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* $T = 0$.

PREUVE : En effet, on a $F(X,Y,0) = 0 \iff X^3 = 0 \iff X = 0$, donc dans le plan projectif $\mathbb{P}^2$, la droite d'équation $T = 0$ et la courbe d'équation $F(X,Y,T) = 0$ se coupent au seul point $P_\infty = [0 : Y : 0] = [0 : 1 : 0]$. Et on a $\frac{\partial F}{\partial T}(P_\infty) = 1$ donc P_∞ est un point lisse. On a aussi $\frac{\partial F}{\partial X}(P_\infty) = 0$ et $\frac{\partial F}{\partial Y}(P_\infty) = 0$. La droite projective tangente à la courbe en ce point a pour équation $\frac{\partial F}{\partial X}(P_\infty)X + \frac{\partial F}{\partial Y}(P_\infty)Y + \frac{\partial F}{\partial T}(P_\infty)T = 0$, donc $T = 0$. (A noter ici qu'il faut préciser que le polynôme F est irréductible pour pouvoir affirmer que $I(C) = (F)$) ∎

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 :*

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

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*

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

PREUVE : La droite projective d'équation $T = 0$ doit être conservée ainsi que le point $[0 : 1 : 0]$. On a donc nécessairement $T' = T$. Pour raison de degrés en x et y, le changement de coordonnées est affine et vu l'absence de terme en y^3, il est forcément de la forme

$$\begin{cases} x &= ax' + r \\ y &= by' + cx' + t \end{cases} \quad \text{avec } ab \neq 0$$

Mais (x,y) et (x',y') vérifient des équations de Weierstrass dont les coefficients de y^2 et de x^3 sont égaux à 1. Or le coefficient de y'^2 est b^2 et celui de x'^3 est a^3. On doit donc avoir $b^2 = a^3$,

et en posant $u = \dfrac{b}{a}$ on a : $u^2 = \dfrac{b^2}{a^2} = \dfrac{a^3}{a^2} = a$ et $u^3 = \dfrac{b^3}{a^3} = \dfrac{b^3}{b^2} = b$. Ainsi, on a $x = u^2x' + r$ et $y = u^3y' + cx' + t$. Enfin, en posant $s = c/u^2$ on a le résultat souhaité. ∎

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

• 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

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

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

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

On définit aussi les quantités

$$\begin{cases} b_8 & = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \\ \Delta & = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \\ j & = c_4^3/\Delta \text{ si } \Delta \neq 0 \end{cases}$$

Définition 2.1 *la quantité Δ 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 $1728\Delta = c_4^3 - c_6^2$:*

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

On remarque que si on donne à chaque a_i le degré i, Δ 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 $(x, y) = (u^2 x', u^3 y')$ 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*

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

PREUVE : (1) est déjà fait (voir ci-dessus)

(2) Remplaçons (x, y) par $(u^2x'+r, u^3y'+u^2sx'+t)$ dans l'équation $y^2 = x^3+ax+b$ on obtient, le coefficient de $x'y'$ est $2su^5$, celui de y' est $2tu^3$et celui de x'^2 est $(s^2-3r)u^4$. Ces trois coefficients doivent être nuls et comme la caractéristique de $\mathbb{K}$ est différente de 2 et 3 et que $u \neq 0$, alors on a $t = 0, s = 0, r = 0$, donc $x = u^2x'$ et $y = u^3y'$.

(3) En reprenant l'équation $y^2 = x^3 + ax + b$, on a $a_1 = a_2 = a_3 = 0; a_4 = a; a_6 = b$, d'où

$$\begin{cases} b_2 &= a_1^2 + 4a_2 = 0 \\ b_4 &= a_1a_3 + 2a_4 = 2a \\ b_6 &= a_3^2 + 4a_6 = 4b \\ c_4 &= b_2^2 - 24b_4 = -48a \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 = -864b \end{cases} \qquad \begin{cases} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 = -a^2 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ &= -8b_4^3 - 27b_6^2 = -16(4a^3 + 27b^2) \\ j(E) &= \dfrac{c_4^3}{\Delta(E)} = \dfrac{2^8 3^3 a^3}{4a^3 + 27b^2} \text{ si } \Delta(E) \neq 0 \end{cases}$$

∎

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 ∎

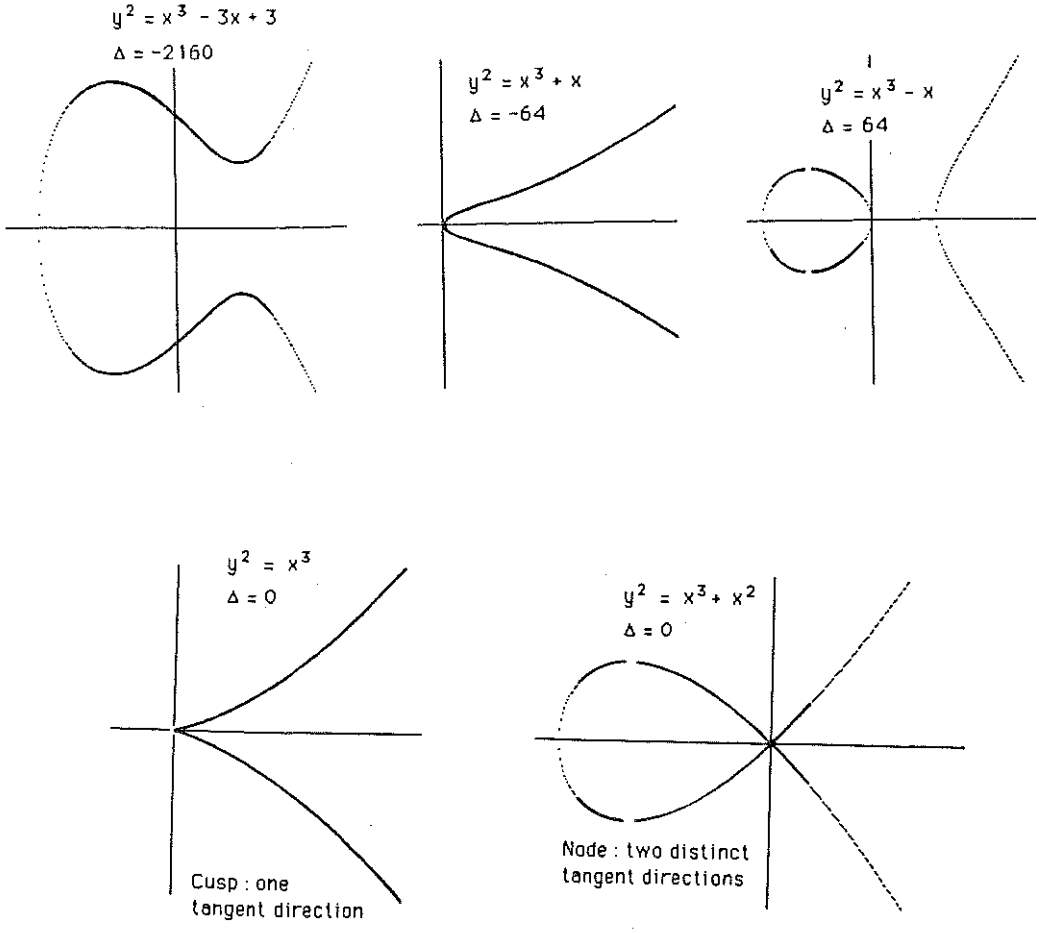
3 Exemples de courbes de Weierstrass

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 $a \geqslant 0$ 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.*

PREUVE : Soit E une courbe de Weierstrass définie sur $\mathbb{K}$ par l'équation de Weierstrass

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

(1) • Supposons que E n'est pas lisse. On sait que le point à l'infini est lisse. Soit alors $P_0 = (x_0, y_0)$ un point singulier de E. En toute caractéristique, le changement de coordonnées $x = x' + x_0$ et $y = y' + y_0$ laisse Δ et c_4 invariants d'après la proposition 2.4, donc on peut supposer que $P_0 = (0, 0)$. On a alors $a_6 = f(0, 0) = 0, a_4 = \frac{\partial f}{\partial x}(0, 0) = 0, a_3 = \frac{\partial f}{\partial y}(0, 0) = 0$ et l'équation E devient $E : f(x, y) = y^2 + a_1xy - a_2x^2 - x^3 = 0$ et pour une telle équation on a : $\Delta(E) = 0$.
• Réciproquement, supposons que $\Delta(E) = 0$ et supposons de plus que la caractéristique de $\mathbb{K}$ est différente de 2 et 3. **(Le cas de la caractéristique 2 ou 3 est traité en exercice 2 des TD)**. L'équation peut être mise sous la forme : $f(x, y) = y^2 - x^3 - a_4x - a_6 = 0$. Un point (x_0, y_0) est un point singulier de E singulier si et seulement si

$$\frac{\partial f}{\partial y}(x_0, y_0) = 2y_0 = 0, \quad \frac{\partial f}{\partial x}(x_0, y_0) = -(3x_0^2 + a_4) = 0, \quad f(x_0, y_0) = 0$$

donc $y_0 = 0$ et x_0 est racine du polynôme $P = x^3 + a_4x + a_6$ et aussi x_0 est racine du polynôme dérivé $P' = 3x^2 + a_4$. Donc le polynôme P admet une racine multiple x_0. Or on a $\Delta(E) = -16(4a_4^3 + 27a_6^2)$. Et par **(l'exercice 4 des TD)**, on sait que $4a_4^3 + 27a_6^2 = 0$ équivaut à dire que le polynôme P admet une racine multiple.

(2) Si $\Delta(E) = 0$ alors la courbe E admet au moins un point singulier $S = (\alpha, 0)$. Or $P := x^3 + a_4x + a_6$ est de degré 3 donc il ne peut avoir qu'une seule racine multiple. Donc S est l'unique point singulier de E. Le polynôme P s'écrit alors $P = (x - \alpha)^2(x - \beta) = x^3 - (2\alpha + \beta)x^2 + (2\alpha\beta + \alpha^2)x - \alpha^2\beta$. D'où $2\alpha + \beta = 0$ donc $\beta = -2\alpha$ et L'équation s'écrit alors :

$$y^2 = x^3 + a_4x + a_6 = (x - \alpha)^2(x + 2\alpha)$$

et par conséquent, on a $a_4 = -3\alpha^2$, $c_4 = -48a_4 = 3^2 2^4 \alpha^2$. Il s'ensuit que :

• Si $c_4 \neq 0$ alors $\alpha \neq 0$, la racine α est donc double. On dit que S est un noeud.

• Si $c_4 = 0$ alors $\alpha = 0$, la racine α est triple. L'équation s'écrit $y^2 = x^3$ et le point singulier S est dit un 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 ϕ, 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 $\ell(D) = \deg D$.*

PREUVE : **de la proposition(4.3)**. Pour tout entier $n \geqslant 1$ l'ensemble $\mathcal{L}(n\mathcal{O}) := \{f \in \mathbb{K}(E), \mathrm{div}(f) + n(\mathcal{O}) \geqslant 0\} \cup \{0\}$ est un espace vectoriel sur $\mathbb{K}$ (car E est définie sur $\mathbb{K}$ voir [S II.5.8]) et il est de $\mathbb{K}$-dimension n d'après le théorème de Riemann-Roch. On choisit des fonctions x, y de $\mathbb{K}(E)$ telles que $\{1, x\}$ soit une base de $\mathcal{L}(2(\mathcal{O}))$ et $\{1, x, y\}$ une base de $\mathcal{L}(3(\mathcal{O}))$ avec $y \notin \mathcal{L}(2(\mathcal{O}))$. Ceci est possible puisque $\mathcal{L}(2(\mathcal{O})) \subset \mathcal{L}(3(\mathcal{O}))$. Remarquons que x admet en $\mathcal{O}$ un pôle d'ordre exact 2 et y admet en $\mathcal{O}$ un pôle d'ordre exact 3 car $x \notin \mathcal{L}((\mathcal{O}))$ sinon elle serait constante car $\mathcal{L}((\mathcal{O}))$ est de dimension 1.

• On a de même $\mathcal{L}(6(\mathcal{O}))$ est de dimension 6. Or, $\mathcal{L}(6(\mathcal{O}))$ contient les 7 fonctions $1, x, y, x^2, xy, y^2, x^3$. Il existe donc des constantes $A_1, \cdots, A_7 \in \mathbb{K}$ tels que

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0$$

On a $A_6A_7 \neq 0$ sinon si $A_6A_7 = 0$, tous les termes de la somme auraient chacun un pôle en O d'ordre tous différents, ce qui les rend linéairement indépendants donc tous les coefficients seraient nuls et la famille de 7 vecteurs dans un espace de dimension 6 serait libre. En remplaçant (x, y) par $(-A_6A_7x, A_6A_7^2y)$ et en divisant par $A_6^3A_7^4$ on obtient l'équation de Weierstrass recherchée et donc l'image de l'application $\phi = [x, y, 1] : E \longrightarrow \mathbb{P}^2$ est contenue dans la courbe de Weierstrass C définie par l'équation ainsi trouvée.

• Enfin, on a bien $\phi(\mathcal{O}) = [x(\mathcal{O}), y(\mathcal{O}), 1] = [\dfrac{x(\mathcal{O})}{y(\mathcal{O})}, 1, \dfrac{1}{y(\mathcal{O})}] = [0, 1, 0]$ car en $\mathcal{O}$, y a un pôle d'ordre 3 et x un pôle d'ordre 2, donc x/y et $1/y$ s'annulent en $\mathcal{O}$.

• Reste à montrer que $\phi : E \longrightarrow C \subset \mathbb{P}^2$ est un isomorphisme de courbes. Or, on sait que **tout morphisme de degré** 1 **entre courbes lisses est un isomorphisme** (voir [S, II, 2. 4.1]). Il suffit donc de montrer que C est lisse et que ϕ est un morphisme de degré 1.

• L'application ϕ est un morphisme (par définition) ou aussi par ([S, II, 2.1]) car E est lisse et $C \subset \mathbb{P}^2$. On sait même qu'il est surjectif par [S, II, 2.3] car non constant et entre deux courbes.

• **Montrons que** $\deg(\phi) = 1$. Par définition $\deg(\phi) = [\mathbb{K}(E) : \phi^*\mathbb{K}(C)]$ où $\phi^* : \mathbb{K}(C) \longrightarrow \mathbb{K}(E)$ est le $\mathbb{K}$-morphisme injectif de corps défini par $\phi^*(f) = f \circ \phi$. Le corps $\phi^*\mathbb{K}(C)$ est le sous-corps de $\mathbb{K}(E)$ engendré sur $\mathbb{K}$ par les fonctions x et y *i.e.* $\phi^*\mathbb{K}(C) = \mathbb{K}(x, y) \subseteq \mathbb{K}(E)$.

• Donc montrer que $\deg(\phi) = 1$ équivaut à montrer que $\mathbb{K}(E) = \mathbb{K}(x, y)$. Pour cela, considérons l'application $\alpha := [x, 1] : E \longrightarrow \mathbb{P}^1$. Puisque x a en O un pôle d'ordre 2 et aucun autre pôle alors $[\mathbb{K}(E) : \mathbb{K}(x)] = 2$. En effet, comme E et $\mathbb{P}^1$ sont lisses alors par [S. II.2.6. a)] on a $\deg(\alpha) = \sum_{P \in \alpha^{-1}(\infty)} e_\alpha(P) = e_\alpha(\mathcal{O})$ car $\alpha(P) = \infty \iff x(P) = \infty \iff P = \mathcal{O}$. Or $e_\alpha(\mathcal{O}) = \mathrm{ord}_{\mathcal{O}}(\alpha^*(t))$ où $t = t_\infty \in \mathbb{K}(\mathbb{P}^1)$ est une uniformisante en $\alpha(\mathcal{O})] = [1, 0] = \infty \in \mathbb{P}^1$. Donc $\alpha^*(t) = \alpha^*(t_\infty) = t_\infty \circ \alpha = 1/x$ et par suite $\deg(\alpha) = e_\alpha(\mathcal{O}) = \mathrm{ord}_{\mathcal{O}}(1/x) = 2$ car $\mathcal{O}$ est un zéro d'ordre 2 de $1/x$. De même l'application $[y, 1] : E \longrightarrow \mathbb{P}^1$ est de degré 3 donc $[\mathbb{K}(E) : \mathbb{K}(y)] = 3$. Il s'ensuit que $[\mathbb{K}(E) : \mathbb{K}(x, y)] = 1$ car ce degré divise 2 et 3. D'où $\mathbb{K}(E) = \mathbb{K}(x, y)$.

• **Montrons maintenant par l'absurde que** C **est lisse**. En fait on montre que toute courbe de Weierstrass singulière est birationnelle à $\mathbb{P}^1$ *i.e.* il existe une application rationnelle $\psi : C \cdots \to \mathbb{P}^1$ de degré 1. En effet, comme le point à l'infini est lisse, soit alors $P = (a, b)$ un point singulier de C. Quitte à faire un changement de coordonnées affines $(X + a, Y + b)$, on peut supposer que le point singulier est le point $(0, 0)$. Le polynôme affine de Weierstrass f qui définit C vérifie alors $F(0, 0) = \dfrac{\partial f}{\partial Y}(0, 0); \dfrac{\partial f}{\partial X}(0, 0) = 0$. Autrement dit $a_6 = a_3 = a_4 = 0$ et l'équation de (C) est donc de la forme

$$Y^2 + a_1XY = X^3 + a_2X^2.$$

L'application rationnelle définie en tout $P \in C$ tel que $X(P) \neq 0$ par

$$\psi = [X, Y] : C \cdots \to \mathbb{P}^1$$

est de degré 1 car de réciproque l'application rationnelle définie par

$$\mathbb{P}^1 \cdots \longrightarrow C\,;\, [1, t] \longrightarrow (t^2 + a_1t - a_2, t(t^2 + a_1t - a_2))$$

On trouve cette réciproque en posant $t = Y/X$ dans $\mathbb{K}(C)$, on a alors : $\dfrac{Y^2}{X^2} + a_1\dfrac{Y}{X} = X + a_2$

i.e. $X = t^2 + a_1 t - a_2$ et par suite $Y = tX = t^3 + a_1 t^2 - a_2 t$.

• Puisque $\phi : E \longrightarrow C$ est aussi de degré 1, la composé $\psi \circ \phi : E \longrightarrow \mathbb{P}^1$ est de degré 1. Or, E et $\mathbb{P}^1$ sont lisses, donc $\psi \circ \phi$ est un isomorphisme. Ceci est absurde car E est de genre 1 et $\mathbb{P}^1$ est de genre 0.

• **Remarque 1.** On peut aussi montrer que $\deg(\psi) = 1$ en utilisant sa définition et le fait que $x = t^2 + a_1 t - a_2$ et $y = tx$:

$\psi^* : \mathbb{K}(\mathbb{P}^1) \longrightarrow \mathbb{K}(C)$ et le degré de ψ est par définition égal au degré de l'extension de corps

$$\deg(\psi) = [\mathbb{K}(C) : \psi^*(\mathbb{K}(\mathbb{P}^1))] = [\mathbb{K}(C) : \mathbb{K}(t)] = [\mathbb{K}(C), \mathbb{K}(X,t)]$$

$$= [\mathbb{K}(C), \mathbb{K}(X,tX)] = [\mathbb{K}(X,Y), \mathbb{K}(X,Y)] = 1$$

car $\psi^*(\mathbb{K}(x))$ est entièrement déterminé par la connaissance de $\psi^*(x) = x \circ \psi = f$ donc $\psi^*(\mathbb{K}(x)) = \mathbb{K}(f)$. Mais dans $\mathbb{K}(C)$ on a :$x = y^2/x^2 + a_1 y/x - a_2 = f^2 + a_1 f - a_2$. Donc $x \in \mathbb{K}(f)$ et $\mathbb{K}(f) = \mathbb{K}(f,x) = \mathbb{K}(x,fx) = \mathbb{K}(x,y) = \mathbb{K}(C)$ et l'extension est donc un isomorphisme de corps et par suite $\psi : C \cdots \to \mathbb{P}^1$ est de degré 1.

• **Remarque 2.** Soient maintenant $\{x,y\}$ et $\{x',y'\}$ deux ensembles de fonctions coordonnées affines de Weierstrass sur E alors $\{1,x\}$ et $\{1,x'\}$ sont deux bases de $\mathcal{L}(2\mathcal{O})$ et de même $\{1,x,y\}$ et $\{1,x',y'\}$ sont deux bases de $\mathcal{L}(3\mathcal{O})$. Il existe donc des constantes $u_1, u_2, r, s_2, t \in \mathbb{K}$ avec $u_1 u_2 \neq 0$ tels que

$$x = u_1 x' + r \qquad y = u_2 y' + s_2 x' + t$$

Mais (x,y) et (x',y') vérifient des équations de Weierstrass dont les coefficients de Y^2 et de X^3 sont égaux à 1. Or le coefficient de y'^2 est u_2^2 et celui de x'^3 est u_1^3. On doit donc avoir $u_2^2 = u_1^3$, et en posant $u = \dfrac{u_2}{u_1}$ et $s = \dfrac{s_2}{u^2}$ on a : $u^2 = \dfrac{u_2^2}{u_1^2} = \dfrac{u_1^3}{u_1^2} = u_1$ et $u^3 = \dfrac{u_2^3}{u_1^3} = \dfrac{u_2^3}{u_2^2} = u_2$ et $s_2 = su^2$. Ainsi, on a $x = u^2 x' + r$ et $y = u^3 y' + su^2 x' + t$. ∎

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 $\mathrm{zeros}(F) \in \mathrm{Div}(C)$:

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

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* $\mathrm{zeros}(L) \in \mathrm{Div}(E)$ *est positif de degré 3 autrement dit*

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

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* $\mathrm{zeros}(L) = (P) + (Q) + (R)$. *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 .*

Preuve : Soit D la droite de $\mathbb{P}^2$ d'équation L. On sait que le support $\mathrm{zeros}(L)$ est l'intersection de D et E. La droite D passe par le point à l'infini $\mathcal{O} = [0 : 1 : 0]$ si et seulement si $\beta = 0$. D'où

deux cas suivant que la droite D passe ou non par le point $\mathcal{O}$.

Cas 1 : si D ne passe pas par le point $\mathcal{O}$, c'est-à-dire si $\beta \neq 0$ alors les points d'intersection de E et D sont à distance finie et on peut faire le calcul avec la courbe affine d'équation

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

De plus, quitte à faire un changement de coordonnées de la forme de (1.4) en posant $y' = \alpha x + \beta y + \gamma$, on peut supposer que D a pour équation $y = 0$. Dans $\overline{\mathbb{K}}[x]$, le polynôme $f(x,0) = -x^3 - a_2x^2 - a_4x - a_6$ définissant l'intersection de E et D est un polynôme de degré 3 en x qui se factorise sous la forme :

$$f(x,0) = -(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

L'intersection de D et de E est donc formée des 3 points (non nécessairement distincts) $P_i = (\alpha_i, 0), i = 1,2,3$. La droite D d'équation $y = 0$ a pour vecteur normal le vecteur $(0,1)$ donc elle est tangente en P_i à E si et seulement si le vecteur $\Big((\partial f/\partial x)(P_i), (\partial f/\partial y)(P_i)\Big)$ est colinéaire à $(0,1)$ autrement dit si et seulement si $(\partial f/\partial x)(\alpha_i, 0) = 0$ ou encore si et seulement α_i est racine multiple de $f(x,0)$. Donc

• si les α_i sont deux à deux distincts alors D n'est pas tangente à E et ils ont 3 points distincts d'intersection, et on sait dans ce cas que $\mathrm{ord}_{P_i}(L) = 1$ car D n'est pas tangente à E en chacun des points P_i. Donc

$$\mathrm{zeros}(L) = (P_1) + (P_2) + (P_3)$$

• Si deux des α_i sont égaux, par exemple $\alpha_1 = \alpha_2 \neq \alpha_3$, il y a 2 points distincts d'intersection (P_1 et P_3) et D n'est pas tangente à E en P_3, donc l'ordre de L en P_3 est 1. Et on a dans $\overline{\mathbb{K}}[E]$:

$$y(y + a_1x + a_3) = y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 = (x-\alpha_1)^2(x-\alpha_3)$$

Le point P_1 est un point lisse de E et puisque $(\partial f/\partial x)(\alpha_1, 0) = 0$ car D est tangente à E en P_1 alors $(\partial f/\partial y)(\alpha_1, 0) = a_1\alpha_1 + a_3 \neq 0$. Donc la fonction $y + a_1x + a_3$ ne s'annule pas en P_1 et par suite $\mathrm{ord}_{P_1}(y + a_1x + a_3) = 0$. D'autre par $\mathrm{ord}_{P_1}(y) > 0$ car la fonction y s'annule en P_1. Donc $\mathrm{ord}_{P_1}(y) + \mathrm{ord}_{P_1}(y + a_1x + a_3) = \mathrm{ord}_{P_1}(y) = \mathrm{ord}_{P_1}(x-\alpha_1)^2(x-\alpha_3) = 2$ Et

$$\mathrm{zeros}(L) = 2(P_1) + (P_3)$$

• Enfin si $\alpha_1 = \alpha_2 = \alpha_3$ on a de même que $\mathrm{ord}_{P_1}(y) = \mathrm{ord}_{P_1}(x-\alpha_1)^3 = 3$ et

$$\mathrm{zeros}(L) = 3(P_1)$$

Cas 2 : si D passe par le point $\mathcal{O}$ alors $\beta = 0$ et $L = \alpha X + \gamma T$. Posons $F(X, Y, T) = 0$ une équation homogène de E. On sait qu'une équation de la tangente à E en $\mathcal{O}$ est $T = 0$ car $\partial F/\partial X(\mathcal{O}) = \partial F/\partial Y(\mathcal{O}) = 0$ et $\partial F/\partial T(\mathcal{O}) = 1$. D'où deux sous-cas selon que la droite D est tangente ou non à E en $\mathcal{O}$:

• Si $\alpha \neq 0$, alors D n'est pas tangente à E en $\mathcal{O}$ et par suite $\text{ord}_{\mathcal{O}}(L) = 1$. On peut, quitte à faire un changement de coordonnées de la forme de (1.4) en posant $x' = \alpha x + \gamma$, on peut supposer que D a pour équation $x = 0$ et faire le calcul comme dans le cas 1. Dans $\overline{\mathbb{K}}[x]$, le polynôme $f(0, y) = y^2 + a_3 y = y(y + a_3)$ définissant l'intersection de E et D est un polynôme de degré 2 en y. L'intersection de D et de E est donc formée des 2 points finis distincts $Q_1 = [0 : 0 : 1]$ et $Q_2 = [0 : a_3 : \lambda]$ si $a_3 \neq 0$ ou un point double fini $Q = [0 : 0 : 1]$ si $a_3 = 0$ et on a respectivement

$$\text{zeros}(L) = (O) + (Q_1) + (Q_2) \quad \text{ou} \quad \text{zeros}(L) = (O) + 2(Q)$$

• Si $\alpha = 0$, une équation de D est $T = 0$ et l'équation $F(X, Y, 0)$ définissant l'intersection de E et D se réduit à $X^3 = 0$ donnant $\mathcal{O}$ comme point triple et on a $\text{zeros}(L) = \text{zeros}(T) = 3(\mathcal{O})$ ∎

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

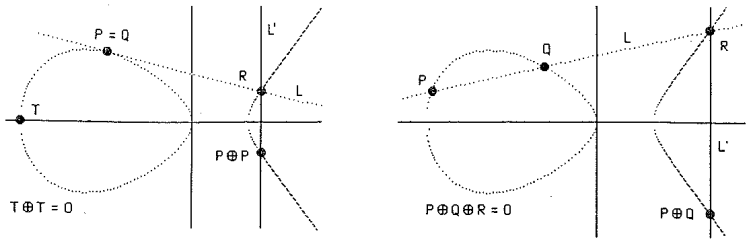
$$\text{zeros}(X) = (P_1) + (P_2) + (\mathcal{O})$$
$$\text{zeros}(Y) = (Q_1) + (Q_2) + (Q_3)$$
$$\text{zeros}(T) = 3(\mathcal{O})$$

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.*

PREUVE : Soit L l'équation de la droite PQ si P et Q sont distincts, et de la tangente en P si $P = Q$. Alors le diviseur $\text{zeros}(L) - (P) - (Q)$ qui est de degré 1 fournit le point cherché. ∎

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'élément 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 $(P+Q)+R=\mathcal{O}$.*

PREUVE : **1)** si P, Q, R sont alignés sur E alors le point $S = P + Q$ est le troisième point d'intersection de E et de la droite (OR). En appliquant (5.4) aux points S et R on a $(S+R)$ est le troisième point d'intersection de E et de la droite $(\mathcal{O}\mathcal{O})$ *i.e.* la tangente à E en $\mathcal{O}$. Or cette tangente coupe E encore en $\mathcal{O}$ car $\mathcal{O}$ est un point d'inflexion de E, donc $(P+Q)+R=\mathcal{O}$.
2) pour tout $P \in E$ on $P+\mathcal{O}=P$. En effet en appliquant (5.4) à P et $Q=\mathcal{O}$ on aura La droite L coupe E en $P, \mathcal{O}, R$ et L' coupe E en $R, \mathcal{O}, P+\mathcal{O}$, donc $P+\mathcal{O}=P$
3) on a $P+Q=Q+P$ car la construction donnée par (5.4) es symétrique en P et Q.
4) pour tout $P \in E$ il existe $R=-P \in E$ tel que $P+R=O$. En effet, la droite $(\mathcal{O}P)$ coupe E en $\mathcal{O}, P$ et R. En utilisant 1) et 2) on a $(P+\mathcal{O})+R=\mathcal{O}$ et par suite $P+R=\mathcal{O}$. Donc $-P$ et le troisième point d'intersection de la droite (OP) et E.
5) l'associativité peut être prouvée à l'aide des formules explicites ci-dessous ou géométriquement.
6) si P et Q sont deux points finis dans $E(\mathbb{K})$, leur coordonnées sont dans $\mathbb{K}$ et les coefficients d'une équation de la droite (PQ) sont dans $\mathbb{K}$. Donc si E est aussi définie sur $\mathbb{K}$ alors le troisième point d'intersection R de E et de la droite (PQ) est dans $E(\mathbb{K})$ car ses coordonnées sont donnés par des fonctions rationnelles en les coordonnées de P et Q et en les coefficients de E. ∎

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*

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

Preuve : Posons $f(x, y) = y^2 + a_xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$

(1) Soit $P_0 = (x_0, y_0) \in E$. Pour calculer $-P$ on prend la droite $L = (OP_0)$ et on cherche $L \cap E$. La droite L a pour équation affine $\ell = x - x_0$ soit pour équation projective $L = X - x_0T$. On vérifie bien que les coordonnées projectives de $\mathcal{O} = [0 : 1 : 0]$ et ceux de $P_0 = [x_0 : y_0 : 1]$ vérifient cette équation. Les points d'intersection de E et L vérifie donc l'équation $f(x_0, y) = 0$ qui est de second degré en y donc ses racines sont y_0 et y_0' où $-P_0 = (x_0, y_0')$. En factorisant $f(x_0, y)$ en $f(x_0, y) = (y - y_0)(y - y_0')$ et en identifiant les coefficients on aura $y_0' = -y_0 - a_1x_0 - a_3$. D'où $-P = (x_0, -y_0 - a_1x_0 - a_3)$.

(2) et (3) si $x_1 = x_2$ et $y_1 + y_2 + a_1x_2 + a_3 = 0$ alors d'après (1) on a $P_1 + P_2 = O$. Sinon la droite $L = (P_1P_2)$ (ou la tangente L à E en P si $P_1 = P_2 = P$) a pour équation affine

$$\ell = y - \lambda x - \nu \quad \text{avec}$$

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

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \quad \text{et} \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \quad \text{si} \quad x_1 = x_2$$

et en remplaçant y par $\lambda x + \nu$ dans l'equation de E on aura une équation de troisième degré , $f(x, \lambda x + \nu) = 0$ qui a pour solutions x_1, x_2, x_3 où $P_3(x_3, y_3)$ est le troisième point d'intersection de L et E. On a $P_1 + P_2 + P_3 = \mathcal{O}$. En écrivant $f(x, \lambda x + \nu) = -(x - x_1)(x - x_2)(x - x_3)$ et en identifiant les coefficients on aura $x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2$. On trouve y_3 en remplaçant x_3 dans l'équation de L. Enfin, on trouve $P_1 + P_2 = -P_3$ en utilisant la formule du (1) qui donne l'opposé d'un point. ∎