# Courbes Elliptiques

# Table des matières

# 1 Équations de Weierstrass

Dans tout le cours $\mathbb{K}$ est un corps commutatif et $\overline{\mathbb{K}}$ une clôture algébrique de $\mathbb{K}$.
On commence par rappeler brièvement la notion d'espace projectif sur $\mathbb{K}$. Soit $n$ un entier $\geqslant 1$. L'ensemble $\mathbb{K}^{n+1}$ est le $\mathbb{K}$-espace vectoriel de dimension $n$. On définit sur $(\mathbb{K}^{n+1})^* = \mathbb{K}^{n+1} \setminus \{0\}$ une relation $\mathcal{R}$ qui identifie les éléments d'une même droite vectorielle.

$$\forall (u,v) \in (\mathbb{K}^{n+1})^* \times (\mathbb{K}^{n+1})^*, \quad u\mathcal{R}v \iff \exists \lambda \in \mathbb{K}^*, \quad u = \lambda v$$

• Cette relation est une relation d'équivalence sur $(\mathbb{K}^{n+1})^*$. L'espace projectif $\mathbb{P}^n(\mathbb{K})$ est par définition l'ensemble quotient $(\mathbb{K}^{n+1})^*/\mathcal{R}$. L'espace projectif $\mathbb{P}^1(\mathbb{K})$ est la droite projective sur $\mathbb{K}$ et l'espace projectif $\mathbb{P}^2(\mathbb{K})$ est le plan projectif sur $\mathbb{K}$.
• Les coordonnées d'un point d'un espace projectif sont appelées **coordonnées homogènes**. Elles sont **non toutes nulles** et sont définies à une constante multiplicative près. Si $u = (x_1, \ldots, x_{n+1})$ est un vecteur non nul de $\mathbb{K}^{n+1}$, la classe de $u$, notée $[u] = [x_1 : x_2 : \cdots : x_{n+1}]$, est constituée de tous les vecteurs non nuls de $\mathbb{K}^{n+1}$ qui sont colinéaires à $u$.
• Si $x_{n+1} \neq 0$, il existe un représentant de $u$ de la forme $(\dfrac{x_1}{x_{n+1}}, \ldots, \dfrac{x_n}{x_{n+1}}, 1)$. Les points de cette forme sont dits les **points finis** de l'espace projectif ou aussi les points à distance finie.
• Si $x_{n+1} = 0$, alors les points de $\mathbb{K}^{n+1}$ de la forme $(x_1, \ldots, x_n, 0)$ appartiennent tous au même hyperplan d'équation $x_{n+1} = 0$. Cet hyperplan est une réunion de classes d'équivalence dans l'espace projectif. Les points de cette forme sont dits les **points à l'infini** de l'espace projectif. Ils constituent **l'hyperplan projectif à l'infini**. L'espace projectif $\mathbb{P}^n(\mathbb{K})$ peut donc être considéré comme la réunion de l'espace affine $\mathbb{A}^n \simeq \mathbb{K}^n$ et de l'hyperplan projectif à l'infini. Ainsi par exemple $\mathbb{P}^1(\mathbb{K}) = \mathbb{K} \cup \{\infty\}$ et $\mathbb{P}^2(\mathbb{K}) = \mathbb{K}^2 \cup D_\infty$. L'espace projectif $\mathbb{P}^n(\overline{\mathbb{K}})$ est noté $\mathbb{P}^n$.

**Définition 1.1** *Une* **courbe de Weierstrass** *est une courbe définie dans le plan projectif* $\mathbb{P}^2$ *par une* **équation homogène de Weierstrass** $F(X,Y,T) = 0$ *où* $F(X,Y,T) \in \overline{\mathbb{K}}[X,Y,T]$ *est le polynôme homogène de Weierstrass défini par :*

$$F(X,Y,T) = (Y^2T + a_1XYT + a_3YT^2) - (X^3 + a_2X^2T + a_4XT^2 + a_6T^3) \qquad a_i \in \overline{\mathbb{K}}$$

*Si les coefficients* $a_i \in \mathbb{K}$ *on dira que la courbe est définie sur* $\mathbb{K}$.

**Proposition 1.2** *Une courbe de Weierstrass a un seul point à l'infini. C'est le point* $[0:1:0]$. *Il est lisse et la droite projective tangente à la courbe en ce point a pour équation* $T = 0$.

**Définition 1.3** *Une équation affine de Weierstrass d'une courbe de Weierstrass s'obtient en posant $x = X/T$ et $y = Y/T$, ou encore en faisant $T = 1$. C'est donc l'équation*

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

Pour simplifier les calculs, on cherchera à faire des changements de coordonnées. Mais un changement quelconque ne préserve pas ces propriétés. Plus précisément :

**Proposition–Définition 1.4** *Un changement de coordonnées projectives transforme* **un polynôme homogène de Weierstrass** *en un autre* **un polynôme homogène de Weierstrass** *(à une unité multiplicative près) si et seulement si il est de la forme :*

$$\begin{cases} X &= u^2X' + rT' \\ Y &= u^3Y' + u^2sX' + tT' \\ T &= T' \end{cases} \qquad \text{avec } u, r, s, t \in \overline{\mathbb{K}} \text{ et } u \neq 0$$

*Deux équations (ou deux courbes) de Weierstrass sont dites* **équivalentes** *si on passe de l'une à l'autre par un tel changement de coordonnées. En particulier, en coordonnées affines on aura*

$$\begin{cases} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{cases} \qquad \text{avec } u, r, s, t \in \overline{\mathbb{K}} \text{ et } u \neq 0$$

## 2 Équation de Weierstrass réduite

On considère une courbe de Weierstrass $E$ d'équation affine

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

Suivant la caractéristique de $\mathbb{K}$ on peut transformer cette équation en une équation équivalente plus simple en utilisant un changement de coordonnées du type (1.4). On a dans tous les cas :

$$\begin{aligned}(2y + a_1x + a_3)^2 &= 4y^2 + a_1^2x^2 + a_3^2 + 4a_1xy + 4a_3y + 2a_1a_3x \\ &= 4(y^2 + a_1xy + a_3y) + (a_1^2x^2 + 2a_1a_3x + a_3^2)\end{aligned}$$

• Si Caract($\mathbb{K}$) $\neq 2$ alors 2 est inversible et on a :

$$\begin{aligned}(E) &\iff \frac{1}{4}(2y + a_1x + a_3)^2 - \frac{1}{4}(a_1^2x^2 + 2a_1a_3x + a_3^2) = x^3 + a_2x^2 + a_4x + a_6 \\ &\iff \left(y + \frac{a_1}{2}x + \frac{a_3}{2}\right)^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}\end{aligned}$$

où

$$\begin{cases} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \end{cases}$$

En posant $y' = y + \frac{a_1}{2}x + \frac{a_3}{2}$ on aura $(E) \iff y'^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$

• Si de plus Carat$(\mathbb{K}) \neq 3$ alors 3 est aussi inversible et on a

$$\begin{aligned} (E) &\iff y'^2 = (x + \frac{b_2}{12})^3 - 3x\frac{b_2^2}{12^2} - \frac{b_2^3}{12^3} + \frac{b_4}{2}x + \frac{b_6}{4} \\ &\iff y'^2 = (x + \frac{b_2}{12})^3 - \frac{b_2^2 - 24b_4}{48}(x + \frac{b_2}{12}) - \frac{-b_2^3 + 36b_2b_4 - 216b_6}{864} \\ &\iff y'^2 = x'^3 - \frac{c_4}{48}x' - \frac{c_6}{864} \end{aligned}$$

où

$$\begin{cases} x' &= x + \frac{b_2}{12} = x + \frac{a_1^2 + 4a_2}{12} \\ y' &= y + \frac{a_1}{2}x + \frac{a_3}{2} \end{cases} \quad \text{et} \quad \begin{cases} c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \end{cases}$$

Donc l'équation $(E)$ est équivalente à une équation de la forme

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

On définit aussi les quantités

$$\begin{cases} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j &= c_4^3/\Delta \text{ si } \Delta \neq 0 \end{cases}$$

**Définition 2.1** *la quantité $\Delta$ est appelé discriminant de l'équation ou de la courbe et est notée $\Delta(E)$ et la quantité $j$ est appelé le j-invariant de l'équation ou de la courbe et est notée $j(E)$.*

**Remarque 2.2** *Remarquons que $b_2, b_4, b_6, c_4, c_6, \Delta \in \mathbb{Z}[a_1, a_2, \cdots, a_6]$ et $1728\Delta = c_4^3 - c_6^2$ :*

$$\begin{cases} c_4 = (a_1^2 + 4a_2)^2 - 24(2a_4 + a_1a_3) \\ c_6 = -(a_1^2 + 12a_1^4a_2 + 48a_1^2a_2^2 + 64a_2^3) - 216(a_3^2 + 4a_6) + 36(a_1^3a_3 + a_1^2a_4 + 8a_2a_4 + 4a_1a_2a_3) \\ \Delta = -{a_1}^6a_6 + {a_1}^5a_3a_4 + \left(-{a_3}^2a_2 - 12\,a_2a_6 + {a_4}^2\right){a_1}^4 + \left({a_3}^3 + 8\,a_3a_2a_4 + 36\,a_3a_6\right){a_1}^3 \\ + \left(72\,a_4a_6 - 30\,{a_3}^2a_4 - 48\,{a_2}^2a_6 - 8\,{a_3}^2{a_2}^2 + 8\,a_2{a_4}^2\right){a_1}^2 \\ + \left(36\,{a_3}^3a_2 + 144\,a_2a_3a_6 + 16\,{a_2}^2a_3a_4 - 96\,a_3{a_4}^2\right)a_1 \\ -27\,{a_3}^4 - 432\,{a_6}^2 - 64\,{a_4}^3 - 16\,{a_3}^2{a_2}^3 - 216\,{a_3}^2a_6 + 16\,{a_2}^2{a_4}^2 + 288\,a_2a_4a_6 \\ +72\,{a_3}^2a_2a_4 - 64\,{a_2}^3a_6 \\ 1728\Delta = c_4^3 - c_6^2 \end{cases}$$

On remarque que si on donne à chaque $a_i$ le degré $i$, $\Delta$ est un polynôme homogène de degré 12. Les résultats ainsi obtenus en caractéristique $\neq 2, 3$ sont résumés dans la proposition suivante :

**Proposition 2.3** *Supposons que la caractéristique de $\mathbb{K}$ est différente de 2 et 3. On a :*

(1) *Toute équation affine de Weierstrass est équivalente à l'équation de la forme $y^2 = x^3 + ax + b$.*

(2) *Deux équations affines de Weierstrass de cette forme sont équivalentes si et seulement si on passe de l'une à l'autre par un changement de coordonnées de la forme $(x, y) = (u^2x', u^3y')$ avec $u \in \overline{K}, u \neq 0$.*

(3) *Pour une équation $E$ sous cette forme réduite $y^2 = x^3 + ax + b$ on a*

$$\begin{cases} c_4 &= -48a \\ c_6 &= -864b \end{cases} \quad \text{et} \quad \begin{cases} \Delta(E) &= -16(4a^3 + 27b^2) \\ j(E) &= \dfrac{2^8 3^3 a^3}{4a^3 + 27b^2} = -1728\dfrac{(4a)^3}{\Delta(E)} \text{ si } \Delta(E) \neq 0 \end{cases}$$

**Proposition 2.4** *Si on fait un changement de coordonnées de la forme de la proposition* (1.4)*, les nouvelles valeurs des quantités $a'_i, b'_i, c'_i, \Delta'$ et du $j$-invariant $j'$ sont telles que :*

$$\begin{cases} ua'_1 &= a_1 + 2s \\ u^2a'_2 &= a_2 - sa_1 + 3r - s^2 \\ u^3a'_3 &= a_3 + ra_1 + 2t \\ u^4a'_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\ u^6a'_6 &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \end{cases}$$

$$\begin{cases} u^2b'_2 &= b_2 + 12r \\ u^4b'_4 &= b_4 + rb_2 + 6r^2 \\ u^6b'_6 &= b_6 + 2rb_4 + r^2b_2 + 4r^3 \\ u^8b'_8 &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \end{cases} \quad \text{et} \quad \begin{cases} u^4c'_4 &= c_4 \\ u^6c'_6 &= c_6 \\ u^{12}\Delta' &= \Delta \\ j' &= j \end{cases}$$

PREUVE : c'est un simple calcul. ∎

En caractéristique 2 et 3 on a le résultat suivant :

**Proposition 2.5** *Soit $E$ une courbe de Weierstrass définie sur un corps $\mathbb{K}$ de caractéristique $p = 2$ ou $p = 3$ par l'équation affine de Weierstrass suivante :*

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

*Alors $E$ est équivalente à une courbe Weierstrass $E'$ d'équation affine de la forme :*

1) $E' : y'^2 = x'^3 + a'_2x'^2 + a'_6$ *si* $p = 3$ *et* $a_1^2 + a_2 \neq 0$ *et on a* $\Delta(E') = -a'^3_2a'_6$, $j \neq 0$

2) $E' : y'^2 = x'^3 + a'_4x' + a'_6$ *si* $p = 3$ *et* $a_1^2 + a_2 = 0$ *et on a* $\Delta(E') = -a'^3_4$, $j = 0$

3) $E' : y'^2 + x'y' = x'^3 + a'_2x'^2 + a'_6$ *si* $p = 2$ *et* $a_1 \neq 0$ *et on a* $\Delta(E') = a'_6$, $j \neq 0$

4) $E' : y'^2 + a'_3y' = x'^3 + a'_4x' + a'_6$ *si* $p = 2$ *et* $a_1 = 0$ *et on a* $\Delta(E') = a'^4_3$, $j = 0$

PREUVE : voir Exercice 1 des TD ∎

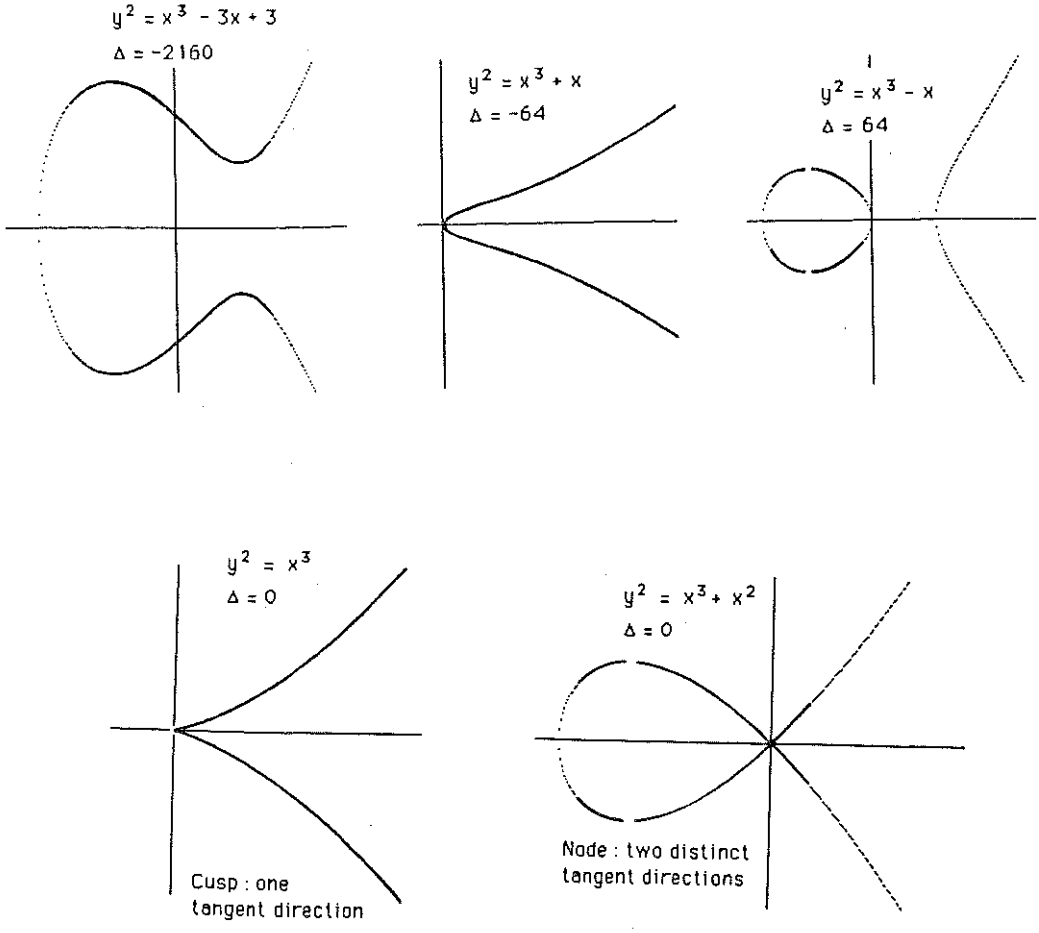
## 3 Exemples de courbes de Weierstrass

Soit $E$ la courbe de Weierstrass définie sur $\mathbb{R}$ par l'équation affine $y^2 = x^3 + ax + b$ et notons $\Delta(E) := -16(4a^3 + 27b^2)$ son discriminant

1) Si $\Delta < 0$ alors le polynôme $f(x) = x^3 + ax + b$ admet une seule racine réelle et le graphe de la courbe admet une seule composante connexe. Si $a > 0$ la courbe admet deux tangentes prallèles à l'axe des abscisses et si $a \leqslant 0$ elle n'a pas de telles tangentes.

2) Si $\Delta > 0$ alors $f(x)$ admet trois racines réelles distinctes et le graphe de la courbe admet deux composantes connexes dont une seule compacte.

3) Si $\Delta = 0$ alors la cubique est singulière. Le polynôme $f(x)$ admet une racine au moins double : $f(x) = (x - c)^2(x - d)$ avec $2c + d = 0$ car $2c + d$ est le coefficient de $x^2$. Si $c > d$ alors le graphe de $E$ admet une seule composante connexe avec un point double en $x = c$ et deux tangentes en ce point de pentes réelles distinctes. C'est un noeud. Si $c < d$ le graphe de $E$ est formé d'un point singulier $(c, 0)$ où les tangentes sont de pentes imaginaires pures et d'une composante connexe non compacte. Si $c = d$ alors $c = d = 0$ car $2c + d = 0$ et la courbe a pour équation $y^2 = x^3$. Son graphe est un bec et admet une pointe au point singulier $(0, 0)$.




$E_1 :\ y^2 = x^3 - 3x + 3 \quad \Delta = -2160$

$E_2 :\ y^2 = x^3 + x \quad \Delta = -64, j = 1728$

$E_3 :\ y^2 = x^3 - x \quad \Delta = 64$

$E_4 :\ y^2 = x^3 \quad \Delta = 0$

$E_5 :\ E_5 : y^2 = x^3 + x^2 \quad \Delta = 0$

Les courbes $E_1, E_2, E_3$ sont des courbes lisses sur $\mathbb{R}$ car $\Delta \neq 0$. Par contre $E_4 : y^2 = x^3$ et $E_5 : y^2 = x^3 + x^2$ sont des courbes singulières sur $\mathbb{R}$ car $\Delta = 0$. Les points affines de $E_4(\mathbb{R})$ forment un cusp ou pointe avec un point singulier $(0, 0)$ et deux tangentes confondues en ce point, et les points affines de $E_5(\mathbb{R})$ forment un noeud avec un point singulier en $(0, 0)$ avec deux tangentes distinctes en ce point. Les points affines de $E_1(\mathbb{R})$ et de $E_2(\mathbb{R})$ forment une seule composante connexe ($\Delta < 0$) et ceux de $E_3(\mathbb{R})$ forment deux composantes connexes ($\Delta > 0$).

# 4 Courbes elliptiques

**Proposition 4.1** *Une courbe de Weierstrass $E$ est lisse si et seulement si $\Delta(E) \neq 0$. Si $\Delta(E) = 0$ alors $E$ admet un seul point singulier. Plus précisément, si $c_4(E) \neq 0$, on dit que c'est un noeud et si $c_4(E) = 0$, c'est une pointe ou point de rebroussement.*

**Définition 4.2** *Une* **courbe elliptique** *est un couple $(E, \mathcal{O})$ où $E$ est une courbe projective lisse de genre 1 et $\mathcal{O}$ un point de $E$, qui est le* **point de base** *ou l'***origine***. Elle est définie sur $\mathbb{K}$ si $E$ est définie sur $\mathbb{K}$ et si $\mathcal{O} \in E(\mathbb{K})$. On dira aussi que c'est une courbe pointée. On dira parfois "soit $E$ une courbe elliptique", cela sous-entendra toujours qu'il y a une origine fixée.*

Dans ce cours on ne va pas utiliser cette définition où les termes utilisés nécessitent eux même d'être définis mais on va utiliser une définition plus simple qui lui est équivalente.
Une courbe de Weierstrass lisse munie de son point à l'infini $[0 : 1 : 0]$ est une courbe elliptique d'origine $\mathcal{O} = [0 : 1 : 0]$. En effet son degré est 3 car le polynôme homogène de Weierstrass qui la définit est de degré $d = 3$, donc son genre est égal à $g := (d-1)(d-2)/2 = 1$ et elle est projective ( car $= I(F)$ où $F$ un polynôme homogène) et lisse (déjà vu). En fait, toute courbe elliptique $(E, \mathcal{O})$ est isomorphe à une courbe de Weierstrass $C \subset \mathbb{P}^2$ par un isomorphisme qui envoie le point de base $\mathcal{O}$ de $E$ sur le point à l'infini $[0 : 1 : 0]$ de la courbe de Weierstrass $C$. Plus précisément, on a le résultat suivant :

**Proposition–Définition 4.3** *Soit $(E, \mathcal{O})$ une courbe elliptique définie sur $\mathbb{K}$. Alors il existe des fonctions $x, y \in \mathbb{K}(E)$ telles que l'application*

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

*soit un isomorphisme de $E$ sur une courbe de Weierstrass $C \subset \mathbb{P}^2$ définie par une équation*

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

*où $a_i \in \mathbb{K}$ et tel que $\phi(\mathcal{O}) = [0 : 1 : 0] \in C$.*
*L'équation de $C$ est l'équation de Weierstrass de $E$ correspondant à $\phi$, et les coordonnées $x$ et $y$ qui interviennent dans cette équation sont des coordonnées de Weierstrass de $E$.*

**Dans ce cours une courbe elliptique sera donc une courbe de Weierstrass lisse.** Pour démontrer ce résultat on a besoin du théorème de Riemann qu'on rappelle et on admet ici

**Théorème 4.4 (Riemann pour les courbes de genre 1(admis))** *Soient $C$ une courbe projective lisse de genre 1 et $D$ un diviseur sur $C$ de degré $> 0$. On associe à $D$ l'ensemble de fonctions $\mathcal{L}(D) = \{f \in \overline{\mathbb{K}}(C) \setminus \{0\} \mid \mathrm{div}(f) + D \geqslant 0\} \cup \{0\}$. Alors, $\mathcal{L}(D)$ est un $\overline{\mathbb{K}}$-espace vectoriel de dimension finie notée $\ell(D)$ et on a $\ell(D) = \deg D$.*

**Définition 4.5** *Une courbe elliptique $E$ définie sur un corps $\mathbb{K}$ est une courbe de Weierstrass lisse définie sur $\mathbb{K}$. Son point à l'infini est toujours noté $\mathcal{O}$. Si $f(x, y)$ est une équation affine de Weierstrass de $E$ alors pour toute extension $L$ de $\mathbb{K}$, l'ensemble $\{(x, y) \in L \times L / f(x, y) = 0\} \cup \{\mathcal{O}\}$ est noté $E(L)$. En particulier on a*

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K} \times \mathbb{K} / f(x, y) = 0\} \cup \{\mathcal{O}\} et$$
$$E(\overline{\mathbb{K}}) = E = \{(x, y) \in \overline{\mathbb{K}} \times \overline{\mathbb{K}} / f(x, y) = 0\} \cup \{\mathcal{O}\}$$

# 5 Loi d'addition sur une courbe elliptique

*Rappel du cours sur les courbes algébriques* : Soit $C$ une courbe **projective lisse** sur $\mathbb{K}$. Le **groupe des diviseurs** de $C$ noté $\mathrm{Div}(C)$ est le groupe abélien libre engendré par les points de $C$. C'est l'ensemble des écritures formelles

$$D = \sum_{P \in C} n_P(P) \text{ où les } n_P \in \mathbb{Z}, \text{ tous nuls sauf un nombre fini}$$

muni de la loi d'addition naturelle obtenue par l'addition des coefficients $n_P$. Le diviseur nul est celui où $n_P = 0$ pour tout $P \in C$. Le **support** de $D$ est l'ensemble des points $P$ tels que $n_P \neq 0$. Le diviseur $D$ est dit **positif** si, $n_P \geqslant 0$ pour tout point $P \in C$. Le **degré** de $D$ est

$$\deg D := \sum_{P \in C} n_P$$

Soit $C$ une courbe algébrique (de Weierstrass ou pas) sur $\mathbb{K}$ et soit $F \in \overline{\mathbb{K}}[X, Y, T]$ un polynôme homogène non nul et non identiquement nul sur $C$. On associe à $F$ le diviseur $\mathrm{zeros}(F) \in \mathrm{Div}(C)$ :

$$\mathrm{zeros}(F) := \sum_{P \in C; F(P) = 0} (P)$$

On appelle **droite projective de** $\mathbb{P}^2$ tout polynôme homogène $L$ de la forme $L = \alpha X + \beta Y + \gamma T$ où $\alpha, \beta, \gamma \in \overline{\mathbb{K}}$ non tous nuls. La proposition suivante permet de définir rigoureusement la notion de points alignés sur une courbe elliptique.

**Proposition–Définition 5.1 (Intersection avec une droite)** *Soient $E$ une courbe elliptique sur $\mathbb{K}$ et soit $L = \alpha X + \beta Y + \gamma T$ une droite de $\mathbb{P}^2$. Alors le diviseur* $\text{zeros}(L) \in \text{Div}(E)$ *est positif de degré 3 autrement dit*

$$\text{zeros}(L) = (P) + (Q) + (R)$$

*où $P, Q, R$ sont des points de $E$ non nécessairement distincts.*
*On dira que 3 points $P$, $Q$, $R$ (non nécessairement distincts) de $E$ sont* **alignés** *s'il existe $L$ homogène de degré 1 non nul tel que* $\text{zeros}(L) = (P) + (Q) + (R)$. *Si $P = Q$, la droite d'équation $L$ est la tangente à $E$ en $P$. Si $P = Q = R$, $P$ est un point d'inflexion de $E$ .*

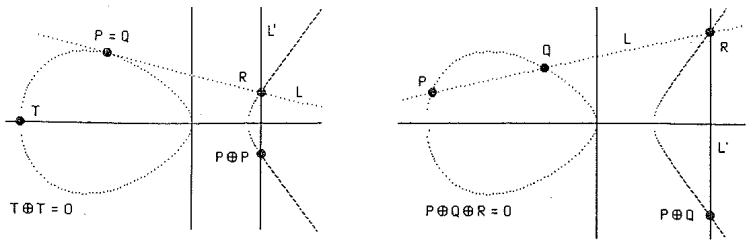
**Corollaire 5.2** *Sur une courbe elliptique d'équation projective $F(X, Y, T) = 0$, on a*

$$\text{zeros}(X) = (P_1) + (P_2) + (\mathcal{O})$$
$$\text{zeros}(Y) = (Q_1) + (Q_2) + (Q_3)$$
$$\text{zeros}(T) = 3(\mathcal{O})$$

*où les $P_i$ et les $Q_i$ sont des points de $E$ pas forcément distincts.*

**Corollaire 5.3** *Soient $E$ une courbe elliptique sur $\mathbb{K}$ et soient $P$ et $Q$ (non nécessairement distincts) deux points de $E$. Il existe un unique point $R \in E$ tel que $P$, $Q$ et $R$ soient alignés.*

**Définition 5.4 (Loi de composition sur $E$)** *Soient $E$ une courbe elliptique et $\mathcal{O}$ son point à l'infini. Si $P$ et $Q$ sont deux points de $E$, d'après* (5.3) *il existe un unique point $R \in E$ tel que $P$, $Q$ et $R$ soient alignés sur une droite $L$. Il existe un unique point $S \in E$ tel que $R$ , $\mathcal{O}$ et $S$ soient alignés sur une droite $L'$. On pose alors $P + Q = S$.*




**Théorème 5.5 (Structure de groupe sur E)** *Soient $E$ une courbe elliptique sur $\mathbb{K}$ et $\mathcal{O}$ son point à l'infini. La loi de composition* (5.4) *munit $E$ d'une structure de groupe commutatif d'élé-*

*ment neutre $\mathcal{O}$ telle que si $E$ est définie sur $\mathbb{K}$ alors $E(\mathbb{K})$ en soit un sous-groupe, et telle que si 3 points $P$, $Q$ et $R$ sont alignés alors on a l'égalité $(P+Q)+R=\mathcal{O}$.*

**Proposition 5.6 (Formules explicites de la loi de groupe)** *Soit $E$ une courbe elliptique de point à l'infini $\mathcal{O}$ et d'équation affine*

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

(1) *Si $P_0 = (x_0, y_0) \in E$ alors $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$*

(2) *Si $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E$ et si $P_1 \neq -P_2$ alors $P_1 + P_2 = (x_3, y_3)$ où*

$$\begin{cases} x_3 &= -x_1 - x_2 - a_2 + m(m + a_1) \\ \\ y_3 &= -y_1 - a_3 - a_1x_3 + m(x_1 - x_3) \end{cases} \quad et\ m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{si} \quad P_1 \neq P_2 \\ \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{si} \quad P_1 = P_2 \end{cases}$$

# 6 Equation de Legendre d'une courbe elliptique

**Proposition 6.1** (1) *Deux courbes elliptiques sont équivalentes (sur $\overline{\mathbb{K}}$) si et seulement si elles ont le même $j$-invariant.*

(2) *Soit $j_0 \in \overline{\mathbb{K}}$. Il existe une courbe elliptique dont le $j$-invariant est égal à $j_0$. Donc le $j$-invariant permet d'établir une bijection entre $\overline{\mathbb{K}}$ et les classes d'équivalence de courbes elliptiques.*

Nous introduisons maintenant une autre forme réduite d'une équation d'une courbe elliptique dite forme de Legendre, utile dans certains contextes.

**Proposition 6.2** *Si la caractéristique de $\mathbb{K}$ est différente de 2 , on a :*

1) *Toute courbe elliptique $E$ est équivalente, sur $\overline{\mathbb{K}}$, à une courbe de la forme*

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

*avec $\lambda \in \overline{\mathbb{K}}$, $\lambda \neq 0, 1$. On dit qu'elle est sous* **forme de Legendre**.

2) *Le $j$-invariant de $E_\lambda$ vaut*

$$j(E_\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

3) *Deux équations de Legendre sont équivalentes au sens de* (1.4) *si on passe de l'une à l'autre par un changement de coordonnées de la forme : $x = u^2x' + r$, $y = u^3y'$, avec*

$$(r, u^2) \in \{(0,1), (0,\lambda), (1,-1), (1,\lambda-1)(\lambda,-\lambda), (\lambda, 1-\lambda)\}.$$

*Plus précisément, l'application*

$$j : \overline{\mathbb{K}} \setminus \{0,1\} \longrightarrow \overline{\mathbb{K}}, \quad \lambda \longmapsto j(E_\lambda)$$

*est surjective et on a pour tout* $j_0 \in \overline{\mathbb{K}}$

$$Card\ \{\lambda \in \overline{\mathbb{K}} \setminus \{0,1\}\ ;\ j(E_\lambda) = j_0\} = \begin{cases} 2 & si \quad j_0 = 0 \\ 3 & si \quad j_0 = 1728 \\ 6 & si \quad j_0 \neq 0, 1728 \end{cases}$$

# 7 Fonctions sur une courbe elliptique

Dans ce paragraphe on rappelle les notions de fonction polynôme et de fonction rationnelle sur une courbe elliptique. Le corps de fonctions d'une telle courbe sera le corps des fonctions rationnelles sur la courbe. Dans toute cette section on considère une courbe elliptique $E$ définie par le polynôme affine de Weierstrass

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \in \overline{\mathbb{K}}[x,y]$$

Deux polynômes $P, Q \in \overline{\mathbb{K}}[X,Y]$ seront dits équivalents s'ils prennent la même valeur en tout point de la courbe $E$ *i.e.* si $P-Q$ est un multiple de $f$. Par exemple le polynôme $Y^2$ est équivalent au polynôme $-(a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6)$.

**Définition 7.1 (anneau des coordonnées )** *L'anneau de coordonnées de la courbe $E$ d'équation $f(x,y) = 0$, est l'anneau, noté $\overline{\mathbb{K}}[E] := \overline{\mathbb{K}}[x,y]/(f(x,y))$, où $(f(x,y))$ est l'idéal de $\overline{\mathbb{K}}[x,y]$ engendré par $f(x,y)$. Un élément de $\overline{\mathbb{K}}[E]$ est appelé fonction polynôme sur $E$.*

Soit $g(x,y) \in \overline{\mathbb{K}}[E]$. Il est toujours possible de remplacer $y^2$ par $-(a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6)$ pour se ramener de proche en proche à une **forme réduite** de la forme

$$g(x,y) = p(x) + yq(x) \text{ où } p(x), q(x) \in \overline{\mathbb{K}}[x]$$

**Proposition 7.2** *La forme réduite d'une fonction polynôme est unique. Cela signifie que l'anneau de coordonnées $\overline{\mathbb{K}}[E]$ d'une courbe elliptique $E$ est un module libre de type fini sur l'anneau de polynômes $\overline{\mathbb{K}}[x]$ et que la famille $\{1, y\}$ en est une base.*

**Définition 7.3 (conjugué, norme, degré)** *Soit $g(x,y) = p(x) + yq(x)$ la forme réduite d'une fonction polynôme $g \in \overline{\mathbb{K}}[E]$ pour une courbe elliptique $E$.*

*Le* **conjugué** *de $g$ est défini par* $\overline{g}(x,y) := p(x) - yq(x)$.

*La* **norme** *de $g$ est définie par* $n(g) := g\overline{g} = p(x)^2 - y^2q(x)^2$.

*Le* **degré** *de $g$ est défini par* $\deg(g) := \deg_x(n(g))$.

Les propriétés qui suivent découlent immédiatement des définitions

(1) Pour tous $g, h \in \overline{\mathbb{K}}[E]$ on a $\overline{g+h} = \overline{g} + \overline{h}$ ; $\overline{gh} = \overline{g}\overline{h}$ et $\overline{\overline{g}} = g$

(2) $\deg(x) = 2$ car $n(x) = x^2$ et $\deg_x(x^2) = 2$.

(3) $\deg(y) = 3$ car $n(y) = y^2 = x^3 + a_2x^2 + (a_4 - a_1y)x + a_6 - a_3$ donc $\deg_x(y^2) = 3$

(4) Pour tous $g, h \in \overline{\mathbb{K}}[E]$ on a $n(gh) = n(g)n(h)$ car $(gh)\overline{gh} = g\overline{g}h\overline{h}$

(5) Il s'ensuit que, pour tous $g, h \in \overline{\mathbb{K}}[E]$, on a $\deg(gh) = \deg(g) + \deg(h)$

(6) En particulier, pour tout entier $k \in \mathbb{N}^*$, $\deg(x^k) = 2k$ et $\deg(y^k) = 3k$

(7) Pour tout $g \in \overline{\mathbb{K}}[E]$ on a $\deg(g) = \deg(\overline{g})$ car $n(g) = n(\overline{g})$

(8) $n(g) = 0 \iff g = 0$ car $n(g) = p(x)^2 - y^2q(x)^2$ est la somme d'un polynôme de degré pair et d'un polynôme de degré impair en $x$, ne peut être nulle que si les deux termes sont nuls.

(9) Puisque $\deg(y) = 3$ alors

$$\deg(p(x) + yq(x)) = \begin{cases} \max\{2\deg_x(p), 3 + 2\deg_x(q)\} & si \quad q \neq 0 \\ 2\deg_x(p) & si \quad q = 0 \end{cases}$$

**Remarque 7.4**

Le polynôme $f = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6 \in \overline{\mathbb{K}}[X,Y]$ est irréductible dans $\overline{\mathbb{K}}[X,Y]$. En effet, si $f$ se factorise dans $\overline{\mathbb{K}}[X,Y]$, c'est nécessairement sous la forme

$$f = Y^2 + (a_1X + a_3)Y - (X^3 + a_2X^2 + a_4X + a_6) = (Y - p)(Y - q)$$

comme polynôme de $\overline{\mathbb{K}}[X][Y]$ de degré 2 en $Y$ et où $p, \in \overline{\mathbb{K}}[X]$. Mais alors dans $\overline{\mathbb{K}}[X]$

$$\deg(pq) = \deg p + \deg q = \deg(-X^3 - a_2X^2 - a_4X - a_6) = 3$$

Donc l'un des polynômes $p$ ou $q$ est de degré 0 et l'autre 3 ou bien l'un de degré 1 et l'autre de degré 2. Dans tous les cas $\deg(p+q) = 2$ ou 3. Or $\deg(p+q) = \deg(a_1X + a_3)$ donc $\deg(p+q) \leqslant 1$. Ainsi, l'anneau de coordonnées $\overline{\mathbb{K}}[E] = \overline{\mathbb{K}}[x,y]/(f(x,y))$ de la courbe $E$ est un anneau intègre. Il admet donc un corps de fractions qu'on note $\overline{\mathbb{K}}(E)$.

**Définition 7.5 (Corps de fonctions sur $E$)** *Pour une courbe elliptique $E$, on appelle corps de fonctions sur $E$, le corps des fractions de l'anneau de coordonnées $\overline{\mathbb{K}}[E]$. On le note $\overline{\mathbb{K}}(E)$ et ses éléments sont appelés des fonctions rationnelles sur $E$ ou fonctions sur $E$.*

Si deux fractions rationnelles $\dfrac{g_1(x,y)}{h_1(x,y)}$ et $\dfrac{g_2(x,y)}{h_2(x,y)}$ représentent la même fonction rationnelle dans $\overline{\mathbb{K}}(E)$ alors $g_1h_2 = h_1g_2$ donc $\deg(g_1)\deg(h_2) = \deg(h_1)\deg(g_2)$ ou encore $\deg(g_1) - \deg(h_1) = \deg(g_2) - \deg(h_2)$. Ceci permet de définir le degré d'une fonction rationnelle sur $E$, pour n'importe quel représentant $g/h$ de la fonction rationnelle, par :

$$\deg\left(\frac{g}{h}\right) = \deg(g) - \deg(h)$$

**Valeur d'une fonction rationnelle en un point de $E$**

On veut ici associer à toute fonction $r \in \overline{\mathbb{K}}(E)$ une application notée encore $r$

$$r : E \longrightarrow \mathbb{P}^1$$

partout définie sur la courbe. Par exemple sur la courbe $E$ d'équation $y^2 = x^3 - x$, la fonction $r(x,y) = x/y$ n'est à priori pas définie au point $P = (0,0)$ de la courbe. Mais on peut transformer cette écriture, pour obtenir un autre représentant de $r(x,y)$ défini en $P$. En effet,

$$g(x,y) = \frac{x}{y} = \frac{xy}{y^2} = \frac{xy}{x^3 - x} = \frac{y}{x^2 - 1}$$

qui est définie en $P$ et qui vaut $r(P) = r(0,0) = 0$.

**Définition 7.6 (point régulier, pôle)** *Soit $E$ une courbe de Weierstrass, $r \in \overline{\mathbb{K}}(E)$ une fonction rationnelle* **non nulle** *sur $E$ et $P$ un point fini de $E$. On dit que $P$ est un point* **régulier** *pour la fonction rationnelle $r$ s'il existe un représentant $g/h$ de $r$ pour lequel $h(P) \neq 0$. Dans le cas contraire on dit que $P$ est* **un pôle** *pour $r$. Pour le point à l'infini, on dit que $\mathcal{O}$ est un pôle de la fonction rationnelle $r$ si $\deg(r) > 0$.*

**Exemple 7.7**

• Sur la courbe d'équation $y^2 = x^3 - x$, la fonction $r = \dfrac{y + x - 1}{x - 1}$ admet un pôle en $P = (1,0)$, car comme $y^2 = x(x-1)(x+1)$, on a $r = \dfrac{x(x+1) + y}{y} = \dfrac{g}{h}$ avec $g(P) = 2$ et $h(P) = 0$.

• Le point $\mathcal{O}$ est pôle pour la fonction $r = \dfrac{y + x + 1}{x + 1} = \dfrac{g}{h}$ car $\deg(g) = 3$ et $\deg(h) = 2$ donc $\deg(f) = \deg(g) - \deg(h) = 1 > 0$.

**Définition 7.8 (valeur d'une fonction en un point)** *Soit $E$ une courbe de Weierstrass, $r \in \overline{\mathbb{K}}(E) \setminus \{0\}$ une fonction non nulle sur $E$ et $P$ un point de $E$. La valeur de $r$ en $P$ est l'élément $r(P) \in \mathbb{P}^1(\overline{\mathbb{K}}) = \mathbb{P}^1 = \overline{\mathbb{K}} \cup \{\infty\}$ et défini par :*

1) *si $P$ est régulier pour $r$, alors $r(P) = \dfrac{g(P)}{h(P)}$ pour un représentant $\dfrac{g}{h}$ de $r$ tel que $h(P) \neq 0$. Si de plus $r(P) = 0$ on dit que $P$ est un zéro de $r$*

2) *si $P$ est un pôle pour $r$ alors $r(P) = \infty$*

3) *si $\deg(r) < 0$ alors $r(\mathcal{O}) = 0$*

4) *si $\deg(r) > 0$ alors $r(\mathcal{O}) = \infty$*

5) *si $\deg(r) = 0$ alors $r(\mathcal{O}) = a/b$ où $a$ et $b$ sont les coefficients dominants respectifs de $g$ et $h$ et où $g/h$ est un représentant de $r$.*

**Exemple 7.9** $x(\mathcal{O}) = \infty$, $y(\mathcal{O}) = \infty$, $\dfrac{x}{y}(\mathcal{O}) = 0$, $\dfrac{y}{x}(\mathcal{O}) = \infty$, $\dfrac{x^3}{y^2}(\mathcal{O}) = 1$

# 8 Uniformisante sur une courbe elliptique

**Proposition–Définition 8.1 (uniformisante et ordre)** *Soit $P$ un point d'une courbe elliptique $E$. Une uniformisante en $P$ est une fonction $u \in \overline{\mathbb{K}}(E) \setminus \{0\}$ dont la valeur est nulle en $P$ et telle que toute fonction rationnelle $f \in \overline{\mathbb{K}}(E) \setminus \{0\}$ s'exprime sous la forme $f = u^d r$ avec $d \in \mathbb{Z}$ et $r \in \overline{\mathbb{K}}(E)$ dont $P$ n'est ni zéro ni pôle i.e. $r(P) \neq 0, \infty$. Si elle existe, une uniformisante en $P$ n'est pas unique mais l'entier $d$ ne dépend pas de l'uniformisante. Il est appelé l'ordre de $f$ en $P$ et est noté $d = \mathrm{ord}_P(f)$.*

**Remarque 8.2** *si $P$ est un zéro de $f$ alors $\mathrm{ord}_P(f) \geqslant 1$, si $P$ est un pôle de $f$ alors $\mathrm{ord}_P(f) \leqslant -1$ et si $P$ est un point régulier et $f(P) \neq 0$ alors $\mathrm{ord}_P(f) = 0$.*

**Proposition 8.3 (propriétés de l'ordre)** *Soit $E$ une courbe elliptique définie sur un corps $\mathbb{K}$. Pour toutes fonctions $f, g \in \overline{\mathbb{K}}(E) \setminus \{0\}$ et pour tout point $P$ de $E$ on a $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$ et $\mathrm{ord}_P(f+g) \geqslant \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g))$ et l'inégalité devient une égalité si $\mathrm{ord}_P(f) \neq \mathrm{ord}_P(g)$. En d'autres termes, $\mathrm{ord}_P$ est une valuation discrète du corps $\overline{\mathbb{K}}(E)$.*

**Proposition 8.4 (caractérisation des uniformisantes)** *Soit $P$ un point d'une courbe elliptique $E$. Une fonction $v \in \overline{\mathbb{K}}(E)$ est une uniformisante en $P$ si et seulement si $\mathrm{ord}_P(v) = 1$.*

On veut montrer qu'en tout point de $E$ il existe une uniformisante en l'explicitement. On distingue le point $\mathcal{O}$ et les points finis de $E$. Pour les points finis on a besoin de différencier ce qu'on appelle les points ordinaires et les points spéciaux.

**Définition 8.5 (point ordinaire, point spécial)** *On dit qu'un point fini $P$ d'une courbe elliptique est un point spécial si $P = -P$. Un point ordinaire est un point fini non spécial.*

**Remarque 8.6** *En caractéristique $\neq 2$, il existe toujours 3 points spéciaux distincts sur une courbe elliptique $E$. En effet, dans ce cas, $E$ est équivalente à une courbe d'équation $y^2 = x^3 + ax^2 + bx + c$ et un point $P = (x_0, y_0)$ est spécial ssi $(x_0, y_0) = (x_0, -y_0)$ donc ssi $y_0 = 0$ et donc $x_0$ est racine du polynôme $P = x^3 + ax^2 + bx + c$. Or ce polynôme, de degré 3 admet 3 racines dans $\overline{\mathbb{K}}$ et ces racines sont distinctes car une racine multiple de $P$ sera l'abscisse d'un point singulier de $E$. Or $E$ est lisse. Les points ordinaires sont donc les points finis de $E$ tels que $y_P \neq 0$.*

**Exercice 8.7** *En caractéristique 2, étudier les points $P \in E$ tels que $y_P = 0$ puis étudier les points spéciaux de $E$.*

**Théorème 8.8** *Soit $E$ une courbe elliptique définie sur un corps $\mathbb{K}$ par l'équation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Alors*

(1) *La fonction $\dfrac{x}{y}$ est une uniformisante au point $\mathcal{O}$ et $\forall f \in \overline{\mathbb{K}}[E] \setminus \{0\}, \mathrm{ord}_{\mathcal{O}}(f) = -\deg(f)$*

(2) *la fonction $x - x_0$ est une uniformisante en tout point ordinaire $P_0 = (x_0, y_0)$*

(3) *la fonction $y - y_0$ est une uniformisante en tout point spécial $P_0 = (x_0, y_0)$. En particulier en caractéristique $\neq 2, 3$, la fonction $y$ est une uniformisante en tout point spécial.*

# 9 Diviseurs principaux sur une courbe elliptique

**Lemme 9.1** *Soit $E$ une courbe elliptique définie sur un corps $\mathbb{K}$. Pour tout point $P$ de $E$ et pour toute fonction $f \in \overline{\mathbb{K}}(E) \setminus \{0\}$ on a : $\mathrm{ord}_P(f) = \mathrm{ord}_{-P}(\overline{f})$*

**Proposition 9.2** *Soit $E$ une courbe elliptique définie sur un corps $\mathbb{K}$ et soit $f \in \overline{\mathbb{K}}(E) \setminus \{0\}$ une fonction sur $E$. Alors la fonction $f$ a un nombre fini de zéros et de pôles sur $E$ et si elle n'a ni zéros ni pôles elle est constante. Enfin, on a $\displaystyle\sum_{P \in E} \mathrm{ord}_P(f) = 0$.*

**Exercice 9.3 Traiter le cas de la caractéristique 2.**

**Corollaire 9.4 (surjectivité des fonctions rationnelles)** *Soit $E$ une courbe elliptique sur un corps $\mathbb{K}$ et soit $f \in \overline{\mathbb{K}}(E)$ une fonction rationnelle non constante. Alors $f$ définit une application* **surjective** *notée encore $f : E \longrightarrow \mathbb{P}^1$.*

Soit $E$ une courbe elliptique sur $\mathbb{K}$. La proposition (9.2) permet d'associer à toute fonction rationnelle non nulle $f \in \overline{\mathbb{K}}(E)$ le diviseur de degré 0 noté $\mathrm{div}(f) \in \mathrm{Div}(E)$, défini par :

$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f)(P) \in \mathrm{Div}(E)$$

Les propriétés suivantes découlent de la définition. Si $f \notin \overline{\mathbb{K}}$, $\mathrm{div}(f) \neq 0$. Les fonctions constantes non nulles ont un diviseur nul et si $f$ et $g$ sont deux fonctions nulles de $\overline{\mathbb{K}}(E)$ on a

$$\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g) \text{ et } \mathrm{div}(f/g) = \mathrm{div}(f) - \mathrm{div}(g)$$

**Exemple 9.5** *Soit $E$ la courbe elliptique définie sur $\mathbb{K}$ par l'équation $y^2 = (x-e_1)(x-e_2)(x-e_3)$ où $e_i$ sont distincts dans $\mathbb{K}$. On pose $P_i = (e_i, 0) \in E$. On a alors*

$$\mathrm{div}(x - e_i) = 2(P_i) - 2(\mathcal{O})$$
$$\mathrm{div}(y) = (P_1) + (P_2) + (P_3) - 3(\mathcal{O})$$
$$\mathrm{div}(x) = (Q) + (-Q) - 2(\mathcal{O})$$

*où $Q = (0, \beta) \in E$ avec $\beta \in \overline{\mathbb{K}}$ est l'un des deux éléments de $\overline{\mathbb{K}}$ tels que $\beta^2 = -e_1e_2e_3$*

**Définition 9.6** *Soit $E$ une courbe elliptique sur $\mathbb{K}$. Un diviseur $D \in \mathrm{Div}(E)$ est principal s'il existe une fonction $f \in \overline{\mathbb{K}}(E) \setminus \{0\}$ telle que $D = \mathrm{div}(f)$. On dit que deux diviseurs $D_1$ et $D_2$ de $\mathrm{Div}(E)$ sont* **linéairement équivalents** *et on note $D_1 \sim D_2$ si $D_1 - D_2$ est un diviseur principal i.e. s'il existe $f \in \overline{\mathbb{K}}(E) \setminus \{0\}$ telle que $D_1 - D_2 = \mathrm{div}(f)$.*

**Proposition 9.7** *Soient $P$ et $Q$ deux points finis distincts d'une courbe elliptique $E$. Alors les diviseurs $(P) + (Q)$ et $(P + Q) + (\mathcal{O})$ sont linéairement équivalents. Plus précisément :*
*1) si $Q = -P$ on a*

$$(P) + (Q) - (P + Q) - (\mathcal{O}) = \mathrm{div}(x - x_P)$$

*2) si $Q \neq -P$. On pose $S = P + Q \neq \mathcal{O}$. On note $f(x, y)$ la droite passant par $P$ et $Q$ et $d(x, y)$ la droite passant par $S$ et $-S$ ($d$ est la tangente à $E$ en $S$ si $S = -S$), alors on a :*

$$(P) + (Q) - (P + Q) - (\mathcal{O}) = \mathrm{div}\left(\frac{f(x, y)}{d(x, y)}\right)$$

**Définition 9.8 (Norme et somme d'un diviseur)** *Soit $E$ une courbe elliptique. Soit $D = \sum_{P\in E} n_P(P) \in \mathrm{Div}(E)$. La norme de $D$, notée $\mid D \mid$ est la somme des valeurs absolues des coefficients des points finis du support de $D$. On a donc $\mid D \mid = \sum_{P\neq\mathcal{O}} \mid n_P \mid$. Les diviseurs de norme 1 sont donc de la forme $D = \pm(P) + n(\mathcal{O})$ pour $n \in \mathbb{Z}$ et $P \neq \mathcal{O}$.*
*La somme de $D$ notée $som(D)$ est le point de $E$ défini par $som(D) = \sum_{P\in E} n_P P$*

**Proposition 9.9 (réduction linéaire d'un diviseur)** *Soit $E$ une courbe elliptique. Pour tout diviseur $D \in \mathrm{Div}(E)$ il existe un diviseur $D_1 \in \mathrm{Div}(E)$ linéairement équivalent à $D$, de même degré et de norme $\mid D_1 \mid \leqslant 1$.*

**Lemme 9.10** *si $P$ et $Q$ sont deux points d'une courbe elliptique alors $(P) \sim (Q) \iff P = Q$*

**Proposition 9.11 (caractérisation des diviseurs principaux)** *Un diviseur d'une courbe elliptique est principal si et seulement si son degré est nul et sa somme est $\mathcal{O}$.*

## 10 Morphismes de courbes elliptiques

Rappelons qu'un **morphisme** de courbes est une application partout définie et dont les composantes sont des fonctions rationnelles. Comme pour les fonctions sur les courbes un morphisme de courbes lisses est alors **constant ou surjectif**. Quand les courbes ne sont pas lisses la notion de morphisme est remplacée par la notion d'application rationnelle. Ce sont des applications qui ne sont pas partout définis sur la courbe. On note les morphismes par $\phi : C_1 \to C_2$ et les applications rationnelles par $\phi : C_1 \cdots \to C_2$. On sait par ([S] II.2.1) que toute application rationnelle $C \to V$ d'une courbe **lisse** $C$ dans une variété projective $V$ est un morphisme.

**Définition 10.1 (morphisme de courbes elliptiques)** *Soient $E$ et $E'$ deux courbes elliptiques définies sur un même corps $\mathbb{K}$. L'application de $E$ dans $E'$ qui à tout point de $E$ associe le point à l'infini de $E'$ est appelée le morphisme nul. Un morphisme non nul de $E$ vers $E'$ est un morphisme de courbes*

$$\alpha : E \longrightarrow E' \,;\, P \to \alpha(P) = (r(P), s(P))$$

*où $r$ et $s$ sont des fonctions rationnelles de $\overline{\mathbb{K}}(E)$. Si $r$ et $s$ sont définies sur $\mathbb{K}$ i.e. $r, s \in \mathbb{K}(E)$ on dit que le morphisme $\alpha$ est défini sur $\mathbb{K}$.*

**Proposition–Définition 10.2 (valeur en un point)** *Soit $\alpha = (r, s) : E \longrightarrow E'$ un morphisme de courbes elliptiques définies sur un même corps $\mathbb{K}$. Un point $P \in E$ est pôle pour $r$ si et seulement si il est pôle pour $s$ et on a :*

$$3\,\mathrm{ord}_P(r) = 2\,\mathrm{ord}_P(s).$$

*Si $P$ est un pôle pour $r$ et $s$, on dira que $P$ est un pôle pour le morphisme $\alpha$ et que $\alpha(P) = \mathcal{O}'$ le point à l'infini de $E'$. Si $P$ est un point régulier pour $r$ et pour $s$ alors on dira que $P$ est un point régulier pour le morphisme $\alpha$ et que la valeur de $\alpha$ en $P$ est $\alpha(P) = (r(P), s(P))$*

**Exemple 10.3** *Soit $E$ une courbe elliptique.*
**1)** *Soit $Q$ un point fixé de $E$. La translation de point $Q$ définie par : $\tau_Q : E \longrightarrow E\,;\, P \to P + Q$ est un morphisme de $E$ vers $E$. En effet, les composantes de $\tau_Q(P)$ sont données par les formules d'addition dans $E$, qui sont des fonctions rationnelles en $x_P$ et $y_P$.*
**2)** *Pour tout entier $n \in \mathbb{Z}$, la multiplication par $n$, notée $[n]$ et définie par $[n] : E \longrightarrow E\,;\, P \to nP$ est un morphisme de $E$ dans $E$ car les formules d'addition et de duplication montrent que les composantes de $[n]$ sont des fonctions rationnelles. La multiplication par $1$ est $[1] = id_E : P \to P$.*

**Remarque 10.4** *Si on suppose que des équations affines des courbes $E$ et de $E'$ sont données par $E : y^2 = x^3 + ax + b$ et $E' : y^2 = x^3 + a'x + b'$. Comme l'image par $\alpha$ de tout point $P$ de $E$ appartient à la courbe $E'$, les fonctions $r$ et $s$ doivent satisfaire la relation suivante : $\forall P \in E, \quad s(P)^2 = r(P)^3 + a'r(P) + b'$. Cette équation correspond à l'égalité suivante, satisfaite dans le corps $\overline{\mathbb{K}}(E)$ :*

$$s^2 = r^3 + a'r + b'$$

*Ainsi le couple $(r, s)$ des composantes du morphisme $\alpha$, est un point de la courbe elliptique d'équation $y^2 = x^3 + a'x + b'$ définie sur le corps $\overline{\mathbb{K}}(E)$ des fonctions rationnelles sur $E$. Cela s'exprime en écrivant que $\alpha$ est un point fini du groupe $E_1(\overline{\mathbb{K}}(E))$. En particulier, l'ensemble des morphismes de $E$ vers $E'$ est muni d'une loi d'addition qui lui confère une structure de groupe commutatif.*

# 11 Ramification des morphismes

Soit $(C)$ une courbe projective lisse sur $\mathbb{K}$. On rappelle que toute fonction rationnelle non constante $f \in \overline{\mathbb{K}}(C)$ définit un morphisme surjectif noté encore $f : C \longrightarrow \mathbb{P}^1$.

**Définition 11.1** *Soit $\phi : C_1 \to C_2$ un morphisme non constant de courbes lisses. On définit un $\overline{\mathbb{K}}$-homomorphisme de corps*

$$\phi^* : \overline{\mathbb{K}}(C_2) \to \overline{\mathbb{K}}(C_1), \;\; f \longmapsto \phi^*(f) = f \circ \phi$$

*Ici les éléments de $\overline{\mathbb{K}}(C_1)$ et $\overline{\mathbb{K}}(C_2)$ sont vus comme morphismes de $C_1$ dans $\mathbb{P}^1$ et de $C_2$ dans $\mathbb{P}^1$. Si $C_1$, $C_2$ et $\phi$ sont définis sur $\mathbb{K}$, la restriction de $\phi^*$ à $\mathbb{K}(C_2)$ est un $\mathbb{K}$-homomorphisme de corps (noté encore $\phi^*$) : $\phi^* : \mathbb{K}(C_2) \to \mathbb{K}(C_1), \;\; f \longmapsto \phi^*(f) = f \circ \phi$*

**Proposition–Définition 11.2** *Soit $\phi : C_1 \to C_2$ un morphisme non constant de courbes lisses sur $\mathbb{K}$. Soient $P$ un point de $C_1$, $Q = \phi(P)$ son image, $t \in \overline{\mathbb{K}}(C_2)$ une uniformisante en $Q$.*
*1) L'ordre en $P$ de $\phi^*(t)$ ne dépend pas du choix de $t$ et est appelé* **indice de ramification** *de $\phi$ en $P$. On le note $e_\phi(P)$ et on a $e_\phi(P) \geqslant 1$. On a donc $e_\phi(P) = \mathrm{ord}_P(\phi^*(t)) = \mathrm{ord}_P(t \circ \phi)$.*
*On dit que $\phi$ est* **non ramifié** *(resp.* **ramifié***) en $P$ si $e_\phi(P) = 1$ (resp. $e_\phi(P) > 1$). On dit que $\phi$ est non ramifié s'il est non ramifié en tout point $P$ de $C_1$.*
*2) Soit $f \in \overline{\mathbb{K}}(C_2) \smallsetminus \{0\}$. On a $\mathrm{ord}_P \phi^*(f) = e_\phi(P)\,\mathrm{ord}_Q(f)$. En particulier, si $f$ et $g$ ont même ordre en $Q$, $\phi^*(f)$ et $\phi^*(g)$ ont même ordre en $P$.*

**Exemple 11.3** *Soit $E$ une courbe elliptique définie sur un corps fini $\mathbb{F}$ de cardinal $q$ alors le morphisme $\varphi_q = (x^q, y^q)$ est ramifié en $\mathcal{O}$. En effet, on a $\varphi(\mathcal{O}) = \mathcal{O}$ car $x^q$ et $y^q$ sont des fonctions polynômes sur $E$. Ensuite, on sait que $(x/y)$ est une uniformisante en $\mathcal{O}$. Donc*

$$e_{\varphi_q}(\mathcal{O}) = \mathrm{ord}_{\mathcal{O}}\left(\frac{x}{y} \circ \varphi_q\right) = \mathrm{ord}_{\mathcal{O}}\left(\frac{x^q}{y^q}\right) = \mathrm{ord}_{\mathcal{O}}\left(\frac{x}{y}\right)^q = q$$

**Proposition 11.4 (composition de morphismes)** *Soit $\alpha : C_1 \longrightarrow C_2$ et $\beta : C_2 \longrightarrow C_3$ des morphismes non constants de courbes lisses définies sur $\mathbb{K}$. Pour tout $P \in C_1$ on a :*

$$e_{\beta\circ\alpha}(P) = e_\alpha(P) \times e_\beta(\alpha(P))$$

**Proposition 11.5 (non ramification des translations)** *Soit $Q$ un point d'une courbe elliptique $E$. Alors la translation $\tau_Q : E \longrightarrow E\,;\, P \to P + Q$ n'est pas ramifiée.*

**Corollaire 11.6** *Soit $f \in \overline{\mathbb{K}}(E) \smallsetminus \{0\}$ une fonction sur une courbe elliptique $E$. Soient $P, Q \in E$ et soit $\tau_Q$ la translation de point $Q$. On a $\mathrm{ord}_P(f \circ \tau_Q) = \mathrm{ord}_{P+Q}(f)$. En particulier, pour $P = \mathcal{O}$, on a $\mathrm{ord}_Q(f) = \mathrm{ord}_{\mathcal{O}}(f \circ \tau_Q)$.*

# 12 Isogénies de courbes elliptiques

**Définition 12.1** *Soient $E_1$ et $E_2$ deux courbes elliptiques définies sur un même corps $\mathbb{K}$. Une* **isogénie** *entre $E_1$ et $E_2$ est un morphisme de courbes elliptiques $\phi : E_1 \to E_2$ tel que $\phi(\mathcal{O}_1) = \mathcal{O}_2$.*

**Exemple 12.2**

1) Pour tout $n \in \mathbb{Z}$ non nul, $[n] : E \to E\,;\, P \mapsto nP$ est une isogénie.
2) Si $Q \neq \mathcal{O}$, la translation par $Q \in E$ n'est pas une isogénie de $E$ ( car $\tau_Q(\mathcal{O}) \neq \mathcal{O}$).
3) Soient $\phi : E_1 \to E_2$ un morphisme de courbes elliptiques et $Q = \phi(\mathcal{O})$. Alors $\tau_{-Q} \circ \phi$ est une isogénie car $\tau_{-Q} \circ \phi(\mathcal{O}) = \tau_{-Q}(Q) = \mathcal{O}$.
4) **Morphisme de Frobenius :** On suppose maintenant $\mathbb{K} = \mathbb{F}_q$ un corps fini de caractéristique $p$ premier et de cardinal $q = p^r$. Pour tout polynôme $f$ à coefficients dans $\mathbb{K}$ on note $f^{(q)}$ le polynôme obtenu en élevant les coefficients de $f$ à la puissance $q$. On a alors $f^{(q)}(X^q) = (f(X))^q \quad \text{et} \quad (f+g)^{(q)} = f^{(q)} + g^{(q)}$. Soit $E$ une courbe elliptique d'équation de Weierstrass sur $\overline{\mathbb{K}}$

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

Le polynôme $f^{(q)}$ définit une courbe de Weierstrass notée $E^{(q)}$, et donc d'équation

$$E^{(q)} : f^{(q)}(x,y) = y^2 + a_1^qxy + a_3^qy - x^3 - a_2^qx^2 - a_4^qx - a_6^q = 0$$

Puisque l'application $\mathbb{K} \to \mathbb{K}, a \mapsto a^q$ est un homomorphisme car $q = p^r$, on a $\Delta(E^{(q)}) = \Delta(E)^q \quad \text{et} \quad j(E^{(q)}) = j(E)^q$. Donc $\Delta(E^{(q)}) \neq 0$ et $E^{(q)}$ est une courbe elliptique. Par ailleurs, le morphisme $\phi : \mathbb{P}^2 \to \mathbb{P}^2$ qui à $[\alpha_0 : \alpha_1 : \alpha_2]$ associe $[\alpha_0^q : \alpha_1^q : \alpha_2^q]$ induit un morphisme de courbes elliptiques appelé le $q$-ième morphisme de Frobenius

$$\varphi_q : E \to E^{(q)}, \quad (x,y) \mapsto (x^q, y^q)$$

On a bien $\varphi_q(E) = E^{(q)}$ car pour tout point $P = (x,y) \in E$ on a $f^{(q)}(\varphi_q(P)) = f^{(q)}(x^q, y^q) = (f(x,y))^q = (f(P))^q = 0$. Si on choisit comme origine sur $E^{(q)}$ le point $\varphi_q(O)$, le morphisme de Frobenius $\varphi_q : E \to E^{(q)}$ est une isogénie. En particulier, Si $E$ est définie sur le corps fini $\mathbb{F}_q$, alors $E^{(q)} = E$ car on a pour tout $a \in \mathbb{F}_q, a^q = a$ et le morphisme $\varphi_q$ est un endomorphisme de $E$ appelé le le $q$-ième endomorphisme de Frobenius et l'ensemble des points de $E$ invariants par $\varphi_q$ est exactement le groupe fini $E(\mathbb{F}_q) = \{P \in E / \varphi_q(P) = P\}$.

On veut maintenant montrer que toute isogénie est un homomorphisme de groupes. Soit $E$ une courbe elliptique sur un corps $\mathbb{K}$. L'ensemble $\mathrm{Pr}(E)$ des diviseurs principaux de $E$ est un sous-groupe du groupe $\mathrm{Div}^0(E)$ des diviseurs de $E$ de degré nul qui est lui même un sous-groupe du groupe $\mathrm{Div}(E)$. On a donc $\mathrm{Pr}(E) \subset \mathrm{Div}^0(E) \subset \mathrm{Div}(E)$. On note $\mathrm{Pic}(E)$ (resp. $\mathrm{Pic}^0(E)$) Les groupes quotient $\mathrm{Div}(E)/\mathrm{Pr}(E)$ (resp. $\mathrm{Div}^0(E)/\mathrm{Pr}(E)$) et on les appelle groupes de Picard de $E$.

**Proposition 12.3** *Soit $E$ une courbe elliptique sur un corps $\mathbb{K}$. L'application $\tilde{\kappa} : E \to \mathrm{Div}^0(E)$ qui à tout $P \in E$ associe le diviseur $(P) - (O)$ induit un isomorphisme de groupes noté $\kappa : E \to \mathrm{Pic}^0(E); P \mapsto [(P) - (\mathcal{O})]$. Attention, $\tilde{\kappa}$ lui même n'est pas un homomorphisme de groupes.*

**Théorème 12.4** *Soit $\phi : E_1 \to E_2$ une isogénie de courbes elliptiques définies sur un même corps $\mathbb{K}$. Alors pour tous points $P$ et $Q$ de $E_1$ on a $\phi(P+Q) = \phi(P) + \phi(Q)$. Autrement dit, $\phi$ est un homomorphisme de groupes.*

**Exemple 12.5**

Supposons que $\mathbb{K}$ est de caractéristique $\neq 2$. Soient $E$ la courbe elliptique d'équation $y^2 = x^3 - x$ et $i \in \overline{\mathbb{K}}$ une racine carrée de $-1$. On définit un endomorphisme : $[i] : (x, y) \mapsto (-x, iy)$ C'est un élément de $\mathrm{End}(E)$. Il appartient à $\mathrm{End}_{\mathbb{K}}(E)$ si et seulement si $\mathbb{K}$ contient $i$.
On vérifie que pour tout point $P = (x, y)$ de $E$, on a $-P = (x, -y)$, donc $[i] \circ [i] = [-1]$ et on a un homomorphisme d'anneaux :

$$\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2 + 1) \to \mathrm{End}(E)\,;\, m + ni \mapsto [m] + [n] \circ [i].$$

Si la caractéristique de $\mathbb{K}$ est égale à 0, on montre que cet homomorphisme est un isomorphisme. On a en particulier $\mathrm{Aut}(E) \simeq Z[i]^* = \{\pm 1, \pm i\}$ un groupe cyclique d'ordre 4.

**Remarque 12.6**

De manière générale, si $E$ est une courbe elliptique définie sur un corps $\mathbb{K}$ de caractéristique $p$ alors $\mathrm{Aut}(E)$ est un groupe fini d'ordre divisant 24 et en plus précisément on a :

$$| \mathrm{Aut}(E) | = \begin{cases} 2 & \text{si} \quad j(E) \neq 0, 1728 \\ 4 & \text{si} \quad j(E) = 1728; p \neq 2, 3 \\ 6 & \text{si} \quad j = 0; p \neq 2, 3 \\ 12 & \text{si} \quad j = 0 = 1728; p = 3 \\ 24 & \text{si} \quad j = 0 = 1728; p = 2 \end{cases}$$

**Lemme 12.7 (forme réduite des isogénies)** *En caractéristique $\neq 2$, une isogénie se réduit sous la forme $\varphi(x,y) = (r(x), ys(x))$ où $r$ et $s$ sont des fonctions de $\overline{\mathbb{K}}(x) \subset \overline{\mathbb{K}}(E)$.*

**Remarque 12.8** *En caractéristique 2 : On peut encore écrire $\varphi = (r(x,y), s(x,y))$ avec $r(x,y) = r_1(x) + yr_2(x)$ et $s(x,y) = s_1(x) + ys_2(x)$ sous formes réduites.*
*Cas 1 : si pour $P = (x,y) \in E$ on a $-P = (x, x+y)$ ou $-P = (x, y+a_3)$ on a $\varphi(-P) = \varphi(x, y+x) = (r_1 + (x+y)r_2, s_1 + (x+y)s_2)$ et $-\varphi(P) = (r_1 + yr_2, r_1 + yr_2 + s_1(x) + ys_2(x))$. Donc la condition $\varphi(-P) = -\varphi(P)$ se traduit par $r_2 = 0$ et $xs_2 = r_1$ i.e. $s_2 = r_1/x$. Donc $\varphi = (r_1, s_1 + yr_1/x)$*
*Cas 2 : si pour $P = (x,y) \in E$ on a $-P = (x, y+a_3)$ on a $\varphi(-P) = \varphi(x, y+a_3) = (r_1 + (y + a_3)r_2, s_1 + (y+a_3)s_2)$ et $-\varphi(P) = (r_1 + yr_2, s_1 + ys_2 + a_3)$. Donc la condition $\varphi(-P) = -\varphi(P)$ se traduit par $r_2 = 0$ et $s_2 = 1$. Donc $\varphi = (r_1, s_1 + y)$*

**Exemple 12.9** *1) Soit $E$ une courbe elliptique définie sur un corps fini à $q$ éléments de caractéristique $p \neq 2, 3$, par l'équation affine $y^2 = x^3 + ax + b$. On a donc $y^q = y \times y^{(q-1)} = y(x^3 + ax + b)^{(q-1)/2}$. La forme réduite de l'isogénie de Frobenius $\varphi_q = (x^q, y^q)$ de $E$ est donc*

$$\varphi_q(x,y) = \Big(x^q,\, y(x^3 + ax + b)^{(q-1)/2}\Big)$$

*2) Soit $E$ une courbe elliptique définie sur un corps $\mathbb{K}$ de caractéristique $p \neq 2, 3$, par l'équation affine $y^2 = F(x) = x^3 + ax + b$. Les formules de duplication montrent que les composantes de l'isogénie de duplication $[2] : E \longrightarrow E\,;\, P = (x,y) \to 2P = (r_2(x), ys_2(x))$ sont*

$$\begin{aligned} r_2(x) &= \frac{F'(x)^2}{4F(x)} - 2x \\ s_2(x) &= -\frac{F'(x)}{2F(x)}(r_2(x) - x) - 1 = -\frac{F'(x)}{2F(x)}\Big(\frac{F'(x)^2}{4F(x)} - 3x\Big) - 1 \end{aligned} \tag{1}$$

*et les formules d'addition montrent que pour tout entier $n \geqslant 2$, les composantes de l'isogénie $[n] : E \longrightarrow E\,;\, P = (x,y) \to nP = (r_n(x), ys_n(x))$ vérifient les relations de récurrence suivantes : soit $\lambda_n = \dfrac{ys_n - y}{r_n - x}$, $\quad \lambda_n^2 = F(x)\Big(\dfrac{s_n - 1}{r_n - x}\Big)^2$*

$$\begin{aligned} r_{n+1} &= \lambda_n^2 - r_n - x \\ s_{n+1} &= -\lambda_n(r_{n+1} - x) - y = y(\Big(\frac{s_n - 1}{r_n - x}(r_{n+1} - x) - 1\Big) \end{aligned}$$

*donc*

$$\begin{aligned} r_{n+1}(x) &= F(x)\Big(\frac{s_n(x)-1}{r_n(x)-x}\Big)^2 - r_n(x) - x \\ s_{n+1}(x) &= -\frac{s_n(x)-1}{r_n(x)-x}(r_{n+1}(x)-x) - 1 \end{aligned} \tag{2}$$

On va montrer dans la suite que l'indice de ramification des morphismes de courbes elliptiques est constant *i.e.* ne dépendd pas du point $P$ de la courbe. On le montre d'abord pour les isogénies, puis en utilisant que tout morphisme est la composée d'une isogénie et d'une translation, on déduit le résultat pour tout morphisme.

**Proposition 12.10** *L'indice de ramification $e_\varphi(P)$ d'une isogénie $\varphi$ de courbes elliptiques au point $P$ ne dépend pas de $P$.*

**Proposition 12.11** *L'indice de ramification $e_\alpha(P)$ d'un morphisme $\alpha$ de courbes elliptiques en un point $P$, ne dépend pas du point $P$. On peut donc parler d'indice de ramification de $\alpha$ sans préciser le point. On note plus simplement $e_\alpha = e_\alpha(P)$.*

**Proposition 12.12** *Pour tout morphisme non constant de courbes elliptiques $\alpha : E_1 \longrightarrow E_2$ et pour tout point $Q \in E_2$, la valeur de $\operatorname{Card}\alpha^{-1}(\{Q\})$ est constante et indépendante du point $Q$.*

## 13 Degré d'une isogénie de courbes elliptiques

Soit $E_1, E_2$ deux courbes elliptiques définies sur un corps $\mathbb{K}$ et soit $\phi : E_1 \longrightarrow E_2$ une isogénie définie sur $\mathbb{K}$ . Comme tout morphisme entre courbes algébriques lisses, l'isogénie $\phi$ est soit constante donc d'image $\phi(E_1) = \{\mathcal{O}\}$, et on la notera $[0]$, soit surjective donc d'image $\phi(E_1) = E_2$ et dans ce cas on a un homomorphisme injectif naturel des corps de fonctions noté

$$\phi^* : \mathbb{K}(E_2) \to \mathbb{K}(E_1)\,;\, f \mapsto \phi^*(f) = f \circ \phi$$

Le degré de $\phi$ est alors par définition égal au degré de l'extension $\mathbb{K}(E_1)/\phi^*(\mathbb{K}(E_2))$ :

$$\deg(\phi) = [\mathbb{K}(E_1) : \phi^*(\mathbb{K}(E_2))]$$

**Définition 13.1** *Soit $\phi : C_1 \to C_2$ un morphisme non constant de courbes algébriques lisses. On définit des homomorphismes de groupes :*

$$\phi^* : \operatorname{Div}(C_2) \to \operatorname{Div}(C_1)\,;\, (Q) \mapsto \phi^*((Q)) = \sum_{P \in \phi^{-1}(\{Q\})} e_\phi(P)(P)$$

$$\phi_* : \mathrm{Div}(C_1) \to \mathrm{Div}(C_2)\,;\,(P) \mapsto \phi_*((P)) = (\phi(P))$$

*puis par linéarité.*

**Proposition 13.2** *Soient $C_1, C_2$ deux courbes algébriques lisses définies sur un corps $\mathbb{K}$ et soit $\phi : C_1 \to C_2$ et $\psi : C_2 \to C_3$ des morphismes non constants définies sur $\mathbb{K}$. On a*

(1) *Pour tout $D \in \mathrm{Div}(C_2)$, $\deg(\phi^*(D)) = (\deg\phi)(\deg D)$.*

(2) *Pour tout $f \in \mathbb{K}(C_2)$ non nul, $\phi^*(\mathrm{div}\, f) = \mathrm{div}(\phi^* f)$.*

(3) *Pour tout $D \in \mathrm{Div}(C_1)$, $\deg(\phi_*(D)) = \deg D$.*

(4) *Pour tout $f \in \overline{\mathbb{K}}(C_1)$ non nul, $\phi_*(\mathrm{div}\, f) = \mathrm{div}(\phi_* f)$.*

(5) *$\phi_* \circ \phi^*$ est la multiplication par $\deg\phi$ sur $\mathrm{Div}(C_2)$.*

(6) *$(\psi \circ \phi)^* = \phi^* \circ \psi^*$ et $(\psi \circ \phi)_* = \psi_* \circ \phi_*$.*

Preuve : [S]II. 3.6. ∎

**Remarque 13.3**

Dans les propriétés (2) et (4) la définitions de $\phi^*(f)$ est donnée par $\phi^*(f) = f \circ \phi$ où $\phi^* : \mathbb{K}(C_2) \longrightarrow \mathbb{K}(C_1)$ et $f$ est vu comme un moprhisme de $C_1 \longrightarrow \mathbb{P}^1$ et $\phi_*(f)$ est défini comme suit : $\phi^*$ est injective car $\phi$ est surjective (car non constante) donc définit un isomorphisme $\phi^* : \mathbb{K}(C_2) \longrightarrow \phi^*(\mathbb{K}(C_2)) \subset \mathbb{K}(C_1)$. Ainsi $\mathbb{K}(C_1)$ est une extension finie de $\phi^*(\mathbb{K}(C_2))$. Pour tout $f \in \mathbb{K}(C_1), \phi_*(f) \in \mathbb{K}(C_2)$ est défini par $\phi_*(f) = (\phi^*)^{-1} \circ N_{\mathbb{K}(C_1)/\phi^*(\mathbb{K}(C_2))}(f)$. Rappelons que si $L/k$ est extension finie de corps et $G$ l'ensemble des $k$-automorphismes de $L$, pour tout $\alpha \in L, \prod_{\sigma\in G}\sigma(\alpha) \in k$ car le polynôme minimal de $\alpha$ sur $k$ est $P = \prod_{\sigma\in G}(X - \sigma(\alpha))$. On a $P \in k[X]$ car il est invariant par tout élément $\tau \in G$ car $P^\tau = \prod_{\sigma\in G}(X - \tau\sigma(\alpha)) = P$ car l'application $\sigma \longrightarrow \tau\circ\sigma$ est une bijection. Le coefficient constant de ce polynôme $P$ est bien $N_{L/k}(\alpha)$.

Si $\phi$ est une isogénie de courbes elliptiques, en appliquant le résultat (1) de cette proposition avec $D = (\mathcal{O})$ et en utilisant le fait que $e_\phi(P) = e_\phi$ est constant on aura $\phi^*((\mathcal{O})) = e_\phi \sum_{P\in\ker\phi}(P)$ et donc $\deg(\phi) \times 1 = \deg(\phi^*((\mathcal{O}))) = e_\phi \times Card\ker(\phi)$. D'où le corollaire :

**Corollaire 13.4** *Soit $\phi : E \longrightarrow E$ une isogénie non nulle d'une courbe elliptique $E$. On a :*

$$\deg(\phi) = e_\phi \times \operatorname{Card}\ker(\phi)$$

**Exemple 13.5** 1) $\ker[2]$ *contient* 4 *points : le point $\mathcal{O}$ et les 3 points spéciaux, et $e_{[2]} = 1$ car $e_{[2]} = e_{[2]}(\mathcal{O}) = \operatorname{ord}_{\mathcal{O}} \frac{x}{y} \circ [2] = \operatorname{ord}_{\mathcal{O}} \dfrac{r_2(x)}{y s_2(x)} = 1$. C'est un calcul simple en utilisant les expressions de $r_2$ et de $s_2$ données en (1). En définitive, on a* $\deg([2]) = 4$.

2*)Le noyau de l'isogénie de Frobenius $\varphi_q$ est réduit à $\{\mathcal{O}\}$ et $e_{\varphi_q} = q$ donc* $\deg(\varphi_q) = q$.

**Corollaire 13.6** *Soient $\varphi$ et $\psi$ deux isogénies d'une courbe elliptique $E$, on a :*

$$\deg(\varphi \circ \psi) = \deg(\varphi) \times \deg(\psi)$$

**Corollaire 13.7** *Soit $\phi : C_1 \to C_2$ un morphisme non constant de courbes algébriques lisses. Alors les homomorphismes $\phi^* : \operatorname{Div}(C_2) \longrightarrow \operatorname{Div}(C_1)$ et $\phi_* : \operatorname{Div}(C_1) \longrightarrow \operatorname{Div}(C_2)$ définis en* (13.1) *induisent des homomorphismes de groupes, notés de la même manière :*

$$\phi^* : \operatorname{Pic}(C_2) \to \operatorname{Pic}(C_1) \quad et \quad \phi_* : \operatorname{Pic}(C_1) \to \operatorname{Pic}(C_2)$$

*qui se restreignent en des homomorphismes de groupes :*

$$\phi^* : \operatorname{Pic}^0(C_2) \to \operatorname{Pic}^0(C_1) \quad et \quad \phi_* : \operatorname{Pic}^0(C_1) \to \operatorname{Pic}^0(C_2)$$

## 14 Isogénie duale d'une isogénie de courbes elliptiques

Soit $\phi : E_1 \to E_2$ une isogénie non nulle de courbes elliptiques. Elle induit un homomorphisme

$$\phi^* : \operatorname{Pic}^0(E_2) \to \operatorname{Pic}^0(E_1)$$

défini en (13.7). D'autre part, pour $i = 1, 2$ on a des applications définis en (12.3) par

$$\tilde{\kappa_i} : E_i \to \operatorname{Div}^0(E_i),\ P \mapsto (P) - (O)$$

et des isomorphismes de groupes

$$\kappa_i : E_i \to \operatorname{Pic}^0(E_i),\ P \mapsto [(P) - (O)]$$

On définit aussi les homomrphismes $\sigma_i$ par

$$\sigma_i : \operatorname{Div}^0(E_i) \to E_i,\ \sum_i n_i(P_i) \mapsto \sum_i [n_i]P_i = \sum_i n_i P$$

Remarquons que touts ces différentes applications vérifient les propriétés suivantes :

- $\sigma_i$ et $\tilde{\kappa_i}$ vérifient $\sigma_i \circ \tilde{\kappa_i} = Id_{E_i}$ mais ne sont pas des bijections
- $\tilde{\kappa_i}$ est injective et n'est pas un morphisme de groupes,
- $\sigma_i$ surjective et $\kappa_i$ est un isomorphisme de groupes.

On en déduit par composition un diagramme commutatif :

$$\begin{array}{ccccc} E_2 & \xrightarrow{\tilde{\kappa_2}} & \mathrm{Div}^0 E_2 & \longrightarrow & \mathrm{Pic}^0 E_2 \\ & & \downarrow{\scriptstyle \phi^*} & & \downarrow{\scriptstyle \phi^*} \\ & & \mathrm{Div}^0 E_1 & \longrightarrow & \mathrm{Pic}^0 E_1 \\ & & & \searrow^{\sigma_1} & \downarrow{\scriptstyle \kappa_1^{-1}} \\ & & & & E_1 \end{array}$$

donc un homomorphisme de **groupes** (abstraits) de $E_2$ dans $E_1$. Nous allons montrer qu'en fait il est induit par une isogénie. Auparavant, un calcul.

**Proposition 14.1** *Soit $\phi : E_1 \longrightarrow E_2$ une isogénie non nulle de courbes elliptiques. Avec les notations ci-dessus, on a :*

$$\sigma_1 \circ \phi^* \circ \tilde{\kappa_2} \circ \phi = \kappa_1^{-1} \circ \phi^* \circ \kappa_2 \circ \phi = [\deg \phi].$$

**Corollaire 14.2** *Avec les notations ci-dessus, on a : $\phi^*((Q) - (O)) \sim (\deg \phi)((P) - (O))$.*

**Théorème–Définition 14.3** *Soit $\phi : E_1 \to E_2$ une isogénie non constante de degré $m$. Il existe une unique isogénie $\hat{\phi} : E_2 \to E_1$ vérifiant : $\hat{\phi} \circ \phi = [m]$. En tant qu'homorphisme de groupes on a : $\hat{\phi} = \sigma_1 \circ \phi^* \circ \tilde{\kappa_2} = \kappa_1^{-1} \circ \phi^* \circ \kappa_2$. L'isogénie $\hat{\phi}$ est* **l'isogénie duale** *de l'isogénie $\phi$.*

**Remarque 14.4** *Rappelons les diagrammes commutatifs, où $\tilde{\kappa_1}(P_1) = (P_1) - (\mathcal{O}_1); \tilde{\kappa_2}(P_2) = (P_2) - (\mathcal{O}_2)$ et $\phi_*(\sum n_i(P_i)) = \sum n_i(\phi(P_i))$ :*

$$\begin{array}{ccccc} E_1 & \xrightarrow{\tilde{\kappa_1}} & \mathrm{Div}^0 E_1 & \longrightarrow & \mathrm{Pic}^0 E_1 \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi_*} & & \downarrow{\scriptstyle \phi_*} \\ E_2 & \xrightarrow[\tilde{\kappa_2}]{} & \mathrm{Div}^0 E_2 & \longrightarrow & \mathrm{Pic}^0 E_2 \end{array}$$

*et on a de même les diagrammes commutatifs suivants avec l'isogénie duale :*

$$\begin{array}{ccccc} E_2 & \xrightarrow{\tilde{\kappa_2}} & \mathrm{Div}^0 E_2 & \longrightarrow & \mathrm{Pic}^0 E_2 \\ \downarrow{\scriptstyle \hat{\phi}} & & \downarrow{\scriptstyle \phi^*} & & \downarrow{\scriptstyle \phi^*} \\ E_1 & \xrightarrow[\tilde{\kappa_2}]{} & \mathrm{Div}^0 E_1 & \longrightarrow & \mathrm{Pic}^0 E_1 \end{array}$$

*Avec les notations ci-dessus, on a donc montré :*

$$\phi_* \circ \tilde{\kappa_1} = \tilde{\kappa_2} \circ \phi \quad et \quad \phi_* \circ \kappa_1 = \kappa_2 \circ \phi \quad et \quad \kappa_1 \circ \hat{\phi} = \phi^* \circ \kappa_2$$

*ce qu'on peut encore écrire :*

$$\phi_*((P) - (O)) = (\phi(P)) - (O) \quad et \quad (\hat{\phi}(Q)) - (O) \sim \phi^*((Q) - (O))$$

Les propriétés principales de l'isogénie duale sont énoncées dans le théorème suivant :

**Théorème 14.5** *Soit $\phi : E_1 \to E_2$ une isogénie de degré $m > 0$.*

1) *$\hat{\phi} \circ \phi = [m]$ sur $E_1$ et $\phi \circ \hat{\phi} = [m]$ sur $E_2$.*

2) *Soit $\lambda : E_2 \to E_3$ une autre isogénie. Alors $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$.*

3) *Soit $\psi : E_1 \to E_2$ une autre isogénie. Alors $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$.*

4) *Pour tout $n \in \mathbb{Z}$, $\hat{[n]} = [n]$ et $\deg[n] = n^2$.*

5) $\deg \hat{\phi} = \deg \phi$.

6) $\hat{\hat{\phi}} = \phi$.

Preuve : Voir [S]III.6.2. ∎

## 15 Séparabilité des isogénies de courbes elliptiques

Soit $\phi : E_1 \to E_2$ une isogénie définie sur un corps $\mathbb{K}$ entre courbes elliptiques définies sur $\mathbb{K}$ et $\phi^* : \mathbb{K}(E_2) \to \mathbb{K}(E_1), f \mapsto f \circ \phi$ l'homomorphisme des corps de fonctions, associés à $\phi$. On dit que $\phi$ est séparable si l'extension $\mathbb{K}(E_1)/\phi^*(\mathbb{K}(E_2))$ est séparable. On donnera et on utilisera dans la suite une autre définition plus pratique de la séparabilité.

**Définition 15.1 (isogénie séparable)** *On dit qu'une isogénie $\phi$ de courbes elliptiques définie par sa forme réduite $\phi(x, y) = (r(x), ys(x))$ est séparable si la dérivé $r'(x)$ n'est pas identiquement nulle. Dans le cas contraire on dit qu'elle est inséparable.*

**Exemple 15.2** 1) *En caractéristique nulle, toute isogénie non constante est séparable.*

2) *Une isogénie inséparable ne peut exister qu'en caractéristique non nulle.*

3) *L'isogénie $[2] : P \to 2P$ est séparable en caractéristique $p \neq 2$.*

4) *L'isogénie de Frobenius $\varphi_q$ est inséparable.*

**Proposition 15.3** *Une isogénie est séparable si et seulement si elle est non ramifiée.*

**Proposition 15.4** *Soit $\alpha$ une isogénie non nulle d'une courbe elliptique $E$ sur un corps de caractéristique $p \neq 2$. Soit $\varphi_p = (x^p, y^p)$ le p-ième Frobenius. On a*
1) *l'isogénie $\alpha$ est inséparable si et seulement si il existe une isogénie $\beta$ de $E$ telle que $\alpha = \beta \circ \varphi_p$*
2) *Si $\alpha$ est inséparable alors son indice de ramification est obligatoirement une puissance $p$.*

Preuve : Exercice ∎

## 16 Groupe des points de $n$-torsion d'une courbe elliptique

Dans toute cette section, $E$ est courbe elliptique définie sur un corps algébriquement clos $\mathbb{K}$. Pour tout entier $n \geqslant 1$, un point de $n$-torsion est par définition un point $P \in E$ tel que $[n](P) = \mathcal{O}$ et plus généralement, un point de torsion est point d'ordre fini.

**Définition 16.1 (groupe de $n$-torsion)** *Pour tout entier $n$, le groupe de $n$-torsion de la courbe elliptique $E$ est le noyau de l'isogénie de multiplication par $n$. Comme tout noyau d'isogénie, c'est un groupe fini. On le note $E[n] := \ker([n]) = \{P \in E / nP = \mathcal{O}\}$.*

On va étudier le groupe $E[n]$ et les polynômes de division sur $E$. Ce sont des polynômes de $\mathbb{K}[E]$ qui permettent de caractériser et de construire les points de $n$-torsion. La proposition qui suit donne quelques propriétés de l'isogénie $[n]$ et elle sera démontrée en TD.

**Proposition 16.2** *Soit $E$ une courbe elliptique définie sur un corps $\mathbb{K}$ de caractéristique $\neq 2$ et ayant pour équation affine $y^2 = x^3 + ax + b$ et soit $n$ un entier $\geqslant 1$. Notons*

$$[n] : (x, y) \to (r_n(x), y s_n(x))$$

*la forme réduite de l'isogénie $[n]$ sur $E$, où $r_n, s_n \in \mathbb{K}(x) \subset \mathbb{K}(E)$. Alors*
1) *Dans $\mathbb{K}(x)$ on a l'égalité $r_n' = n s_n$.*
2) *L'isongénie $[n]$ est séparable si et seulement $n$ est premier à la caractéristique du corps $\mathbb{K}$.*
3) *La fonction $r_n$ vérifie l'équation différentielle suivante*

$$r_n'' = \frac{n^2(3r_n^2 + a) - r_n'(3x^2 + a)}{2(x^3 + ax + b)} \tag{3}$$

4) *Si $n$ est premier à la caractéristique du corps alors on a*

$$\deg(r_n) = 2, \quad \deg(s_n) = 0, \quad \frac{r_n}{x}(\mathcal{O}) = \frac{1}{n^2}, \quad s_n(\mathcal{O}) = \frac{1}{n^3} \tag{4}$$

*Si $n$ est multiple de la caractéristique alors le point $\mathcal{O}$ est un pôle pour $r_n$ et $s_n$.*

5) *Si $P = (\alpha, 0) \in E$ est un point spécial et si $n$ est impair alors $s_n(\alpha) = n$.*

Pour donner la structure du groupe $E[n]$, on commence par donner une notation du diviseur d'un ensemble fini $F$ de points de $E$. C'est tout simplement le diviseur noté $(F)$ et défini par :

$$(F) = \sum_{P \in F} (P)$$

Ainsi on a par exemple $CardF = \deg(F)$. La structure du groupe $E[n]$ et la construction des polynômes de division reposent sur le résultat suivant :

**Lemme 16.3** *Soit $n$ et $m$ deux entiers tels que $n, m, m-n$ et $m+n$ ne sont pas multiples de la caractéristique du corps $\mathbb{K}$. On a dans* $\mathrm{Div}(E)$ *l'égalité :*

$$\mathrm{div}(r_n - r_m) = (E[n+m]) + (E[n-m]) - 2(E[n]) - 2(E[m]) \tag{5}$$

**Théorème 16.4 (cardinal du groupe de $n$-torsion)** *Soit $E$ une courbe elliptique définie sur un corps $\mathbb{K}$. Pour tout entier $n$ non multiple de la caractéristique de $\mathbb{K}$, on a*

$$\mathrm{Card}(E[n]) = \deg([n]) = n^2$$

On rappelle maintenant la structure des groupes abéliens finis.

**Théorème 16.5 (structure des groupes abéliens finis)** *Tout groupe commutatif fini est isomorphe à un produit direct fini $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ où pour tout $i = 1, \ldots, k-1$, chaque entier $n_i$ divise l'entier $n_{i+1}$.*

**Proposition 16.6 (structure du groupe des points de $n$-torsion)** *Si la caractéristique du corps ne divise pas $n$, alors $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

**Remarque 16.7** *Il existe donc une base de $E[n]$, en tant que $\mathbb{Z}/n\mathbb{Z}$-module libre de rang 2, formée de deux points $S$ et $T$ de $E[n]$, chacun engendrant un groupe isomorphe à $\mathbb{Z}/n\mathbb{Z}$, donc d'ordre $n$, et tel que pour tout point $P \in E[n]$, il existe $a, b \in \mathbb{Z}/n\mathbb{Z}$ tels que $P = aS + bT$. Si $n = p$ est premier alors $E[p]$ a une structure d'espace vectoriel de dimension 2 sur $\mathbb{F}_p$.*

La proposition (16.6) permet de déduire la structure de groupes des points d'une courbe elliptique sur un corps fini.

**Théorème 16.8 (Cassel 1966)** *Soit $E$ une courbe elliptique sur un corps fini $\mathbb{K}$. Alors ou bien $E(\mathbb{K})$ est un groupe cyclique ou bien $E(\mathbb{K})$ est isomorphe à un produit direct $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ avec $n_1 \mid n_2$.*

# 17 Polynômes de division sur une courbe elliptique

Les polynômes de division d'une courbe elliptique sont des fonctions polynômes sur la courbe dont les zéros finis sont précisément les points de torsion. Ils permettent de caractériser ces points et donnent un moyen de les construire. Soit $n$ un entier non divisible par la caractéristique du corps de base $\mathbb{K}$. Rappelons que les points finis de $n$-torsion sont les points dont les coordonnées sont les pôles des composantes $r_n(x)$ et $ys_n(x)$ de la forme réduite de l'isogénie $[n]$.

**Lemme 17.1** *Soit $E$ une courbe elliptique définie sur un corps $\mathbb{K}$ et soit $n$ un entier non nul premier à la caractéristique de $\mathbb{K}$. On a*

$$\sum_{P \in E[n]} P = \mathcal{O}$$

Montrer l'existence de polynômes de division est facile. Comme le groupe $E[n]$ est d'ordre $n^2$, le diviseur $(E[n]) - n^2(\mathcal{O})$ est de degré et de somme nuls donc est principal. Il est est le diviseur d'une fonction qui n'a pas de pôle fini et qui est donc un polynôme.

**Définition 17.2 (polynôme de division)** *Soit $E$ une courbe elliptique définie sur un corps $\mathbb{K}$ et soit $n$ un entier non nul premier à la caractéristique de $\mathbb{K}$. Le polynôme de division $\psi_n$ est la fonction polynôme de $\mathbb{K}[E]$ de coefficient dominant $n$ et de diviseur*

$$\operatorname{div}(\psi_n) = (E[n]) - n^2(\mathcal{O})$$

**Remarque** : il est commode de convenir que $\psi_0 = 0$, car $E[0] = E$ et finalement, tout point de $E$ annule $\psi_0$. Les propriétés suivantes sont immédiates :

1) $\psi_1 = 1$ car $E[1] = \{\mathcal{O}\}$

2) $\psi_2 = 2y$ car les trois points spéciaux sont alignés sur la droit d'équation $y = 0$ et $\operatorname{div}(\psi_2) = (P_\alpha) + (P_\beta) + (P_\gamma) - 3(\mathcal{O})$

3) $\psi_{-n} = -\psi_n$ en raison de la condition sur les coefficients dominants.

**• Caractérisation des points de torsion**

Rappelons que pour tout point $P = (x_P, y_P)$ de $E$, on a $\text{div}(x - x_P) = (P) + (-P) - 2(\mathcal{O})$. Considérons une partition de l'ensemble des points ordinaires de $E[n]$ comme réunion $F \cup (-F)$.
1) si $n$ est impair : les points finis de $E[n]$ sont tous des points ordinaires. On a $E[n] = F \cup (-F) \cup \{\mathcal{O}\}$. Donc

$$\psi_n(x, y) = n \prod_{P \in F} (x - x_P) = f_n(x)$$

il s'agit d'un produit sur les abscisses des points ordinaires de $E[n]$. La forme réduite de $\psi_n(x, y)$ est dans ce cas un polynôme en $x$ seulement.
2) Si $n$ est pair : dans ce cas $E[n] = F \cup (-F) \cup \{\mathcal{O}, P_\alpha, P_\beta, P_\gamma\}$ où $P_\alpha, P_\beta, P_\gamma$ sont les points spéciaux. Comme $\text{div}(y) = P_\alpha + P_\beta + P_\gamma - 3(\mathcal{O})$ alors l'expression de $\psi_n(x, y)$ est

$$\psi_n(x, y) = ny \prod_{P \in F} (x - x_P)$$

C'est dans ce cas un polynôme de la forme $yf_n(x)$ où $f_n(x)$ est un polynôme en $x$.
La proposition qui suit résume la situation

**Proposition 17.3 (caractérisation des points de $n$-torsion)** *Soit $E$ une courbe elliptique définie sur un corps $\mathbb{K}$ et soit $n$ un entier non nul premier à la caractéristique de $\mathbb{K}$. Posons*

$$\psi_n(x, y) = \begin{cases} f_n(x) & \text{si } n \text{ est impair} \\ yf_n(x) & \text{si } n \text{ est pair.} \end{cases}$$

*Un point ordinaire $P = (x_P, y_P)$ de la courbe sur une clôture algébrique de $\mathbb{K}$, est un point de $n$-torsion si et seulement si son abscisse $x_P$ est racine de $f_n(x)$. Si $n$ est pair les points spéciaux sont également des points de $n$-torsion.*

**Remarque 17.4** *si $m$ et $n$ sont de même parité et premiers à la caractéristique de $\mathbb{K}$ alors $\psi_n\psi_m$ est toujours un polynôme en $x$ seul. En effet, si $m$ et $n$ sont impairs alors $(\psi_m\psi_n)(x, y) = (f_m f_n)(x)$ et s'ils sont pairs alors $(\psi_m\psi_n)(x, y) = y^2(f_m f_n)(x) = (x^3 + ax + b)(f_m f_n)(x)$. Si $\mathbb{K}$ est de caractéristique 2 alors $m$ et $n$ sont forcément impairs car premiers à 2.*

**Proposition 17.5** *Soit $E$ une courbe elliptique définie sur un corps $\mathbb{K}$. Si $n$ est un entier non nul premier à la caractéristique de $\mathbb{K}$ on note $(r_n, ys_n)$ la forme réduite de l'isogénie $[n]$. Si $n$ et*

*$m$ sont des entiers tels que $n, m, n+m, n-m$ sont premiers à la caractéristique de $\mathbb{K}$, alors*

$$r_n - r_m = -\frac{\psi_{n+m}\psi_{n-m}}{\psi_n^2\psi_m^2} \tag{6}$$

**Remarque** : les entiers $n+m$ et $n-m$ sont de même parité. D'après la remarque ci-dessus le membre de droite de la relation (9) est bien un polynôme en $x$ seulement.

**Proposition 17.6 (Construction par récurrence des polynômes de division)** *On a*

1) *pour* $n \geqslant 2, \psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n+1}^3\psi_{n-1}$
2) *pour* $n \geqslant 3, \psi_{2n} = \dfrac{\psi_n}{2y}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$

Ces relations permettent de calculer les polynômes $\psi_n$ à partir de $\psi_5$ et $\psi_6$. Il faut donc connaitre les premières valeurs de $\psi_n$ jusqu'à $n = 4$.

**Proposition 17.7 (premières valeurs des polynômes de division)** *Soit $E$ une courbe elliptique définie sur un corps $\mathbb{K}$ de caractéristique $\neq 2$, d'équation affine $y^2 = x^3 + ax + b$. On a :*

$\psi_0 = 0, \psi_1 = 1, \psi_2 = 2y$

$\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$

$\psi_4 = 4y(x^6 + 5ax^4 + 20bx^2 - 5a^2x^2 - 4abx - 8b^2 - a^3)$

## 18 Couplage de Weil sur une courbe elliptique

Soit $E$ une courbe elliptique sur un corps $\mathbb{K}$. Rappelons qu'on a un isomorphisme de groupes $\kappa : E \longrightarrow \mathrm{Pic}^0(E) : P \longmapsto [(P) - (\mathcal{O})]$ et que pour tout entier non nul $m$, l'isogénie $[m] : E \longrightarrow E$ induit deux endomorphismes $[m]^*, [m]_* : \mathrm{Pic}^0(E) \longrightarrow \mathrm{Pic}^0(E)$ tous deux égaux à la multiplication par $m$ et aussi un endomorphisme injectif du corps de fonctions sur $E$, noté aussi $[m]^* : \overline{\mathbb{K}}(E) \longrightarrow \overline{\mathbb{K}}(E), f \longmapsto f \circ [m]$

**Proposition 18.1** *Soient $E$ une courbe elliptique définie sur $\mathbb{K}$, $m$ un entier premier à la caractéristique de $\mathbb{K}$ et $T \in E[m]$. Il existe deux fonctions non nulles $f$ et $g$ de $\overline{\mathbb{K}}(E)$ telles que :*

1) $\mathrm{div}(f) = m(T) - m(\mathcal{O})$,
2) $\mathrm{div}(g) = [m]^*((T) - (\mathcal{O}))$,
3) $[m]^*(f) := f \circ [m] = g^m$.
4) *Pour tout point $S$ de $E[m]$, la fonction $\tau_S^*(g)/g := (g \circ \tau_S)/g$ est constante sur $E$, et est une racine $m$-ième de l'unité de $\overline{\mathbb{K}}$.*

**Remarque 18.2** *La fonction $g$ est définie seulement par son diviseur, donc à multiplication près par une constante non nulle, mais cela ne change pas $\tau_S^*(g)/g$.*

**Définition 18.3 (couplage de Weil)** *Soient $E$ une courbe elliptique définie sur un corps $\mathbb{K}$, $m$ un entier* **premier à la caractéristique** *$p$* **de** *$\mathbb{K}$, $T$ et $S$ deux points de $E[m]$, $g \in \overline{\mathbb{K}}(E)$ une fonction sur $E$ définie par son diviseur par l'égalité $\operatorname{div} g = [m]^*((T)) - [m]^*((O))$. On pose $e_m(S,T) = \tau_S^*(g)/g$. On définit ainsi une application appelée couplage de Weil :*

$$e_m : E[m] \times E[m] \to \mu_{\mathbf{m}} \,;\, (S,T) \longmapsto e_m(S,T) = \tau_S^*(g)/g$$

*où $\mu_{\mathbf{m}}$ est le groupe des racines m-ièmes de l'unité de $\overline{\mathbb{K}}$.*

**Remarque 18.4** *Pour tout point $P$ de $E$ tel que $g$ soit définie et non nulle en $P$ et $P+S$, on a donc $e_m(S,T) = g(P+S)/g(P)$.*

**Proposition 18.5** *(Admise) Le couplage de Weil a les propriétés suivantes :*

1) *bilinéaire : $e_m(S_1+S_2,T) = e_m(S_1,T)e_m(S_2,T)$ ; $e_m(S,T_1+T_2) = e_m(S,T_1)e_m(S,T_2)$;*
2) *alterné : $e_m(T,T) = 1$ d'où $e_m(S,T) = e_m(T,S))^{-1}$ ;*
3) *non-dégénéré : si $e_m(S,T) = 1$ pour tout $S \in E[m]$, alors $T = \mathcal{O}$ ;*
4) *Galois-invariant : pour tout $\sigma \in Gal(\overline{\mathbb{K}}/\mathbb{K})$, $e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$;*
5) *compatible : si $S \in E[mm']$ et $T \in E[m]$, $e_{mm'}(S,T) = e_m([m']S,T)$.*

Le résultat suivant montre que si $\phi$ est une isogénie entre deux courbes elliptiques $E_1$ et $E_2$ et si $\hat{\phi}$ est l'isogénie duale, de $E_2$ dans $E_1$, $\phi$ et $\hat{\phi}$ sont adjointes par rapport au couplage de Weil.

**Proposition 18.6** *Soient $E_1$ et $E_2$ deux courbes elliptiques, $\phi : E_1 \to E_2$ une isogénie, $\hat{\phi}$ l'isogénie duale, $T \in E_2[m]$ et $S \in E_1[m]$. Alors :*

$$e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T)$$

**Proposition 18.7 (autre expression du couplage de Weil)** *(Admise) Soit $E$ une courbe elliptique sur un corps $\mathbb{K}$, soit $n$ un entier premier à la caractéristique de $\mathbb{K}$ et soient $T, S \in E[n]$ deux points* **distincts**. *Soient $f_T, f_S \in \overline{\mathbb{K}}(E)$ telles que $\operatorname{div}(f_T) = n(T) - n(\mathcal{O})$ $\operatorname{div}(f_S) = n(S) - n(\mathcal{O})$. Ces fonctions sont définies à un facteur multiplicatif près et ont le même degré. On dit qu'elles sont normalisées si $\dfrac{f_T}{f_S}(\mathcal{O}) = 1$. Dans ce cas on a*

$$e_n(S,T) = (-1)^n \frac{f_T(S)}{f_S(T)}$$

# 19 Théorèmes de Hasse et de Weil

On considère maintenant un corps fini $\mathbb{F}_q$ à $q$ éléments et de caractéristique $p > 0$ (donc $q$ une puissance de $p$). Soit $E$ une courbe elliptique définie sur $\mathbb{F}_q$ par l'équation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. On veut estimer le nombre de points du groupe $E(\mathbb{F}_q) = \{\mathcal{O}\} \cup \{(x, y) \in \mathbb{F}_q^2 \text{ solution de } E\}$. Une première estimation grossière consiste à dire pour chaque valeur de $x \in \mathbb{F}_q$, correspond au plus deux valeurs de $y \in \mathbb{F}_q$ car pour $x$ fixé l'équation en $y$ est de degré 2. Donc Card$E(F_q) \leqslant 2q + 1$. Par ailleurs, l'application $\mathbb{F}_q^* \to \mathbb{F}_q^*,\ x \mapsto x^2$ est un homomorphisme de groupes multiplicatifs de noyau $\{\pm 1\}$, donc d'image de cardinal $(q-1)/2$. Ainsi le discriminant de l'équation en $y$ a 50% de chances d'être un carré non nul dans $\mathbb{F}_q$ auquel l'équation en $y$ admet deux solutions. Donc on peut raisonnablement dire que l'ordre de grandeur de Card$(E(\mathbb{F}_q)$ est plutôt $q$ que $2q + 1$. Le théorème de Hasse qu'on démontrera plus loin donne l'encadrement plus précis suivant : $|\ \mathrm{Card}\, E(\mathbb{F}_q) - (q + 1)\ | \leqslant 2\sqrt{q}$. Pour démontrer ce résultat on a besoin de quelques outils préliminaires.

Soit $E$ est une courbe elliptique définie sur un corps $\mathbb{K}$ et $n$ un entier premier à la caractéristique de $\mathbb{K}$. On sait que le groupe $E[n]$ des points de $n$-torsion est isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. En tant que $\mathbb{Z}/n\mathbb{Z}$-module il est donc libre de rang 2. Il existe alors une famille génératrice de groupe constituée de deux points $(S, T)$ et tout point de $E[n]$ s'écrit sous la forme $P = aS + bT$ avec $a, b \in \mathbb{Z}/n\mathbb{Z}$ et se représente donc par le couple $(a, b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Le point $\mathcal{O}$ s'écrit $\mathcal{O} = 0S + 0T$. Par ailleurs, le groupe $E[n]$ est stable par toute isogénie $\varphi$ car si $P \in E[n]$, puisque $\varphi$ est un morphisme de groupe alors le point $\varphi(P)$ appartient aussi à $E[n]$. Ainsi, si on pose $\varphi(S) = aS + bT$ et $\varphi(T) = cS + dT$, la restriction de $\varphi$ à $E[n]$ sera représentée par la matrice

$$\Phi_n = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in M_2(\mathbb{Z}/n\mathbb{Z})$$

**Proposition 19.1** *Soit $\varphi$ une isogénie de $E$, $n$ un entier non divisible par la caractéristique de $\mathbb{K}$ et $\Phi_n$ la matrice dans une base de $E[n]$ de la restriction de $\varphi$ à $E[n]$. On a :*

$$\deg(\varphi) \equiv \det(\Phi_n) \pmod{n}$$

**Proposition 19.2** *Soit $E$ une courbe elliptique définie sur $\mathbb{F}_q$ et soit $\varphi_q = (x^q, y^q)$ l'isogénie de Frobenius sur $E$. Alors Le morphisme $\varphi_q - [1] : P \to \varphi_q(P) - P$ est une isogénie séparable de $E$ de degré égal à l'ordre du groupe $E(\mathbb{F}_q)$ i.e.* $\deg(\varphi_q - [1]) = \mathrm{Card}\, E(\mathbb{F}_q)$

**Définition 19.3 (Trace d'une courbe elliptique)** *Soit $E$ une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. La trace de $E(\mathbb{F}_q)$ est l'entier $t = q + 1 - \operatorname{Card} E(\mathbb{F}_q)$. Plus généralement, la trace de $E(\mathbb{F}_{q^d})$ de $E$ sur toute extension de degré $d$ de $\mathbb{F}_q$ est $t_d = q^d + 1 - \operatorname{Card} E(\mathbb{F}_{q^d})$*

**Proposition 19.4** *Pour tout entier $n$ non divisible par la caractéristique de $\mathbb{F}_q$, la restriction de $\varphi_q^2 - [t] \circ \varphi_q + [q]$ au groupe de $n$-torsion $E[n]$ est l'isogénie nulle.*

**Corollaire 19.5** *Soit $E$ une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. La trace de $E(\mathbb{F}_q)$ est l'unique entier $t$ vérifiant : $\forall P \in E(\mathbb{F}_q), \varphi_q^2(P) - \varphi_q(tP) + qP = \mathcal{O}$. i.e. que le polynôme $X^2 - tX + q$ peut être vu comme le polynôme caractéristique du Frobenius.*

**Théorème 19.6 (Hasse 1934)** *La trace $t$ de $E(\mathbb{F}_q)$ d'une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ est telle que $-2\sqrt{q} \leqslant t \leqslant 2\sqrt{q}$, autrement dit*

$$| \, q + 1 - \operatorname{Card} E(\mathbb{F}_q) \, | \leqslant 2\sqrt{q}$$

**Théorème 19.7 (Weil)** *Soit $E$ une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ et soit $t$ sa trace i.e. $Card(E(\mathbb{F}_q)) = q + 1 - t$. Alors, pour tout entier non nul $n$, la trace $t_n$ de $E(\mathbb{F}_{q^n})$ vaut $\alpha^n + \beta^n$ où $\alpha$ et $\beta$ sont les racines complexes du polynôme caractéristique de l'isogénie de Frobenius $\varphi_q$. En particulier on a :*

$$\operatorname{Card} E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

**Exemple 19.8** *soit $E : y^2 + y = x^3$ sur le corps $\mathbb{F}_2$. On $\operatorname{Card} E(\mathbb{F}_2) = 3$ donc $t(E(\mathbb{F}_2) = t = q + 1 - t = 2 + 1 - 3 = 0$. Il s'ensuit que le polynôme caractéristique du Frobenius est $X^2 + 2$ dont les racines complexes sont $\pm i\sqrt{2}$ d'où pour tout entier $r > 0$,*

$$\operatorname{Card} E(\mathbb{F}_{2^r}) = \begin{cases} 2^r + 1 & \text{si } r \text{ est impair} \\ 2^r + 1 - 2(-2)^{r/2} & \text{si } r \text{ est pair} \end{cases}$$