnelle.

Définition 2.35 (Application régulière)
Soient $V_1, V_2 \subset \mathbb{P}^n$ deux variétés projectives. Une application rationnelle $\varphi = [f_0, \ldots, f_n] : V_1 \to V_2$ est dite *régulière* ou *définie en* P s'il existe une fonction $g \in \bar{K}(V_1)$ telle que gf_i soit régulier en P pour tout $i = 0, \ldots, n$ et s'il existe $j = 0, \ldots, n$ tel que $(gf_j)(P) \neq 0$. Pour un tel g, on pose $\varphi(P) = [(gf_0)(P), \ldots, (gf_n)(P)]$. Si φ est régulière en P pour tout $P \in C$, on dit que c'est un *morphisme (de variétés).*

Définition 2.36
Soient $V_1, V_2 \subset \mathbb{P}^n$ deux variétés projectives. On dit que V_1 et V_2 sont *isomorphes* et on note $V_1 \cong V_2$, s'il existe un morphisme $\varphi : V_1 \to V_2$ inversible tel que φ^{-1} soit aussi un morphisme. De plus, si V_1 et V_2 sont définis sur K, on dit qu'ils sont *isomorphes sur* K si φ et φ^{-1} sont définis sur K.

2.3 Courbes algébriques

Définition 2.37 (Courbe (algébrique))
Une courbe (algébrique) est une variété projective de dimension 1. On appelle les morphismes de variétés sur des courbes, des morphismes de courbes ou, tout simplement, morphismes.

Exemples 2.38 (i) Soit V la variété projective engendrée par $X - Y \in \mathbb{C}[X, Y]$. Alors, $I(V) = \langle X - Y \rangle$ et donc $\mathbb{C}(V_1) = \mathbb{C}[X, Y]/_{I(V)} \cong \mathbb{C}[X]$. Ainsi, V est de dimension 1 et est une courbe algébrique.

(ii) De même, la variété définie par l'équation $Y^2 = X^3 + 17$ est une courbe dans $\mathbb{P}^1(\mathbb{C})$.

Définition 2.39 (Valuation (normalisée))
Soient C une courbe et $P \in C$ un point lisse. La *valuation (normalisée)* sur $\bar{K}[V]_P$ est donnée par

$$\begin{aligned} \mathrm{ord}_P : \bar{K}[C]_P &\longrightarrow \mathbb{N}_0 \cup \{\infty\} \\ \frac{f}{g} &\longmapsto \sup\{d \in \mathbb{N}_0 : f \in M_P^d\}. \end{aligned}$$

Notons que $g \in \bar{K}[C] \setminus M_P = M_P^0 \setminus M_P$ et donc $\sup\{d \in \mathbb{N}_0 : g \in M_P^d\} = 0$.
De plus, on peut étendre ord_P à $\bar{K}(C)$ en posant $\mathrm{ord}_P\left(\frac{f'}{g'}\right) = \mathrm{ord}_P(f') - \mathrm{ord}_P(g')$ pour tous $f', g' \in K[C], g' \neq 0$. On appelle *paramètre uniformisant pour C en P* une fonction $t \in \bar{K}(C)$ telle que $\mathrm{ord}_P(t) = 1$, c'est-à-dire que t est un générateur pour M_P.

On vérifie que ord_P est bien une valuation discrète.

Définition 2.40
Soient C une courbe, $P \in C$ un point lisse et $f \in \bar{K}(C)$. *L'ordre de f en P* est défini comme étant $\mathrm{ord}_P(f)$. Si $\mathrm{ord}_P(f) \geq 0$, alors on dit que f est *régulier* en P, sinon on dit que f a un *pôle* en P. Si $\mathrm{ord}_P(f) > 0$, alors on dit que f a un *zéro* en P.

Si f est régulier en P, alors $f(P)$ est bien défini. Si non f a un pôle en P et on note $f(P) = \infty$. Remarquons que si f est régulier dans ce sens, alors il l'est aussi dans le sens défini dans la définition 2.35.

Proposition 2.41
Soient C une courbe lisse et $f \in \bar{K}(C)$. Alors, f n'as qu'un nombre fini de zéros et de pôles dans C. De plus, si f n'as pas de pôle, alors $f \in \bar{K}$.

Démonstration. Voir [Sil09], page 18. □

Proposition 2.42
Soient C une courbe définie sur K et $t \in K(C)$ un paramètre uniformisant en un point lisse $P \in C$. Alors, $K(C)$ est une extension séparable finie de $K(t)$.

Démonstration. Voir [Sil09], pages $18 - 19$. □

Proposition 2.43
Soient C une courbe, $V \subset \mathbb{P}^n$ une variété projective, $P \in C$ un point lisse et $\varphi : C \to V$ une application rationnelle. Alors, φ est régulière en P. En particulier, si la courbe C est lisse, alors φ est un morphisme.

Démonstration. Soit $t \in \bar{K}(C)$ un paramètre uniformisant de C en P. Comme φ est rationnelle, on peut l'écrire sous la forme $\varphi = [f_0, \ldots, f_n]$, où $f_0, \ldots, f_n \in \bar{K}(C)$. Posons

$$m := \min_{0 \leq i \leq n} \{\mathrm{ord}_P f_i\}.$$

Alors, $\mathrm{ord}_P(t^{-m} f_i) \geq 0$ pour tout $i = 0, \ldots, n$ et il existe un $j \in \{0, \ldots, n\}$ tel que $\mathrm{ord}_P(t^{-m} f_j) = 0$. Ainsi, $t^{-m} f_i$ est régulier pour tout $i = 0, \ldots, n$ et $t^{-m} f_j(P) \neq 0$, ce qui implique que φ est régulière en P. □

Proposition 2.44
Soit $\varphi : C_1 \to C_2$ un morphisme de courbes. Alors, φ est soit surjectif, soit constant.

Démonstration. Voir [Har77], page 137. □

Remarque 2.45
Soient C_1, C_2 deux courbes définies sur K et $\varphi : C_1 \to C_2$ un application non-constante définie sur K. Alors, la composition par φ induit une application injective qui fixe K,

$$\begin{aligned} \varphi^* : K(C_2) &\to K(C_1) \\ \varphi^* f &= f \circ \varphi. \end{aligned}$$

Théorème 2.46
Soient $C_1/K, C_2/K$ deux courbes définies sur K et $\varphi : C_1 \to C_2$ un application non-constante définie sur K. Alors, $K(C_1)$ est une extension finie de $\varphi^* K(C_2)$.

Démonstration. Voir [Har77], page 137. □

Définition 2.47 (Degré)
Soient $C_1/K, C_2/K$ des courbes et $\varphi : C_1 \to C_2$ une application définie sur K. On dit que le *degré de* φ est zéro si φ est constante, et égal à $\deg \varphi = [K(C_1) : \varphi^*(K(C_2))]$ sinon. On dit aussi que φ est *zéro*, respectivement *finie*.

2.3.1 Diviseurs

Soit C une courbe lisse sur un corps K.

Définition 2.48 (Groupe des diviseurs)
Le groupe des diviseurs de C, noté $\mathrm{Div}(C)$, est le groupe abélien libre généré par les points de C, c'est-à-dire qu'un diviseur $D \in \mathrm{Div}(C)$ est une somme formelle $D = \sum_{P \in C} n_P(P)$, où $n_P \in \mathbb{Z}$ et $n_P = 0$ sauf pour un nombre fini de $P \in C$.

Définition 2.49 (Degré d'un diviseur)
Le degré d'un diviseur D est $\deg D = \sum_{P \in C} n_P$.

Les diviseur de degré 0 forment un sous-groupe de $\mathrm{Div}(C)$ que l'on note $\mathrm{Div}^0(C)$. En effet, soient $x, y \in \mathrm{Div}^0(C)$. Alors, $x = \sum_{P \in C} n_P(P)$ et $y = \sum_{P \in C} m_P(P)$ avec $\sum_{P \in C} n_P = 0$ et $\sum_{P \in C} m_P = 0$, ainsi $x + y = \sum_{P \in C}(n_P + m_P)(P)$ et donc $\deg(x+y) = \sum_{P \in C} n_p + m_p = 0$.

Soit $f \in \bar{K}(C)^*$. Alors, on peut associer à f le diviseur

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P).$$

Remarquons que $\mathrm{div}(f)$ est bien un diviseur par la proposition 2.41. De plus, ord_P est une valuation, en particulier $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$ pour tous $f, g \in \bar{K}(C)^*$. Ainsi, $\mathrm{div} : \bar{K}(C)^* \to \mathrm{Div}(C)$ est un homomorphisme de groupes abéliens.

Proposition 2.50
Soient C une courbe lisse et $f \in \bar{K}(C)^*$.

(*i*) *Alors,* $\mathrm{div}(f) = 0$ *si et seulement si* $f \in \bar{K}^*$.

(*ii*) *On a* $\deg(\mathrm{div}(f)) = 0$.

Démonstration. (i) Si $f \in \bar{K}^*$, alors $f \notin M_P$ et donc $\mathrm{ord}_P(f) = 0$, pour tout $P \in C$. Réciproquement, si $\mathrm{div}(f) = 0$, alors $n_P(f) = 0$ pour tout $P \in C$, en particulier f n'as pas de pôles et donc par la proposition 2.41, $f \in \bar{K}^*$.

(ii) Voir [Har77], page 138.

□

Définition 2.51 (i) Un diviseur $D \in \mathrm{Div}(C)$ est dit *principal* si $D = \mathrm{div}(f)$ pour un $f \in \bar{K}(C)^*$.

(ii) On dit que deux diviseurs D_1 et D_2 sont *linéairement équivalents* et on note $D_1 \sim D_2$ si $D_1 - D_2$ est principal.

(iii) *Le groupe de Picard de C*, noté $\mathrm{Pic}(C)$, est le quotient de $\mathrm{Div}(C)$ par le sous-groupe des diviseurs principaux.

Notons que l'ensemble des diviseurs principaux est en effet un sous-groupe du groupe des diviseurs. Si D_1, D_2 sont des diviseurs principaux, on a $D_1 = \mathrm{div}(f_1)$ et $D_2 = \mathrm{div}(f_2)$ et donc $D_1 + D_2 = \mathrm{div}(f_1 f_2)$ et $-D_1 = \mathrm{div}(f_1^{-1})$. De plus, les diviseurs forment un sous-groupe de $\mathrm{Div}^0(C)$, par la proposition 2.50. On définit alors le *groupe de Picard de degré* 0 *de* C, noté $\mathrm{Pic}^0(C)$, comme étant le quotient de $\mathrm{Div}^0(C)$ par le sous-groupe des diviseurs principaux.

2.3.2 Théorème de Riemann-Roch

Soit C une courbe lisse sur un corps K.

Définition 2.52
L'espace des formes différentielles sur C, noté Ω_C, est le $\bar{K}(C)$-espace vectoriel généré par les symboles dx, où $x \in \bar{K}(C)$, tels que

(i) $d(x+y) = dx + dy$;

(ii) $d(xy) = xdy + ydx$;

(iii) $da = 0$,

pour tous $x, y \in \bar{K}(C)$ et tout $a \in \bar{K}$.

Proposition 2.53
Soient C une courbe et $x \in \bar{K}(C)$. Alors, Ω_C est de dimension 1 et dx en est une base si et seulement si $\bar{K}(C)$ est une extension séparable finie de $\bar{K}(x)$.

Démonstration. Voir [Sil09], pages $30 - 31$. □

Proposition 2.54
Soient $P \in C$ et $t \in \bar{K}(C)$ un paramètre uniformisant en P.

(i) Pour tout $\omega \in \Omega_C$, il existe une unique fonction $g \in \bar{K}(C)$, qui dépend de ω et de t, telle que $\omega = gdt$. On écrit aussi $\frac{\omega}{dt}$ à la place de g.

(ii) Soit $f \in \bar{K}(C)$ une fonction régulière en P. Alors, $\frac{df}{dt}$ est aussi régulière en P.

(iii) La valeur $\mathrm{ord}_P\left(\frac{\omega}{dt}\right)$ ne dépend que de ω et de P. On l'appelle alors ordre de ω *et on le note $\mathrm{ord}_P(\omega)$.*

(iv) L'ordre de ω est non-nul seulement pour un nombre fini de formes différentielles ω.

(v) Soient $x, f \in \bar{K}(C)$ avec $x(P) = 0$ et soit $p = \mathrm{Car}\, K$. Si $p = 0$ ou $(p, \mathrm{ord}_P(x)) = 1$, alors

$$\mathrm{ord}_P(fdx) = \mathrm{ord}_P(f) + \mathrm{ord}_P(dx) - 1.$$

Si $p \neq 0$ et $p \mid \mathrm{ord}_P(x)$, alors

$$\mathrm{ord}_P(fdx) \geq \mathrm{ord}_P(f) + \mathrm{ord}_P(dx).$$

Démonstration. (i) Par la proposition 2.42, $\bar{K}(C)$ est une extension séparable finie de $\bar{K}(t)$ et donc, par la proposition 2.53, dt est une base de Ω_C.

(ii) Voir [Har77], page 300.

(iii) Soit t' un autre paramètre uniformisant en P. Par le point précédent, $\frac{dt}{dt'}$ et $\frac{dt'}{dt}$ sont réguliers. Ainsi, on obtient $\mathrm{ord}_P\left(\frac{dt}{dt'}\right) = 0$. Comme $\omega = gdt = d\frac{dt}{dt'}dt'$, on a le résultat.

(iv) Voir [Sil09], pages $31 - 32$.

(v) Idem.

□

Définition 2.55
Soit $\omega \in \Omega_C$. On définit le diviseur associé à ω par

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)(P).$$

C'est bien un diviseur par le point (iv) de la proposition précédente.

Définition 2.56
Une forme différentielle $\omega \in \Omega_C$ est dite *holomorphe* ou *régulière* si $\mathrm{ord}_P(\omega) \geq 0$ pour tout $P \in C$. On dit qu'elle *ne s'annule pas* si $ord_P \leq 0$ pour tout $P \in C$.

Soient ω_1 et ω_2 deux formes différentielles non-nulles. Comme Ω_C est un $\bar{K}(C)$-espace vectoriel de dimension 1, il existe $f \in \bar{K}(C)^*$ tel que $\omega_1 = f\omega_2$ et donc la définition suivante fait sens.

Définition 2.57 (Classe de diviseur canonique)
La classe des diviseurs canoniques de C est l'image dans $\mathrm{Pic}(C)$ de $\mathrm{div}(\omega)$ pour un $\omega \in \Omega_C$ non-nul. Tout diviseur dans cette classe est appelé *diviseur canonique*.

Nous allons maintenant définir un ordre partiel sur $\mathrm{Div}(C)$.

Définition 2.58 (Diviseur positif)
Soit $D = \sum_{P \in C} n_P(P) \in \mathrm{Div}(C)$ un diviseur. On dit que D est positif et on note $D \geq 0$ si $n_P \geq 0$ pour tout $P \in C$. Soient $D_1, D_2 \in \mathrm{Div}(C)$. On écrit $D_1 \geq D_2$ si $D_1 - D_2$ est positif.

Définition 2.59
Soit $D \in \mathrm{Div}(C)$. On définit l'ensemble

$$\mathcal{L}(D) = \{f \in \bar{K}(C)^* : \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

Proposition 2.60
L'ensemble $\mathcal{L}(D)$ *est un* $\bar{K}$*-espace vectoriel de dimension finie. On note sa dimension* $l(D)$.

Démonstration. Voir [Sil09], page 34. □

Proposition 2.61 (i) *Soit* $D \in \mathrm{Div}(C)$ *tel que* $\deg D < 0$. *Alors,* $\mathcal{L}(D) = 0$ *et* $l(D) = 0$.

(ii) *Si* $D, D' \in \mathrm{Div}(C)$ *sont linéairement équivalents, alors* $\mathcal{L}(D)$ *est isomorphe à* $\mathcal{L}(D')$ *et donc* $l(D) = l(D')$.

Démonstration. (i) Supposons qu'il existe $0 \neq f \in \mathcal{L}(D)$. Par le point (ii) de la proposition 2.50, $0 = \deg(\mathrm{div}(f)) \geq \deg(-D) = -\deg(D)$ et donc $\deg D \geq 0$.

(ii) Comme $D \sim D'$, il existe $f \in \bar{K}(C)$ tel que $D = D' + \mathrm{div}(f)$. Alors, l'application

$$\begin{aligned} \varphi : \mathcal{L}(D) &\longrightarrow \mathcal{L}(D') \\ g &\longmapsto fg \end{aligned}$$

est un isomorphisme. En effet, si $g \in \mathcal{L}(D)$, alors on a $\mathrm{div}(g) \geq -D$ et donc

$$\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g) \geq \mathrm{div}(f) - D = -D'.$$

L'application φ est clairement $\bar{K}$-linéaire et inversible.

□

Soient $K_C = \mathrm{div}(\omega) \in \mathrm{Div}(C)$ un diviseur canonique de C et $f \in \bar{K}(C)^*$. Alors, on a $f \in \mathcal{L}(K_C)$ si et seulement si $\mathrm{div}(f\omega) \geq 0$. Or, cette dernière équation est équivalente au fait que la forme différentielle $f\omega$ soit holomorphe. De plus, comme toute forme différentielle sur C est de la forme $f\omega$ pour $f \in \mathcal{L}(K_C)$, on a que $\mathcal{L}(K_C)$ et $\{\omega \in \Omega_C : \omega \text{ est holomorphe}\}$ sont isomorphes.

Théorème 2.62 (Théorème de Riemann-Roch)
Soient C une courbe lisse et K_C un diviseur canonique de C. Alors, il existe un entier $g \geq 0$, appelé le genre de C, *tel que*

$$l(D) - l(K_C - D) = \deg D - g + 1,$$

pour tout $D \in \mathrm{Div}(C)$.

Démonstration. Voir [Har77], pages 295 et suivantes. □

Corollaire 2.63
Avec les mêmes notations que dans le théorème précédent, on obtient :

(*i*) $l(K_C) = g$;

(*ii*) $\deg(K_C) = 2g - 2$;

(*iii*) *si* $\deg D > 2g - 2$, *alors* $l(D) = \deg D - g + 1$.

Démonstration. (i) Remarquons d'abord que $\mathcal{L}(0) = \bar{K}$ par la proposition 2.41 et donc $l(0) = 1$. En appliquant le théorème de Riemann-Roch à $D = 0$, on obtient $l(0) - l(K_C) = -g + 1$.

(ii) On applique le théorème avec $D = K_C$ et on utilise le point précédent.

(iii) Puisque $\deg D > 2g - 2 = \deg(K_C)$, on a $\deg(K_C - D) < 0$ et donc, par la proposition 2.61, on a $l(K_C - D) = 0$.

□

Exemple 2.64
Soit la courbe définie par l'équation $Y^2 = X^3 + 17$. Nous verrons dans le théorème 3.5 que cette courbe est de genre 1.

Exemple 2.65
Soient $g \in \mathbb{N}$ et C une courbe satisfaisant l'équation $y^2 + h(x)y = f(x)$, où $h(x) \in K[x]$ est de degré plus petit ou égal à g, le polynôme $f(x) \in K[x]$ est de degré $2g+1$ et telle que C n'ait pas de point singulier, c'est-à-dire qu'il n'existe pas de $(u, v) \in K \times K$ tel que $v^2 + h(u) = f(u), 2v + h(u) = 0$ et $h'(u)v = f'(u)$. Alors C est appelée *courbe hyperelliptique de genre g*. On peut vérifier que C est effectivement de genre g. De plus, les courbes hyperelliptiques sont une généralisation des courbes elliptiques, en effet si $g = 1$, alors C est une courbe elliptique, ce que nous verrons dans le chapitre suivant.

3 Introduction aux courbes elliptiques

Une *courbe elliptique* est une courbe lisse de genre 1 avec un point de base fixé. Nous montrerons dans le deuxième paragraphe que toute courbe elliptique peut être définie par une équation cubique homogène

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

où $a_1, \ldots, a_6 \in \bar{K}$ et où on pose $O = [0, 1, 0]$ comme point de base. Une telle équation est appelée *équation de Weierstrass*. On appelle E la courbe définie par cette équation.

3.1 Équation de Weierstrass

Nous allons maintenant étudier les équations de Weierstrass. Pour simplifier, nous noterons ces équations sous une forme non homogène, c'est-à-dire en posant $x = \dfrac{X}{Z}$ et $y = \dfrac{Y}{Z}$. Dans ce cas, l'équation est de la forme

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

Toutefois, il faut se rappeler qu'il existe un point de base que nous considérerons comme étant l'infini. Si $a_1, \ldots, a_6 \in K$, on dit que E est *définie sur* K. Supposons que $\mathrm{Car}(\bar{K}) \neq 2$. Alors, on peut simplifier l'équation en complétant le carré. En effectuant le changement de variable $y \mapsto \dfrac{y - a_1x - a_3}{2}$, on obtient l'équation suivante :

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

où $b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3$ et $b_6 = a_3^2 + 4a_6$. On définit encore les quantités suivantes :

$$\begin{aligned}
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
j &= \frac{c_4^3}{\Delta} \\
\omega &= \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}.
\end{aligned}$$

Si la caractéristique de $\bar{K}$ n'est ni 2, ni 3, on peut effectuer le changement de variable $(x, y) \mapsto \left(\dfrac{x - 3b_2}{36}, \dfrac{y}{108}\right)$ pour éliminer le terme en x^2. On obtient alors l'équation simplifiée

$$y^2 = x^3 - 27c_4x - 54c_6,$$

qui est de la forme $y^2 = x^3 + ax + b$, avec $a = -27c_4 \in \bar{K}$ et $b = -54c_6 \in \bar{K}$. Par la suite, on ne fait plus d'hypothèse sur la caractéristique de K.

Définition 3.1
La quantité Δ est le *discriminant de l'équation de Weierstrass*, j est le *j-invariant de E* et ω est *l'invariant différentiel de E*.

Proposition 3.2 (*i*) *La courbe E est lisse si et seulement si $\Delta \neq 0$.*

(*ii*) *Deux courbes définies par des équations de Weierstrass sont isomorphes sur $\bar{K}$ si et seulement si elles ont le même j-invariant.*

Démonstration. Voir [Sil09], pages $45 - 47$. □

Proposition 3.3
L'invariant différentiel ω associé à la courbe lisse E est une forme différentielle holomorphe qui se n'annule pas, c'est-à-dire $\mathrm{div}(\omega) = 0$.

Démonstration. Voir [Sil09], page 48. □

3.2 Courbes elliptiques

Définition 3.4 (Courbe elliptique)
Une courbe elliptique est une paire (E, O), où E est une courbe lisse sur $\bar{K}$ de genre 1 et $O \in E$. On dit que O est le *point à l'infini de E*. On dit que E est définie sur K et on note E/K si E est définie sur K en tant que courbe et si $O \in E(K)$.

On va souvent écrire seulement E pour une courbe elliptique, le O étant sous-entendu.

Nous allons maintenant montrer, en utilisant le théorème de Riemann-Roch, qu'une courbe elliptique peut être décrite par une équation de Weierstrass et réciproquement que toute courbe décrite par une équation de Weierstrass est une courbe elliptique.

Théorème 3.5
Soit E une courbe elliptique définie sur K.

(*i*) *Il existe $x, y \in K(E)$ tels que l'application*

$$\varphi : E \longrightarrow \mathbb{P}^2$$
$$\varphi = [x, y, 1]$$

donne un isomorphisme entre E/K et une courbe définie par l'équation de Weierstrass

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

où $a_1, \ldots, a_6 \in K$ et $\varphi(O) = [0, 1, 0]$. On appelle x, y les coordonnées de Weierstrass *de E.*

(*ii*) *Soient $C \in K[X, Y]$ et $C' \in K[X', Y']$ deux équations de Weierstrass qui définissent E comme dans le point précédent. Alors, C' peut être obtenue à partir de C en effectuant un changement de variables de la forme*

$$X = u^2X' + r,$$
$$Y = u^3Y' + su^2X' + t,$$

où $u, r, s, t \in K$ et $u \neq 0$.

(*iii*) *Soit C une courbe lisse donnée par une équation de Weierstrass comme dans le point (i). Alors, C est une courbe elliptique avec O comme point à l'infini.*

Démonstration. (i) Considérons les espaces vectoriels $\mathcal{L}(n(O))$ pour $n \in \mathbb{N}$. Alors, par le corollaire du théorème de Riemann-Roch (corollaire 2.63), on a

$$l(n(O)) = \deg n(O) - g + 1 = \deg n(O) = n.$$

Il est possible de trouver une base de $\mathcal{L}(n(O))$ ne contenant que des fonctions de $K(E)$, voir [Sil09] page 36. Alors, il existe des fonctions $x, y \in K(E)$ tels que $\{1, x\}$ soit une base de $\mathcal{L}(2(O))$ et $\{1, x, y\}$ soit une base de $\mathcal{L}(3(O))$. Ainsi, x a un pôle d'ordre 2 en O. En effet, il appartient à $\mathcal{L}(2(O))$ et donc $ord_O(x) \geq -2$ et comme $\{1, x\}$ est une base de $\mathcal{L}(2(O))$ et $\mathrm{ord}_O(1) = 0$, on doit avoir $\mathrm{ord}_O(x) = -2$. De même, y a un pôle d'ordre 3 en O. Remarquons qu'alors $\mathrm{ord}_O(f) \geq -6$ pour tout $f \in \{1, x, y, x^2, xy, y^2, x^3\}$. Par conséquent, $\mathcal{L}(6(O))$, qui est de dimension 6, contient les sept vecteurs $1, x, y, x^2, xy, y^2, x^3$. Ces vecteurs sont donc linéairement dépendants. On écrit cette dépendance par

$$b_1 + b_2x + b_3y + b_4x^2 + b_5xy + b_6y^2 + b_7x^3 = 0,$$

où $b_i \in K$ pour $0 \leq i \leq 7$ et ne sont pas tous nuls. Notons que b_6 et b_7 ne peuvent pas être nuls. Sinon tous les termes auraient des pôles d'ordre différents en O et donc les b_i s'annulerait tous. Appliquons maintenant le changement de variables

$$x \mapsto -b_6 b_7 x,$$
$$y \mapsto b_6 b_7^2 y$$

et divisons l'équation résultante par $b_6^3 b_7^4$. Cela nous donne une équation de Weierstrass. On définit donc l'application

$$\varphi : E \longrightarrow C,$$
$$\varphi = [x, y, 1]$$

où C est la courbe donnée par l'équation de Weierstrass. On vérifie ensuite que φ est un isomorphisme, voir [Sil09] pages $59 - 60$ pour les détails.

(ii) Soient x, y et x', y les coordonnées de Weierstrass de C, respectivement C'. Comme x et x' ont un pôle d'ordre 2 en O et y et y' ont un pôle d'ordre 3 en O, on a que $\{1, x\}$ et $\{1, x'\}$ sont des bases de $\mathcal{L}(2(O))$ et que $\{1, x, y\}$ et $\{1, x', y'\}$ sont des bases de $\mathcal{L}(3(O))$. Ainsi, il existe $u_1, u_2, r, s_2, t \in K$ avec $u_1 \neq 0 \neq u_2$ tels que

$$x = u_1 x' + r$$
$$y = u_2 y' + s_2 x' + t.$$

Comme (x, y) et (x', y') sont des solutions d'une équation de Weierstrass dont les coefficients en X^3 et en Y^2 sont 1, on a $u_1^3 = u_2^2$. Ainsi, on a le résultat en posant $u = \dfrac{u_2}{u_1}$ et $s = \dfrac{s_2}{u^2}$.

(iii) Posons g le genre de C. Par la proposition 3.3, l'invariant différentiel ω de la courbe C est holomorphe et ne s'annule pas. Ainsi, $\mathrm{div}(\omega) = 0$. Par le deuxième point du corollaire 2.63, on obtient $0 = \deg(\mathrm{div}(\omega)) = 2g - 2$ et donc $g = 1$.

□

Grâce à ce théorème, nous pouvons maintenant voir les courbes elliptiques comme les solutions d'une équations de Weierstrass.

Exemple 3.6
La courbe définie par l'équation $Y^2 = X^3 + 17$ est une courbe elliptique, en effet son discriminant est $\Delta = 124848 \neq 0$.

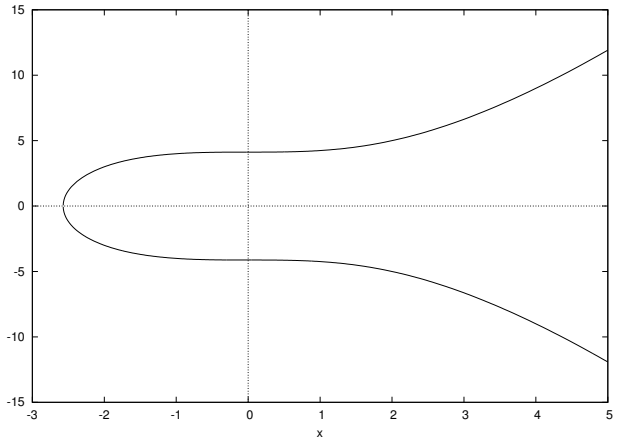

FIGURE 3 – La courbe elliptique $Y^2 = X^3 + 17$

3.3 La structure de groupe d'une courbe elliptique

Soit E la courbe définie par une équation de Weierstrass

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Rappelons qu'on a identifié la variété affine définie par l'équation à sa clôture projective et qu'on a un point de base O. Soit $L \subset \mathbb{P}^2$ une droite. Comme l'équation est de degré 3, on obtient, par le théorème de Bézout (voir [Har77] page 54), l'existence de trois points non nécessairement distincts P, Q et R dans l'intersection de L et E.

Définition 3.7 (Loi de composition sur E)
Soit $P, Q \in E$. Si $P \neq Q$, soit L la droite reliant P et Q, sinon soit L la tangente à E en P. Soit encore R le troisième point d'intersection dans $L \cap E$. Soit encore L' la droite reliant R et O. On définit alors $P \oplus Q$ comme étant le troisième point d'intersection de L' et E.

Nous allons maintenant montrer que la loi $\oplus$ munit E d'une structure de groupe abélien avec élément neutre O.

Proposition 3.8 *(i) Soient L une droite et P, Q et R les points d'intersection de L et E. Alors, $(P \oplus Q) \oplus R = O$.*

(ii) $P \oplus Q = Q \oplus P$, pour tout $P, Q \in E$.

(iii) Pour tout $P \in E$, on a $P \oplus O = P$.

(iv) Soit $P \in E$. Il existe un point dans E, noté $-P$, tel que $P \oplus (-P) = O$.

(v) Soient $P, Q, R \in E$. Alors, $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

(vi) Si E est définie sur K, alors

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

est un sous-groupe de E.

Démonstration. (i) Clair.

(ii) La droite reliant P et Q est la même que celle reliant Q et P.

(iii) Les droites L et L' sont les mêmes si $Q = O$. Comme L a P, O et R comme points d'intersection et R, O et $P \oplus O$ sont ceux de L', on en déduit que $P \oplus O = P$.

(iv) Soient L la droite reliant P à O et R le troisième point d'intersection. On a alors $O = (P \oplus O) \oplus R = P \oplus R$ par les points (i) et (iii).

(v) Par la suite, nous allons donner des formules explicites pour l'addition. On pourra alors vérifier que la loi est bien associative.

(vi) Si P et Q ont leurs coordonnées dans K, alors la droite les reliant a aussi ses coefficients dans K. Les coordonnées du troisième point d'intersection est une combinaison rationnelle des coefficients de la droite et de E. Comme E est définie sur K, le troisième point le sera aussi.

□

Notation 3.9
On note $+$ au lieu de $\oplus$.

Soit $P \in E$. On définit alors la fonction $[\,\cdot\,] : E \to E$ par $[m]P = P + \ldots + P$ (m fois) pour $m > 0$, $[0]P = O$ et $[m]P = [-m](-P)$ pour $m < 0$. On appelle cette fonction la *multiplication par m*.

Nous allons maintenant donner des formules explicites pour l'addition et l'opposé des points de E.

Proposition 3.10 *(i) Soit $P_0 = (x_0, y_0) \in E$. Alors, $-P_0 = (x_0, -(y_0 + a_1x_0 + a_3))$.*

(*ii*) *Soient* $P_1 = (x_1, y_1) \in E, P_2 = (x_2, y_2) \in E$ *et* $P_3 := P_1 + P_2 = (x_3, y_3)$. *Si* $x_1 = x_2$ *et* $y_1 + y_2 + a_1x_2 + a_3 = 0$, *alors* $P_1 + P_2 = O$. *Sinon, on pose*

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ et } v = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, \text{ si } x_1 \neq x_2,$$

et

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \text{ et } v = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3},$$

si $x_1 = x_2$. *Alors,* P_3 *est donné par*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$
$$y_3 = -(\lambda + a_1)x_3 - v - a_3.$$

(*iii*) *En particulier, si* $P_1 \neq \pm P_2$, *on a*

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2,$$

où $x(P)$ *est la coordonnée en* x *de* P. *Pour* $P = (x, y) \in E$, *on a la formule de duplication*

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}.$$

Démonstration. (i) Pour calculer $-P_0$, on doit prendre l'intersection de E et de la droite qui relie O et P_0. Cette droite est donnée par $x - x_0 = 0$. En remplaçant ceci dans l'équation de E, on trouve un polynôme quadratique $f(x_0, y)$ qui a donc deux racines $y_0, y_0' \in \bar{K}$ puisque $-P_0 \in E$. Ainsi $-P_0 = (x_0, y_0')$. De plus, $f(x_0, y) = (y - y_0)(y - y_0')$ puisque $f(x_0, y)$ est unitaire en y. L'étude des coefficients de ce polynôme en y donne

$$a_1x_0 + a_3 = -y_0 - y_0'.$$

(ii) Soient L la droite reliant P_1 et P_2 ou la tangente si $P_1 = P_2$ et $Q = (x_3', y_3')$ le troisième point de l'intersection de L et E. Alors, l'équation de L est $y = \lambda x + v$. En remplaçant dans l'équation de E, on trouve que $f(x, \lambda x + v)$ est un polynôme cubique avec racines x_1, x_2, x_3'. On a donc $f(x, \lambda x + v) = -(x - x_1)(x - x_2)(x - x_3')$ et en regardant les coefficients en x^2, on trouve

$$x_1 + x_2 + x_3' = \lambda^2 + a_1\lambda - a_2.$$

Nous avons ainsi une formule pour x_3' et donc aussi pour $y_3' = \lambda x_3' + v$. On remarque pour finir que $P_1 + P_2 + Q = O$ et donc $P_1 + P_2 = -Q$. On applique finalement la formule d'inversion à Q.

(iii) C'est un cas particulier du point (*ii*).

□

Exemple 3.11
Soient $K = \mathbb{Q}$ et E la courbe elliptique sur $\mathbb{Q}$ définie par $y^2 = x^3 + 17$. On peut vérifier que les $P_1 = (-2, 3), P_2 = (-1, 4), P_3 = (2, 5), P_4 = (4, 9)$ et $P_5 = (8, 23)$ sont des points de E. En utilisant les relations ci-dessus, on voit que

$$P_5 = [-2]P_1 \text{ et } P_4 = P_1 - P_3.$$

Lemme 3.12
Soient C *une courbe de genre* 1 *et* $P, Q \in C$. *Alors,* $(P) \sim (Q)$ *si et seulement si* $P = Q$.

Démonstration. Soit $f \in \bar{K}(C)^*$ tel que $\operatorname{div}(f) = (P) - (Q)$. Puisque $\operatorname{div}(f) + (Q) = (P) \geq 0$, on a $f \in \mathcal{L}\big((Q)\big)$. Comme $\deg P = 1 > 0$, on obtient, par le point *(iii)* du corollaire 2.63, que $l\big((Q)\big) = 1$. De plus, $\bar{K} \subset \mathcal{L}\big((Q)\big)$ et ainsi $f \in \bar{K}$. Finalement, on voit que $(P) - (Q) = \operatorname{div}(f) = 0$. La réciproque est claire. □

Proposition 3.13
Soit (E, O) une courbe elliptique.

(i) Soit $D \in \operatorname{Div}^0(E)$. Alors, il existe un unique point $P_D \in E$ tel que $D \sim (P_D) - (O)$. On définit

$$\begin{aligned} \sigma : \operatorname{Div}^0(E) &\longrightarrow E \\ D &\longmapsto P_D. \end{aligned}$$

(ii) L'application σ définie ci-dessus est surjective.

(iii) Soient $D_1, D_2 \in \operatorname{Div}^0(E)$. Alors, on a $\sigma(D_1) = \sigma(D_2)$ si et seulement si $D_1 \sim D_2$. Ainsi σ induit une bijection, que l'on notera aussi σ, de $\operatorname{Pic}^0(E)$ dans E.

(iv) L'inverse de sigma est l'application

$$\begin{aligned} \kappa : E &\longrightarrow \operatorname{Pic}^0(E) \\ P &\longmapsto \big((P) - (O)\big) + \operatorname{Pr}(E). \end{aligned}$$

(v) La loi de groupe «géométrique» donnée par l'équation de Weierstrass et la loi de groupe «algébrique» induite par $\operatorname{Pic}^0(E)$ sont les mêmes.

Démonstration. Soit (E, O) une courbe elliptique.

(i) Le degré de $D + (O)$ est 1. Ainsi par le corollaire 2.63, on a $l(D + (O)) = 1$. Soit $0 \neq f \in \mathcal{L}(D + (O))$ et écrivons $\operatorname{div}(f) + D + (O) = \sum_{P \in E} n_P(P)$. Alors, comme $\operatorname{div}(f) + D + (O) \geq 0$ et $\deg(\operatorname{div}(f) + D + (O)) = 1$, il existe un seul $P \in E$ tel que $n_P = 1$ et $n_Q = 0$ pour tout $Q \in E \setminus \{P\}$. Ainsi, $\operatorname{div}(f) + D + (O) = (P)$. S'il existe un autre Q tel que $D \sim (Q) - (O)$, alors $(P) - (O) \sim (Q) - (O)$. Donc il existe $f \in \bar{K}(E)^*$ tel que $\operatorname{div}(f) = (P) - (O) - (Q) + (O)$, ce qui implique que $(P) \sim (Q)$ et donc $P = Q$, par le lemme 3.12.

(ii) On a que $(P) - (O)$ est de degré 0 et $\sigma\big((P) - (O)\big) = P$.

(iii) Si $P_{D_1} = P_{D_2}$, alors $D_1 \sim (P_{D_1}) - (O) = (P_{D_2}) - (O) \sim D_2$. Réciproquement, si $D_1 \sim D_2$, alors $(P_{D_1}) - (O) \sim D_1 \sim D_2 \sim (P_{D_2}) - (O)$ et donc $P_{D_1} = P_{D_2}$, par le lemme 3.12.

(iv) Clair.

(v) Voir [Sil09], pages $62 - 63$.

□

Corollaire 3.14
Soient E une courbe elliptique et $D = \sum_{P \in E} n_P(P) \in \operatorname{Div}^0(E)$. Alors, D est principal si et seulement si $\sum_{P \in E} [n_P]P = O$.

Démonstration. On a que D est principal si et seulement si $D \sim 0$, ce qui est équivalent à $\sigma(D) = O$. Comme $\deg D = 0$, on a

$$\sum_{P \in E} [n_P]\sigma\big((P)\big) = \sum_{P \in E} [n_P]\sigma\big((P)\big) - \sum_{P \in E} [n_P]\sigma\big((O)\big) = \sum_{P \in E} [n_P]\sigma\big((P) - (O)\big).$$

Ainsi, on a

$$0 = \sigma\left(\sum_{P \in E} n_P(P)\right) = \sum_{P \in E} [n_P]\sigma\big((P)\big) = \sum_{P \in E} [n_P]\sigma\big((P) - (O)\big) = \sum_{P \in E} [n_P]P,$$

ce qui termine la démonstration. □

Proposition 3.15
Soit E/K une courbe elliptique. Alors, l'addition et la prise d'opposé des points de E sont des morphismes de courbes algébriques.

Démonstration. Voir [Sil09], pages $64 - 65$. □

3.4 Isogénies entre courbes elliptiques

Nous allons maintenant parler des morphismes de courbes elliptiques.

Définition 3.16 (Isogénie, courbes isogènes)
Soit $(E_1, O_1), (E_2, O_2)$ deux courbes elliptiques. Une *isogénie* entre E_1 et E_2 est un morphisme $\varphi : E_1 \to E_2$ tel que $\varphi(O_1) = O_2$. On dit que E_1 et E_2 sont *isogènes* s'il existe une isogénie φ entre eux telle que $\varphi(E_1) \neq \{O_2\}$.

Définition 3.17 (Degré d'une isogénie)
Le *degré d'une isogénie* est son degré en tant que morphisme.

Par la proposition 2.44, une isogénie φ satisfait soit $\varphi(E_1) = \{O_2\}$, soit $\varphi(E_1) = E_2$. Ainsi, la seule isogénie de degré zéro est l'isogénie $[0] : E_1 \to E_2$, où $[0](P) = O$ pour tout $P \in E_1$.

Théorème 3.18
Soit $\varphi : E_1 \to E_2$ une isogénie. Alors, φ est un homomorphisme de groupes.

Démonstration. Si φ est de degré 0, il n'y a rien à prouver. Sinon, considérons l'application

$$\begin{gathered}\varphi_* : \mathrm{Pic}^0(E_1) \longrightarrow \mathrm{Pic}^0(E_2) \\ \left(\sum_{P \in E_1} n_P(P)\right) + \mathrm{Pr}(E_1) \longmapsto \left(\sum_{P \in E_1} n_P(\varphi(P))\right) + \mathrm{Pr}(E_2).\end{gathered}$$

C'est clairement un homomorphisme de groupes. Soient

$$\begin{aligned}\sigma_i : \mathrm{Pic}^0(E_i) &\longrightarrow E_i, i = 1, 2 \\ D + \mathrm{Pr}(E_i) &\longmapsto P_D\end{aligned}$$

les isomorphismes de groupes définis dans la proposition 3.13. Puisque $\varphi(O) = O$, on vérifie que $\varphi = \sigma_2 \circ \varphi_* \circ \sigma_1^{-1}$. Ainsi, φ est un homomorphisme de groupes en tant que composition d'homomorphismes. □

Exemple 3.19
Soit E une courbe elliptique. La multiplication par m définie au début du chapitre est une isogénie. En effet, $[m] : E \to E$ est un morphisme par la proposition 3.15 et $[m](O) = O$.

Proposition 3.20
Soient E/K une courbe elliptique et $0 \neq m \in \mathbb{Z}$. Alors, la multiplication par m, $[m] : E \to E$ est non constante.

Démonstration. Voir [Sil09], page 68. □

Définition 3.21 (Sous-groupe de torsion)
Soient E/K une courbe elliptique et $0 \neq m \in \mathbb{Z}$. Le *sous-groupe de m-torsion de E*, noté $E[m]$, est l'ensemble des points de E dont l'ordre divise m. Autrement dit, il s'agit de

$$E[m] = \{P \in E : [m]P = O\} = \ker[m].$$

Le *sous-groupe de torsion de E*, noté E_{tors} est l'ensemble des points d'ordre fini, c'est-à-dire $E_{tors} = \bigcup_{m=1}^{\infty} E[m]$. Si E est définie sur K, on note $E_{tors}(K)$ les points d'ordre fini de $E(K)$.

Proposition 3.22
Soient E/K une courbe elliptique, $0 \neq m \in \mathbb{Z}$ et posons $p = \mathrm{Car}(K)$. Si $p = 0$ ou $(m, p) = 1$, alors $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Si p est premier, alors soit $E[p^n] = \{O\}$ pour tout $n \in \mathbb{N}$, soit $E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z}$ pour tout $n \in \mathbb{N}$.

Démonstration. Voir [Sil09], page 86. □

3.5 Couplage de Weil

Soient E/K une courbe elliptique et $m \in \mathbb{N}, m \geq 2$ tel que m soit premier avec $\mathrm{Car}(K)$ si $\mathrm{Car}(K) > 0$. Rappelons qu'un diviseur $D = \sum_{P \in C} n_P(P)$ est principal si et seulement si $\deg D = 0$ et $\sum_{P \in C}[n_P]P = O$. Soit $T \in E[m]$. Alors, $m(T) - m(O)$ est principal et donc il existe $f \in \bar{K}(E)$ tel que $\mathrm{div}(f) = m(T) - m(O)$. Comme la multiplication par m n'est pas constante, elle est surjective et donc il existe $T' \in E$ tel que $[m]T' = T$. Notons que $\sum_{R \in E[m]}(T' + R) - (R)$ est aussi un diviseur principal. En effet, $|E[m]| = m^2$ et $[m^2]T' = O$. Ainsi, il existe $g \in \bar{K}(E)$ tel que $\mathrm{div}(g) = \sum_{R \in E[m]}(T' + R) - (R)$. En calculant, on peut voir que $f \circ [m]$ et g^m ont le même diviseur. Alors, on a $\mathrm{ord}_P(f \circ [m]) = \mathrm{ord}_P(g^m)$ pour tout $P \in C$ et donc $\dfrac{f \circ [m]}{g^m} \in \bar{K}$, par la proposition 2.50. Quitte à multiplier f par un élément de $\bar{K}^*$, on peut donc supposer que $f \circ [m] = g$.

Soit $S \in E[m]$. Alors, on a

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m$$

pour tout $X \in E$. Posons μ_m le groupe des racines m-ièmes de l'unité de $\bar{K}$. Alors, on peut définir un application

$$\begin{aligned} e_m : E[m] \times E[m] &\longrightarrow \mu_m, \\ (S, T) &\longmapsto \frac{g(X + S)}{g(X)} \end{aligned}$$

où X est un point de E tel que $g(X+S)$ et $g(X)$ soient tous deux définis et non-nuls. Notons que cette application est bien définie, puisque $\dfrac{g(X + S)}{g(X)}$ est une racine m-ème de l'unité et le fait que g soit défini à multiplication par un scalaire près ne gêne pas puisque l'on a une fraction. On appelle ce couplage *le e_m-couplage de Weil*.

Proposition 3.23
Le e_m-couplage de Weil a les propriétés suivantes :

(*i*) *Bilinéaire :*

$$\begin{aligned} e_m(S_1 + S_2, T) &= e_m(S_1, T)e_m(S_2, T), \\ e_m(S, T_1 + T_2) &= e_m(S, T_1)e_m(S, T_2) \end{aligned}$$

pour tous $S, S_1, S_2, T, T_1, T_2 \in E[m]$.

(*ii*) *Alterné : $e_m(S, T) = e_m(T, S)^{-1}$ et $e_m(T, T) = 1$ pour tout $S, T \in E[m]$.*

(*iii*) *Non-dégénéré : Si $e_m(S, T) = 1$ pour tout $S \in E[m]$, alors $T = O$.*

(*iv*) *Il existe $S, T \in E[m]$ tels que $e_m(S, T)$ soit une racine m-ième primitive de l'unité. De plus, si $E[m] \subset E[K]$, alors $e_m(S, T) \in K^*$ pour tous $S, T \in E[m]$.*

Démonstration. Voir [Sil09], pages 94-96. □

3.6 Courbes elliptiques sur des corps finis

Soient $q = p^m$, où p est un nombre premier, $K = \mathbb{F}_q$ et E/K une courbe elliptique. Nous allons donner une estimation du nombre de points de $E(K)$.

Théorème 3.24 (Théorème de Hasse)
On a la borne suivante :

$$|\#E(K) - q - 1| \leq 2\sqrt{q}.$$

Démonstration. Voir [Sil09], page 138. □

Théorème 3.25 (Théorème de Weil)
Soit $t = q + 1 - \#E(\mathbb{F}_q)$. Alors, $\#E(\mathbb{F}_{q^k}) = q^k + 1 - \alpha^k - \beta^k$, où $\alpha, \beta \in \mathbb{C}$ sont tels que $qT^2 - tT + 1 = (\alpha T - 1)(\beta T - 1)$.

Démonstration. Voir [Sil09], page $142 - 143$. □

Proposition 3.26
Le groupe $E(\mathbb{F}_q)$ est isomorphe à $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$, où $n_1, n_2 \in \mathbb{N}$ sont tels que $n_2 \mid n_1$ et $n_2 \mid q - 1$.

Notons tout de même que n_2 peut être 1, par exemple si le groupe est cyclique.

Démonstration. Par la classification des groupes abéliens finis, $E(\mathbb{F}_q) \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$ avec $d_i \in \mathbb{N}$ et $d_{i+1} \mid d_i$. Soit $N = \#E(\mathbb{F}_q)$. Alors, par le théorème 3.24, on a $(N, q) = 1$, ce qui implique, par la proposition 3.22 $E[N] = \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Comme $E(\mathbb{F}_q) \subset E[N]$, on a l'inclusion suivante

$$\mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

Ainsi par la classification des groupes abéliens finis, $n \leq 2$. Supposons maintenant que $E(\mathbb{F}_q)$ soit isomorphe à $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ avec $n_2 \mid n_1$. Comme $E[n_2] \subset E(\mathbb{F}_q)$, on a, par le point (iv) de la proposition 3.23, que $\mu_{n_2} \subset \mathbb{F}_q^*$ et ainsi $n_2 \mid q - 1$. □

Définition 3.27 (Courbe supersingulière)
Soit $q = p^m$ avec p premier. On dit qu'une courbe elliptique E définie sur $\mathbb{F}_q$ est *supersingulière* si $p \mid t$, où $t = q + 1 - \#E(F_q)$.

Lemme 3.28
Il existe une courbe elliptique d'ordre $q+1-t$ si et seulement si l'une des conditions suivantes est vérifiée :

- (i) *$p \nmid t$ et $t^2 \leq 4q$.*
- (ii) *m est impair et l'une des conditions suivantes est vraie :*
  - *(a) $t = 0$;*
  - *(b) $t^2 = 2q$ et $p = 2$;*
  - *(c) $t^2 = 3q$ et $p = 3$.*
- (iii) *m est pair et l'une des conditions suivantes est vraie :*
  - *(a) $t^2 = 4q$;*
  - *(b) $t^2 = q$ et $p \not\equiv 1 \pmod 3$;*
  - *(c) $t = 0$ et $p \not\equiv 1 \pmod 4$.*

Démonstration. Voir [Wat69], pages $536 - 537$. □

Grâce au lemme précédent, on voit que si E est une courbe supersingulière, alors $t^2 \in \{0, q, 2q, 3q, 4q\}$.

Le lemme suivant nous donne la structure de groupe des courbes supersingulières.

Lemme 3.29
Soit $t = q + 1 - |E(F_q)|$.

(*i*) *Si* $t^2 = q, 2q$ *ou* $3q$, *alors* $E(\mathbb{F}_q)$ *est cyclique.*

(*ii*) *Si* $t = 2\sqrt{q}$, *alors* $E(\mathbb{F}_q) = \mathbb{Z}/(\sqrt{q}-1)\mathbb{Z} \times \mathbb{Z}/(\sqrt{q}-1)\mathbb{Z}$.

(*iii*) *Si* $t = -2\sqrt{q}$, *alors* $E(\mathbb{F}_q) = \mathbb{Z}/(\sqrt{q}+1)\mathbb{Z} \times \mathbb{Z}/(\sqrt{q}+1)\mathbb{Z}$.

(*iv*) *Si* $t = 0$ *et* $q \not\equiv 3 \pmod 4$, *alors* $E(\mathbb{F}_q)$ *est cyclique.*

(*v*) *Si* $t = 0$ *et* $q \equiv 3 \pmod 4$, *alors soit* $E(\mathbb{F}_q)$ *est cyclique, soit* $E(\mathbb{F}_q) = \mathbb{Z}/\left(\frac{q+1}{2}\right)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Démonstration. Voir [Sch87], pages $196 - 197$. □

Lemme 3.30
Soit $n \in \mathbb{N}$ *tel que* $(n, q) = 1$ *et* $E[n] \subset E(\mathbb{F}_q)$. *Soient encore* $P, P_1, P_2 \in E[n]$. *Alors,* $\bar{P}_1 = \bar{P}_2 \in E[n]/\langle P \rangle$ *si et seulement si* $e_n(P, P_1) = e_n(P, P_2)$, *où* $e_n(P, P_1)$ *est le* e_n*-couplage de Weil de* $E(\mathbb{F}_q)$.

Démonstration. Comme $E(\mathbb{F}_q)$ est de type 2 par la proposition 3.26, il existe $Q \in E[n]$ tels que P, Q génèrent $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Supposons que $P_1 = P_2 + kP$. Alors,

$$e_n(P, P_1) = e_n(P, P_2)e_n(P, P)^k = e_n(P, P_2).$$

Supposons maintenant que $P_1 - P_2 = kP + k'Q$ avec $k'Q \neq O$. Ainsi, $e_n(P, k'Q) \neq 1$ par non-dégénérescence du couplage de Weil. Alors,

$$e_n(P, P_1) = e_n(P, P_2 + kP + k'Q) = e_n(P, P_2)e_n(P, P)^k e_n(P, k'Q) \neq e_n(P, P_2)$$

□

Soit $k \in \mathbb{N}$ le plus petit entier tel que $E[n] \subset E(\mathbb{F}_{q^k})$.

Théorème 3.31
Il existe $Q \in E[n]$ *tel que* $e_n(P, Q)$ *soit une racine primitive* n*-ème de l'unité.*

Démonstration. Soit $Q \in E[n]$. Alors,

$$e_n(P, Q)^n = e_n(P, nQ) = e_n(P, O) = 1.$$

Ainsi, $e_n(P, Q) \in \mu_n$, où μ_n est le groupe des racines n-èmes de l'unité dans $\mathbb{F}_{q^k}$. Comme $n = |\langle P \rangle|$ et $(n, q) = 1$, on a $|E[n]| = n^2$ et donc $\langle P \rangle$ est d'indice n dans $E[n]$. Par le lemme 3.30, on observe que si Q parcourt les représentants des classes de $\langle P \rangle$ dans $E[n]$, alors $e_n(P, Q)$ parcourt les éléments de μ_n. □

Corollaire 3.32
Soient $Q \in E[n]$ *tel que* $e_n(P, Q)$ *soit une racines primitive* n*-ème de l'unité et*

$$\begin{aligned} f : \langle P \rangle &\longrightarrow \mu_n \\ R &\longmapsto e_n(R, Q). \end{aligned}$$

Alors, f *est un isomorphisme de groupes.*

Démonstration. Clair. □

4 Considérations cryptographiques

Nous allons parler de quelques notions basiques de cryptographie, à savoir le cryptage RSA et l'équivalent sur les courbes elliptiques de l'échange de clé de Diffie-Hellman, de la transmission de message de ElGamal et de Massey-Omura ainsi que de l'algorithme de signature digitale (DSA).

4.1 Le cryptage RSA

Pour la culture général, nous allons décrire le principe de fonctionnement du célèbre cryptage RSA (Rivest-Shamir-Adleman). Le principe de ce cryptage est d'utiliser un clé publique pour crypter les données et une clé privée qui servira à les décrypter. Nous allons maintenant décrire l'algorithme qui permet de créer les clés.

Algorithm 1 Algorithme de création des clés

Entrée : -
Sortie : Une clé publique et une clé privée.
1: Choisir p et q deux nombres premiers distincts.
2: Calculer $n = pq$.
3: Calculer l'indicatrice d'Euler du produit : $\varphi(n) = (p-1)(q-1)$.
4: Choisir e un entier naturel tel que $(e, n) = 1$.
5: Calculer l'entier d tel que $d \equiv e^{-1} \pmod{\varphi(n)}$ et $d \leq \varphi(n)$.
6: **return** La clé publique est le couple (n, e), la clé privée est le couple (n, d).

En pratique, les nombres premiers sont choisis suffisamment grands. Une fois les clés crées, si Alice veut écrire un message à Bob, elle doit d'abord connaître la clé publique de Bob, qu'il lui aura donc envoyé de manière sécurisée. Puis, Alice crypte son message grâce à la clé publique de Bob, l'envoie à ce dernier qui peut le décrypter avec sa clé privée. Les algorithmes utilisés sont décrits si-dessous.

Algorithm 2 Algorithme de chiffrement du message

Entrée : Un entier $M < n$ représentant le message à crypter.
Sortie : Le message crypté.
1: **return** Le message crypté est $C \in \mathbb{N}$ tel que $C \equiv M^e \pmod{n}$ et $C < n$.

Algorithm 3 Algorithme de déchiffrement du message

Entrée : Un message crypté C.
Sortie : Le message décrypté.
1: **return** Le message décrypté est $M \in \mathbb{N}$ tel que $M \equiv C^d \pmod{n}$ et $M < n$.

Notons que l'algorithme de déchiffrement redonne le bon message. En effet,

$$C^d \equiv M^{ed} \equiv M^{1+k(p-1)(q-1)} \pmod{n}$$

pour un $k \in \mathbb{Z}$. De plus, si $p \mid M$, alors $M^{1+k(p-1)(q-1)} \equiv 0 \equiv M \pmod{p}$ et si $(p, M) = 1$, alors $M^{1+k(p-1)(q-1)} \equiv M \pmod{p}$ par le petit théorème de Fermat. On effectue le même raisonnement pour q et le théorème des restes chinois permet de conclure que

$$C^d \equiv M \pmod{n}.$$

Pour calculer d à l'aide de e et n, c'est-à-dire trouver la clé privée à partir de la clé publique, il faut trouver l'inverse de e modulo $(p-1)(q-1)$, ce qui nécessite de connaître la factorisation de n.

4.2 Application des courbes elliptiques à la cryptographie

Soient E une courbe elliptique sur $\mathbb{F}_q$ et $Q \in E$ et supposons que ces éléments soient publics.

4.2.1 L'échange de clé de Diffie-Hellman

L'un des buts principaux de la cryptographie à clé publique est de pouvoir échanger une clé privée qui servira à crypter les messages envoyés par la suite. Nous allons décrire le protocole d'échange de clés de Diffie-Hellman adapté aux courbes elliptiques. Celui-ci doit permettre à Alice et Bob de trouver une clé secrète commune à partir de communications publiques.

Notons d'abord qu'un point P sur une courbe elliptique définie sur un corps fini peut être utilisé comme clé. En effet, Alice et Bob peuvent se mettre d'accord sur un moyen de convertir P en un nombre naturel, par exemple en prenant la coordonnée en x de P et en lui appliquant une fonction $\mathbb{F}_q \to \mathbb{N}$.

Alice choisit aléatoirement un nombre entier k_A, calcule k_AQ et l'envoie à Bob, qui fait de même de son côté. La clé secrète sera alors $P := k_Ak_BQ$. Alice et Bob peuvent tous deux connaître P en multipliant le point reçu par le nombre aléatoire qu'ils ont choisi. Mais une personne qui écouterait leur conversation ne connaîtrait que Q, k_AQ et k_BQ pour trouver P.

Définition 4.1
La tâche de l'espion, à savoir trouver k_Ak_BQ en connaissant Q, k_AQ et k_BQ, s'appelle *le problème de Diffie-Hellman pour les courbes elliptiques.*

4.2.2 La transmission de messages de ElGamal

On peut facilement modifier le protocole d'échange de clé de Diffie-Hellman pour transmettre des messages. Supposons que nous ayons un moyen de codifier les messages par les points d'une courbe elliptique et qu'Alice et Bob se sont déjà échangés les points k_AQ et k_BQ. Si Alice veut transmettre à Bob un message $M \in E$, elle choisit un nombre entier aléatoire secret l et elle envoie $(lQ, M + l(k_BQ))$ à Bob. Pour déchiffrer le message, Bob multiplie le premier terme par k_B et le soustrait au deuxième.

Définition 4.2
La tâche de l'espion, autrement dit trouver M en connaissant $lQ, M + l(k_BQ), Q, k_AQ$ et k_BQ, s'appelle *le problème d'ElGamal pour les courbes elliptiques.*

4.2.3 La transmission de messages de Massey-Omura

Supposons que nous ayons un moyen de codifier les messages par les points d'une courbe elliptique et que le nombre de points n de la courbe dans $\mathbb{F}_q$ est publique. Alice et Bob choisissent tous deux un nombre entier aléatoire e_A, respectivement e_B, tels que $(e_A, n) = (e_B, n) = 1$ et calculent $d_A = e_A^{-1} \pmod{n}$, respectivement $d_A = e_A^{-1} \pmod{N}$ en utilisant l'algorithme d'Euclide. Si Alice veut envoyer le message $M \in E$ à Bob, elle envoie d'abord e_AM. Toutefois, Bob ne peut pas le décrypter et donc Bob renvoie e_Be_AM à Alice. Alice renvoie alors $d_Ae_Be_AM$ à Bob, et comme $nM = O$ et $d_Ae_A \equiv 1 \pmod{n}$, on a $d_Ae_Be_AM = e_BM$ et donc Bob peut décrypter le message.

Définition 4.3
La tâche de l'espion, autrement dit trouver M en connaissant n, e_AM, e_Be_AM, e_BM, s'appelle *le problème de Massey-Omura pour les courbes elliptiques.*

4.2.4 Le problème du logarithme discret

Soient G un groupe et $g \in G$.

Définition 4.4 (Le problème du logarithme discret)
Le problème du logarithme discret de G par rapport à la base g est le problème suivant : étant donné $y \in G$, trouver $x \in \mathbb{N}$ tel que $g^x = y$ si un tel x existe.

Remarque 4.5
Dans le cas des courbes elliptiques, le problème du logarithme discret de E par rapport à la base P est : étant donné $Q \in E$, de trouver $x \in \mathbb{N}$ tel que $Q = xP$. Il est facile de voir que si le problème du logarithme discret est résolu, ceux de Diffie-Hellman, de ElGamal et de Massey-Omura le sont aussi.

Définition 4.6 (B-lisse)
Soit $B \in \mathbb{R}_+^*$. On dit qu'un naturel $n \in \mathbb{N}$ est *B-lisse* si tout premier qui divise n est plus petit que B.

Si l'ordre de G est B-lisse pour un B suffisamment petit, alors le logarithme discret dans G peut être calculé efficacement par la méthode suivante :

Soit $|G| = \prod_{i=1}^{n} p_i^{s_i}$ la factorisation de $|G|$. Supposons que G soit abélien et B-lisse pour un B suffisamment petit, c'est-à-dire $p_i \leq B$. On commence par calculer l'ordre N de g. Le but est de trouver un $x \in \mathbb{N}, x < N$ tel que $xg = y$. Si un tel x n'existe pas, alors l'algorithme s'arrête et on saura alors qu'il n'y a pas de solution. Il suffit de trouver un tel x modulo $p_j^{r_j}$ pour tout $p_j^{r_j}$, où $N = \prod_{j=1}^{m} p_j^{r_j}$. Fixons $p = p_j$ et $r = r_j$ et écrivons

$$x \equiv x_0 + x_1 p + \ldots + x_{r-1} p^{r-1} \pmod{p^r}$$

avec $0 \leq x_i \leq p-1$. Pour trouver x_0, on multiplie l'équation $xg = y$ par $N' = \dfrac{N}{p}$. Ainsi, $x_0(N'g) = N'y$ et on peut tester les p possibilités pour x_0. S'il n'existe pas de tel x_0, alors $y \notin \langle g \rangle$. Ceci prend $\mathcal{O}(p)$ étapes. On peut même améliorer ce processus pour qu'il ne prenne que $\mathcal{O}(\sqrt{p})$ étapes en utilisant la technique de Shanks «baby-step-giant-step», voir [Coh93] page 241. Une fois x_0 connu, on calcule x_1 en multipliant l'équation $y = xg$ par $N'' = \dfrac{N}{p^2}$, ce qui donne $(x_0 + x_1 p)N'' = N''y$, c'est-à-dire $x_1(N'g) = N''(y - x_0 g)$. On utilise la même technique pour trouver $x_1, x_2, \ldots, x_{r-1}$. On connaît ainsi x modulo $p_j^{r_j}$ pour tout $j = 1, \ldots, m$. On conclut en utilisant le théorème des restes chinois.

4.2.5 Signature numérique

Il est important de pouvoir signer un message que l'on envoie, c'est-à-dire de pouvoir authentifier un document et en garantir l'intégrité. Pour cela, nous allons présenter l'algorithme de signature digitale sur des courbes elliptiques (ECDSA), qui est l'analogue sur les courbes elliptiques du système DSA.

Pour commencer, nous définissons ce qu'est une fonction de hachage, notion que nous utiliserons dans la signature de messages.

Définition 4.7 (Fonction de hachage)
Soit $m \in \mathbb{N}$ un message. Une *fonction de hachage* est une fonction qui envoie m sur h, où $h \in \mathbb{N}$ est un entier beaucoup plus petit que m telle que f soit facilement calculable et informatiquement injective, c'est-à-dire qu'il soit extrêmement long pour un ordinateur de trouver deux messages m et m' tels que $f(m) = f(m')$.

Nous allons maintenant donner les algorithmes de génération et de vérification de signatures. Soit une courbe elliptique E sur un corps fini $\mathbb{F}_p$, où $p \in \mathbb{N}$ est premier et $P \in E(\mathbb{F}_p)$ un point d'ordre n. Chaque utilisateur possède une clé privée $x \in \mathbb{N}$ choisie aléatoirement dans l'intervalle $]1, n-1[$ et une clé publique $Q = xP$.

Algorithm 4 Algorithme de génération de la signature

Entrée : Un message $m \in \mathbb{N}$.
Sortie : Une signature au message m.

1: Choisir un nombre entier k aléatoirement dans l'intervalle $]1, n-1[$.
2: Calculer $kP = (x_1, y_1)$ et $r = x_1 \pmod{n}$.
3: Si $r = 0$, retourner à l'étape 1.
4: Calculer $k^{-1} \pmod{n}$.
5: Calculer $s = k^{-1}(H(m) + xr)$.
6: **return** La signature du message m est le couple (r, s).

Algorithm 5 Algorithme de vérification de la signature

Entrée : Un message m signé par le couple (r, s).
Sortie : Une vérification de la signature.

1: Vérifier que r, s soient dans l'intervalle $[1, n-1]$.
2: Calculer $w = s^{-1} \pmod{n}$ et $H(m)$.
3: Calculer $u_1 = H(m)w \pmod{n}$ et $u_2 = rw \pmod{n}$.
4: Calculer $u_1P + u_2Q = (x_0, y_0)$ et $v = x_0 \pmod{n}$.
5: **return** La signature est acceptée si $v = r$.

Vérifions que les signatures authentiques seront toujours acceptée : En effet,

$$u_1 + u_2x \equiv H(m)w + rwx \equiv w(H(m) + rx) \equiv k \pmod{n}.$$

De plus,

$$(x_0, y_0) = u_1P + u_2Q = u_1P + u_2xP = (u_1 + u_2x)P = kP.$$

5 La réduction du problème du logarithme discret

Dans ce chapitre, nous allons présenter le contenu de l'article de Menezes, Okamoto et Vanstone «Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field» (pour la référence voir [MOV93]). Le résultat de cet article est qu'il existe un algorithme probabiliste de complexité polynomiale pour réduire le problème du logarithme discret sur le groupe d'un certain type de courbes elliptiques définies sur un corps fini $\mathbb{F}_q$ au problème du logarithme discret sur le groupe multiplicatif d'une certaine extension $\mathbb{F}_{q^k}$ de $\mathbb{F}_q$. Le terme «probabiliste» veut dire que l'algorithme a une chance d'échouer et par «de complexité polynomiale», on entend que le temps d'exécution de l'algorithme est borné par un polynôme en la taille de l'entrée, on dit aussi «en temps polynomial». Cette réduction est montrée en établissant un isomorphisme de groupes entre le sous-groupe $\langle P\rangle \subset E$ engendré par un point P de E et le groupe des racines n-èmes de l'unité de $\mathbb{F}_{q^k}$, où n est l'ordre de P. Cet isomorphisme est donné par le couplage de Weil. Miller a développé un algorithme probabiliste en temps polynomial pour calculer le couplage de Weil d'une courbe elliptique, voir [Mil86].

Il sera parfois nécessaire (par exemple pour appliquer le lemme 3.30) de pouvoir choisir aléatoirement et uniformément des points d'une courbe elliptique E en temps polynomial. On procède de la manière suivante : On choisit aléatoirement un point x sur $\mathbb{F}_q$. Si x est la première coordonnées d'un point de $E(\mathbb{F}_q)$, alors pour trouver y tel que $(x,y) \in E(\mathbb{F}_q)$, il suffit de résoudre une racine carrée dans $\mathbb{F}_q$, ce qui est un problème probabiliste en temps polynomial, voir [BO81] pages $395-396$. On pose alors $P=(x,y)$ ou $P=(x,-y)$ si q n'est pas une puissance de 2, sinon on pose $P=(x,y)$ ou $P=(x,y+a_3)$ si l'équation de Weierstrass de E est $y^2+a_3y=x^3+a_4x+a_6$ et $P=(x,y)$ ou $P=(x,y+x)$ si l'équation de Weierstrass de E est $y^2+xy=x^3+a_2x^2+a_6$. Si x n'est pas la première coordonnées d'un point de $E(\mathbb{F}_q)$, on recommence le processus.

Nous allons maintenant énoncer deux lemmes que nous utiliserons par la suite.

Lemme 5.1
Soient G un groupe, $\alpha \in G$ et $n=\prod_{i=1}^m p_i^{k_i}$ la factorisation de $n \in \mathbb{N}$. Alors, l'ordre de α est n si et seulement si $\alpha^n=1$ et $\alpha^{\frac{n}{p_i}} \neq 1$ pour tout $i=1,\ldots,m$.

Lemme 5.2
Soit G un groupe abélien de type (cn,cn). Si les éléments $\{\alpha_i\}$ sont choisis aléatoirement et uniformément dans G, alors les éléments $\{c\alpha_i\}$ sont distribués uniformément dans un sous-groupe de G de type de (n,n).

5.1 La méthode de réduction MOV

Soit $q=p^m$. Soient $E(\mathbb{F}_q)$ une courbe elliptique supersingulière sur un corps fini $\mathbb{F}_q$ avec une structure de groupe (n_1,n_2), où $n_2 \mid n_1$ et $t=q+1-|E(F_q)|$. Soient encore $P \in E(\mathbb{F}_q)$ d'ordre n divisant n_1 et $R \in E(\mathbb{F}_q)$.

Il existe un algorithme en temps polynomial développé par Schoof pour calculer $|E(\mathbb{F}_q)|$, voir [Sch85] page 484. De plus, Miller a trouvé un algorithme probabiliste en temps polynomial pour calculer n_1 et n_2, étant donné la factorisation de $(|E(\mathbb{F}_q)|, q-1)$. On suppose aussi que n est connu. Dans ce cas, le problème du logarithme discret est de trouver $l \in \{0,\ldots,n-1\}$ tel que $R=lP$. Par le lemme 3.30 et comme $e_n(P,P)=1$, on a que $R \in \langle P\rangle$ si et seulement si $nR=O$ et $e_n(P,R)=1$. Ces conditions étant vérifiées de manière probabiliste en temps polynomial, on peut supposer que $R \in \langle P\rangle$.

Comme $E(\mathbb{F}_q)$ est supersingulière, $p \mid t$ et donc $(|E(\mathbb{F}_q)|, q)=1$. Cela implique que $E[n_1] = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z}$.

Par les lemmes 3.28 et 3.29, E appartient à l'une des classes de courbes elliptiques supersingulières suivante :

(I) $t=0$ et $E(\mathbb{F}_q) \cong \mathbb{Z}/(q+1)\mathbb{Z}$;

(II) $t=0, E(\mathbb{F}_q) \cong \mathbb{Z}/(\frac{q+1}{2})\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $q \equiv 3 \pmod 4$;

(III) $t^2 = q$ et m est pair ;

(IV) $t^2 = 2q, p = 2$ et m est impair ;

(V) $t^2 = 3q, p = 3$ et m est impair ;

(VI) $t^2 = 4q$ et m est pair.

Soit $k \in \mathbb{N}$ le plus petit entier tel que $E[n_1] \subset E(\mathbb{F}_{q^k})$.

En appliquant le théorème 3.25 et le lemme 3.29, on peut facilement calculer un tel k. En effet, on cherche le plus petit k tel que $n_1 \mid |E(\mathbb{F}_{q^k})|$. De plus, ceci implique que $E(\mathbb{F}_{q^k})$ est de type (cn_1, cn_1) pour un $c \in \mathbb{N}$. On résume toutes ces informations dans le tableau ci-dessous.

Classe	t	Structure de $E(\mathbb{F}_q)$	n_1	k	Type de $E(\mathbb{F}_{q^k})$	c
I	0	cyclique	$q+1$	2	$(q+1, q+1)$	1
II	0	$\mathbb{Z}/(\frac{q+1}{2})\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\frac{q+1}{2}$	2	$(q+1, q+1)$	2
III	$\pm\sqrt{q}$	cyclique	$q+1 \mp \sqrt{q}$	3	$(q^{\frac{3}{2}} \pm 1, q^{\frac{3}{2}} \pm 1)$	$\sqrt{q} \pm 1$
IV	$\pm\sqrt{2q}$	cyclique	$q+1 \mp \sqrt{2q}$	4	(q^2+1, q^2+1)	$q \pm \sqrt{2q} + 1$
V	$\pm\sqrt{3q}$	cyclique	$q+1 \mp \sqrt{3q}$	6	(q^3+1, q^3+1)	$(q+1)(q \pm \sqrt{3q} + 1)$
VI	$\pm 2\sqrt{q}$	$\mathbb{Z}/(\sqrt{q} \mp 1)\mathbb{Z} \times \mathbb{Z}/(\sqrt{q} \mp 1)\mathbb{Z}$	$q \mp 1$	1	$(\sqrt{q} \mp 1, \sqrt{q} \mp 1)$	1

TABLE 1 – Informations importantes des courbes supersingulières

Nous allons maintenant décrire l'algorithme utilisé pour décrire la réduction du problème du logarithme discret.

5.2 L'algorithme de réduction

Algorithm 6 Algorithme de réduction

Entrée : Un élément P d'ordre n divisant n_1 d'une courbe elliptique supersingulière et $R \in \langle P \rangle$.

Sortie : Un entier $l \in \mathbb{N}$ tel que $R = lP$

1: Déterminer k et c avec la table 1.
2: Choisir un élément $Q' \in \mathbb{F}_{q^k}$ aléatoirement et poser $Q = \frac{cn_1}{n}$.
3: Calculer $\gamma = e_n(P, Q)$ et $\delta = e_n(R, Q)$.
4: Calculer le logarithme discret l' de δ en base γ dans $\mathbb{F}_{q^k}$.
5: Vérifier si $l'P = R$. Si tel est le cas, alors $l = l'$. Sinon, l'ordre de α est plus petit que n et on recommence au point (ii).
6: **return** l'

En appliquant le lemme 5.2 à

$$E(\mathbb{F}_{q^k}) \cong \mathbb{Z}/cn_1\mathbb{Z} \times \mathbb{Z}/cn_1\mathbb{Z}$$

puis à

$$E[n_1] \cong \mathbb{Z}/(\frac{n_1}{n}n)\mathbb{Z} \times \mathbb{Z}/(\frac{n_1}{n}n)\mathbb{Z},$$

on trouve que Q est un point aléatoire de $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. De plus la probabilité que γ soit d'ordre n est $\dfrac{\varphi(n)}{n}$. En effet, comme il y a $\varphi(n)$ éléments d'ordre n dans $\mathbb{F}_{q^k}$ et comme $\langle P \rangle$ est d'indice n, il suffit d'appliquer le lemme 3.30 pour trouver que le nombre d'élément d'ordre n de $E[n]$ est $\varphi(n)n$. Ainsi, la probabilité que α soit d'ordre n est $\dfrac{\varphi(n)n}{n^2}$.

Théorème 5.3
Si $E(\mathbb{F}_q)$ est une courbe elliptique supersingulière, alors la réduction du problème du logarithme discret dans $E(\mathbb{F}_q)$ au problème du logarithme discret dans $\mathbb{F}_{q^k}$ est une réduction probabiliste en temps polynomial (polynôme en $\ln q$).

Démonstration. Pour construire $\mathbb{F}_{q^k}$ depuis $\mathbb{F}_q$, il faut trouver un polynôme irréductible de degré k sur $\mathbb{F}_q$, ce qui peut être fait de manière probabiliste en temps polynomial, voir [BO81] page 395. Dans ce cas, $\mathbb{F}_{q^k} \cong \mathbb{F}_q[X]/\langle f \rangle$. Comme $Q' \in E(\mathbb{F}_{q^k})$ et $k \leq 6$, le point Q' et donc le point Q peuvent aussi être choisis de manière probabiliste en temps polynomial. L'algorithme de Miller permet de calculer γ et δ de manière probabiliste en temps polynomial, voir [Mil86] page 5. De plus, comme $\dfrac{n}{\varphi(n)} \leq 6 \ln \ln n$ pour $n \geq 5$ (voir [RS62], page $71 - 72$), le nombre d'itérations nécessaires pour trouver un γ convenable est $O(\ln \ln n)$. Finalement, $l'P = R$ peut être testé en temps polynomial et $n = O(q)$. □

Notation

(a, b)	Le plus petit diviseur commun des nombres entiers a et b
$\mathbb{A}^n$	L'espace affine de dimension n
C_n	Le groupe cyclique à n éléments
$\mathrm{Car}(K)$	La caractéristique du corps K
$\mathrm{Div}(C)$	Le groupe des diviseurs d'une courbe C
$\mathrm{Div}^0(C)$	Le sous-groupe des diviseurs de degré 0 d'une courbe C
$E(K)$	L'ensemble des points de la courbe elliptique E à coordonnées dans K
$E[m]$	L'ensemble des points de la courbe elliptique E d'ordre divisant m
E_{tors}	L'ensemble des points de la courbe elliptique E d'ordre fini
$\mathbb{F}_q$	Le corps à $q = p^f$ éléments
$I(V)$	L'idéal engendré par l'ensemble algébrique V
$\bar{K}$	Une clôture algébrique fixée du corps K
$\bar{K}[V]$	L'anneau de coordonnée affine sur V
$\bar{K}[V]_P$	L'anneau local de V en P
$\mathcal{L}(D)$	Le $\bar{K}$-espace vectoriel $\{f \in \bar{K}(C)^* : \mathrm{div}(f) \geq -D\} \cup \{0\}$
$l(D)$	La dimension de l'espace vectoriel $\mathcal{L}(D)$
M_P	L'idéal maximal de $\bar{K}[V]_P$
μ_n	Le groupe des racines n-èmes de l'unité
$\mathbb{N}$	$\{1, 2, 3, \ldots\}$
$\mathbb{N}_0$	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{P}^n$	L'espace projectif de dimension n
$\mathrm{Pic}(C)$	Le groupe de Picard d'une courbe C
$V(I)$	L'ensemble algébrique (affine ou projectif) associé à l'idéal I
Ω_C	L'espace des formes différentielles sur une courbe C

Références

[BO81] Michael Ben-Or, *Probabilistic algorithms in finite fields*, Proceedings of the 22nd Annual Symposium on Foundations of Computer Science, 1981, pp. 394–398.

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.

[Har77] Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Mil86] Victor Miller, *Short Programs for Functions on Curves*, http ://crypto.stanford.edu/miller/miller.pdf.

[MOV93] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone, *Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field*, IEEE Trans. Inform. Theory **39** (1993), no. 5, 1639–1646.

[RS62] J. Barkley Rosser and Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[Sch85] René Schoof, *Elliptic Curves over Finite Fields and the Computation of Square Roots mod p*, Math. Comp. **44** (1985), no. 170, 483–494.

[Sch87] ———, *Nonsingular Plane Cubic Curves over Finite Fields*, J. Combin. Theory Ser. A **46** (1987), no. 2, 183–211.

[Sil09] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[Wat69] William C. Waterhouse, *Abelian Varieties over Finite Fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.