Cryptographie à base de courbes elliptiques

Par Bachir Jean El Hage

10 Avril 2006

Université Joseph Fourier
Master Mathématique - TER Recherche
Grenoble 1 - FRANCE

Table des matières

1 Préliminaire

1.1 Espace projectif

Définition 1.1. *Soit K un corps commutatif. L'*espace projectif $\mathbb{P}_n(K)$ *de dimension n sur K est l'ensemble des droites vectorielles de K^{n+1}.*

L'application :

$$\pi : K^{n+1} - \{0\} \longrightarrow \mathbb{P}_n(K), \;\; X \longmapsto KX$$

est appelée la projection canonique et l'on a, pour tout $(X, Y) \in K^{n+1} - \{0\}$,

$$\pi(X) = \pi(Y) \Leftrightarrow X = \lambda Y (\text{X et Y sont colinéaires}).$$

On peut alors écrire l'espace projectif $\mathbb{P}_n(K)$ comme un quotient de $K^{n+1} - \{0\}$par la relation d'équivalence définie par :

$$X \sim X' \Leftrightarrow (\exists \lambda \in K^*, X = \lambda X') \tag{1}$$

On note $(x_1 : x_2 : ... : x_n)$ l'image de $(x_1, .., x_{n+1})$ par π.

Définition 1.2. *Le* plan projectif $\mathbb{P}_2(K)$ *sur K est un espace projectif de dimension 2.*

Définition 1.3. *Soit K un corps. On dit qu'un polynôme $F \in K[x, y, w]$ est* homogène *de degré d si tout les monômes de F sont de degré d.*

Exemple : $P(x, y) = x^7 + 4y^3x^4 + 8yx^6$.

Remarque : $F \in K[x_1, .., x_n]$ de degré $d > 0$ est homogène si et seulement si

$$F(\lambda x_1, \cdots, \lambda x_n) = \lambda^d F(x_1, \cdots, x_n) \text{ pour } x_i, \lambda \in K.$$

1.2 Courbes projectives planes

Définition 1.4. *Soit K un corps et $\overline{K}$ une clôture algébrique de K. Une* courbe projective plane *C est un sous-ensemble de $\mathbb{P}_2(\overline{K})$ défini par un polynôme homogène non constant $F \in K[X,Y,Z]$:*

$$C \in C_F = \{(X:Y:Z) \in \mathbb{P}_2(K) \,|F(X,Y,Z) = 0\}\,.$$

- *Si deg(F)=1* : alors C_F est une *droite projective.*

- *Si deg(F)=2* : alors C_F est une *conique.*
- *Si deg(F)=3* : alors C_F est une *cubique plane.*
  Exemple : C : Y^2Z= $X^3 + aXZ^2 + bZ^3$ est une cubique.

1. **Remarque 1 :** $\mathbb{P}_2(K) = U_0 \cup L_\infty(K)$ (union disjointe)
   pour $U_0 = \{(x:y:z)\,|z \neq 0\}$, $L_\infty(K) = \{(x:y:z)\,|z = 0\}$(droite a l'infini).
   Notons $\mathbb{A}^2$(K)=$\{(x,y) \in K^2\}$ le plan affine sur K.
   L'application

$$\begin{array}{ccc} \mathbb{A}^2(K) & \longrightarrow & U_0 \\ (x,y) & \longmapsto & (x:y:z) \end{array}$$

   est bijective (l'application réciproque est $(x:y:z) \longmapsto (x/z, y/z)$).
   De même l'application $\mathbb{P}^1$(k) $\to L_\infty$, $(x,y) \longmapsto (x:y:0)$ est bijective.
   Les plans $U_1 = \{(x:y:z)\,|x \neq 0\}$ et $U_2 = \{(x:y:z)\,|y \neq 0\}$ peuvent être également vus commes des plans affines :
   On a une bijection de U_1 sur $\mathbb{A}^2(K)$ $(x:1:z) \longmapsto (x,z)$ et on a $\mathbb{P}^2(k) = U_0 \cup U_1 \cup U_2$ (un des x, y, z est non nul)

2. **Remarque 2** : Soit C : Y^2Z= $X^3 + aXZ^2 + bZ^3$ une cubique,
   $C \cap L_\infty$=(0 :1 :0) c'est l'unique point de C se trouvant sur L_∞, on l'appelle le « point à l'infini ».
   Et on vérifie que :
   - $C \cap U_0$ est la courbe affine plane $C_0 : Y^2 = X^3 + aX + b$
   - $C \cap U_1$ est la courbe affine plane $C_1 : Z = X^3 + aXZ^2 + bZ^3$
   - $C \cap U_2$ est la courbe affine plane $C_2 : Y^2Z = aZ^2 + bZ + 1$

Proposition 1.1. *Soit K un corps.*
1. Soient $L_1 : aX + bY + cW = 0$ et $L_2 : a'X + b'Y + c'W = 0$ deux droites distinctes de $\mathbb{P}_2(K)$, alors L_1 et L_2 admettent un unique point d'intersection.
2. Par deux points distincts $p_1 = (a_1, b_1, c_1)$ et $p_2 = (a_2, b_2, c_2)$ de $\mathbb{P}_2$ passe une unique droite.

Démonstration. 1. Soit l'application linéaire,

$$\begin{array}{ccc} \mathbb{P}_2(K) & \to & \mathbb{P}_2(K) \\ \begin{pmatrix} X \\ Y \\ W \end{pmatrix} & \longmapsto & \begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} \begin{pmatrix} X \\ Y \\ W \end{pmatrix} \end{array}$$

Le rang de la matrice $\begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix}$ est 2, puisque L_1 et L_2 sont distinctes,

et donc le noyau est de dimension 3-2=1.

2. De même, on prend l'application linéaire

$$\begin{array}{ccc} \mathbb{P}_2(K) & \to & \mathbb{P}_2(K) \\ \begin{pmatrix} a \\ b \\ c \end{pmatrix} & \longmapsto & \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} \end{array}$$

comme p_1 et p_2 sont distincts, la matrice $\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix}$ est de rang 2, et donc le noyau est de dimension 1.

□

1.3 Intersection d'une droite et d'une courbe

Soient L une droite définie par le polynôme $D(X,Y,W) \in K[X,Y,W]_1$, $C \in \mathbb{P}_2(K)$ une courbe projective définie sur K par le polynôme $F(X,Y,W) \in K[X,Y,W]_d$ et $p_1 = (x_0, y_0, w_0) \in L(K) \cap C(K)$.

Soit ϕ une transformation projective telle que $\phi(x_0, y_0, w_0) = (0,0,1)$, et alors

$$\begin{aligned} f(x,y) = F(\phi^{-1}(x,y,1)) &= f_1(x,y) + ... + f_d(x,y) \\ &\text{(les } f_i \text{ sont homogènes)} \\ l(x,y) = D(\phi^{-1}(x,y,1)). & \end{aligned}$$

$l(0,0) = D(\phi^{-1}(0,0,1)) = D(x_0, y_0, w_0) = 0$ donc $l(x,y) = bx - ay$ avec a, b constantes non toutes les deux nulles. Alors $\varphi(t) = \begin{pmatrix} at \\ bt \end{pmatrix}$ paramètre

$l(x,y) = 0$, $\varphi(0) = 0$. Nous pouvons écrire $f(\varphi(t))$ comme un polynôme en t, i.e

$$\begin{aligned} f(\varphi(t)) &= f_1(at,bt) + f_2(at,bt) + .. + f_d(at,bt) \\ &= tf_1(a,b) + t^2 f_2(a,b) + .. + t^d f_d(a,b) \end{aligned}$$

donc $f(\varphi(t))$ est un polynôme en t vérifiant $f(\varphi(0)) = 0$.

Définition 1.5. *Pour les même notation qu'avant, on dit que la* multiplicité d'intersection *de L avec C en p_1 est m si*

$$f_m \neq 0 \text{ et } \forall\ k < m\ f_k = 0$$

On dit que cette multiplicité est infinie si $f \circ \varphi = 0$, ce qui revient à dire que $L \in C$. On note $i(p_1, L, C)$ cette multiplicité d'intersection. Par abus de langage, si C est définie par un polynôme F n'admettant pas de facteurs carré, on note également $i(p_1, L, F)$ pour $i(p_1, L, C)$.

Remarque :

- ▷ Si $p \notin\ L(k) \cap C(k)$, on définit $I(p_1, L, C) = 0$.
- ▷ $I(p, L, C)$ ne dépend pas de ϕ choisie.

Autrement dit, la multiplicité d'intersection de L et de C en p est l'ordre de 0 comme racine du polynôme $F(0, T, 1)$ en $T = 0$.

Exemple : Soit la courbe projective d'équation $YT^{n-1} = X^n$ à laquelle correspond la courbe affine $Y = X^n$ qu'on appelle C, la multiplicité d'intersection de C avec la droite $Y = 0$ en (0,0) est donné par l'ordre de 0 comme racine de x^n, c'est à dire n.

1.4 Transformation projective

Soit K un corps et ϕ une matrice de $GL_3(K)$, ϕ induit une application de $\mathbb{P}_2(K) \to \mathbb{P}_2(K)$ ($\phi v = 0$ si et seulement si $v = 0$).

Soit (x_0, y_0, w_0) un point de $\mathbb{P}_2(K)$ et choisissons $\phi \in GL_3(K)$ telle que $\phi(x_0, y_0, w_0) = (0, 0, 1)$. Cela permet de définir des coordonnées affines sur $\phi^{-1}(K \times K \times \{1\})$ par

$$\varphi(\phi^{-1}(x, y, 1)) = (x, y)$$

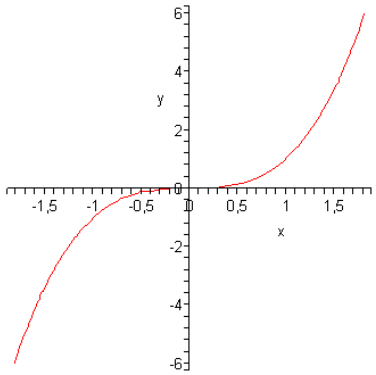


FIGURE 1 – multiplicité d'intersection de $Y = X^3$ avec $Y = 0$ égal à 3 en (0,0).

Exemple 1. Soit $(x_0, y_0, w_0) = (x_0, y_0, 1)$. On peut choisir $\phi = \begin{pmatrix} 1 & 0 & -x_0 \\ 0 & 1 & -y_0 \\ 0 & 0 & 1 \end{pmatrix}$.

Alors

$$\phi \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -x_0 \\ 0 & 1 & -y_0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} x - x_0 \\ y - y_0 \\ 1 \end{pmatrix}$$

dans ce cas, les coordonnées affines sont définies sur

$$\phi^{-1}(K \times K \times \{1\}) = K \times K \times \{1\}$$

et sont données par

$$\begin{aligned} \varphi(x, y, 1) &= \varphi(\phi^{-1}(\phi(x, y, 1))) \\ &= \varphi(\phi^{-1}(x - x_0, y - y_0, 1)) = (x - x_0, y - y_0, 1). \end{aligned}$$

Un tel ϕ est utile pour passer de $(x_0, y_0, 1) \in \mathbb{P}_2(K)$ à $(0, 0) \in K^2$.

Exemple 2. Soit maintenant $(x_0, y_0, w_0) = (0, 1, 0)$. On peut choisir $\phi = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. Alors

$$\phi \begin{pmatrix} x \\ 1 \\ w \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ 1 \\ w \end{pmatrix} = \begin{pmatrix} w \\ x \\ 1 \end{pmatrix}$$

et

$$\varphi(x,1,w) = \varphi(\phi^{-1}(\phi(x,1,w))) = \varphi(\phi(w,x,1)) = (w,x).$$

Un tel ϕ sera utile pour l'étude du « point à l'infini »sur une courbe sous forme de Weierstrass.

Soit F un polynôme homogène non nul de degré strictement positif et soit $\phi \in GL_3(K)$ telle que $\phi(x_0, y_0, 1) = (0, 0, 1)$, on définit

$$f(x,y) = F(\phi^{-1}(x,y,1)).$$

Application. Soit $(x_0, y_0, w_0) = (x_0, y_0, 1)$ et soit

$$\phi = \begin{pmatrix} 1 & 0 & -x_0 \\ 0 & 1 & -y_0 \\ 0 & 0 & 1 \end{pmatrix}$$

Alors

$$\phi^{-1} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} x + x_0 \\ y + y_0 \\ 1 \end{pmatrix}$$

Alors

$$f(x,y) = F(x + x_0, y + y_0, 1).$$

Pour $F(x,y,w) = x^2y + xyw + w^3$.

$$\begin{aligned} f(x,y) &= (x_0^2y_0 + x_0y_0 + 1) + ((2x_0y_0 + y_0)x + (x_0^2 + x_0)y) \\ &\quad + (y_0x^2 + (2x_0 + 1)xy) + (x^2y) \\ &= (x_0^2y_0 + x_0y_0 + 1) + (x_0^2y + 2x_0y_0x + x_0y + y_0x) \\ &\quad + (y_0x^2 + 2x_0xy + xy) + (x^2y) \\ &= f_0(x,y) + f_1(x,y) + f_2(x,y) + f_3(x,y) \end{aligned}$$

pour tout $i \in \{0,1,2,3\}$ f_i est un polynôme homogène de degré i.

$f_0 = 0$ si $(x_0, y_0, 1)$ est sur la courbe C définie par le polynôme F (ie si $F((x_0, y_0, 1) = 0)$.

Dans cet exemple, et en général, f est la somme de d polynômes homogènes de degré allant de 1 à d qui dépendent de $(x_0, y_0, 1)$ et de ϕ.

1.5 Singularité et points d'inflexion

Pour ce paragraphe nous utiliserons les mêmes notation de ce qui précède.

Définition 1.6. *Soit K un corps, C une courbe projective définie par le polynôme F sur K et soit $p = (x_0 : y_0 : w_0) \in C$. On dit que p est un* point singulier *de C si et seulement si f_1 est le polynôme nul dans $K[x, y]$. La courbe C est dite non-singulière si elle n'admet aucun point singulier.*

Remarque. La définition 1.6 est équivalente à :
Un point p de C est un point singulier si est seulement si

$$\left(\frac{\partial F}{\partial X}\right)_p = \left(\frac{\partial F}{\partial Y}\right)_p = \left(\frac{\partial F}{\partial Z}\right)_p = 0 \tag{2}$$

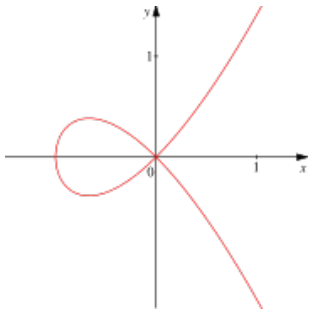


FIGURE 2 – exemple de courbe possédant un point singulier.

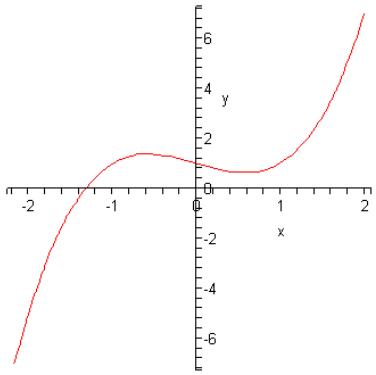


FIGURE 3 – exemple de courbe sans point singulier.

Définition 1.7. *Un point P non-singulier d'une courbe projective plane C est appelé* point d'inflexion *de C lorsque la multiplicité d'intersection en P de C et de la tangente à C en P est supérieure ou égale à trois.*

Exemple 1. Recherche de points singuliers par passage au *plan affine.*
Soit C une courbe projective définie par un polynôme F, soit $(x_0, y_0, z_0) \in C(\overline{K})$ et si ϕ une matrice 3×3 telle qu'on ait $\phi(x_0, y_0, w_0) = (0, 0, 1)$, alors l'équation de la courbe C dans le plan affine correspondant est

$$f(x, y) = F(\phi^{-1}(x, y, 1)) \in k[x, y]. \tag{3}$$

On cherche les point singuliers (x, y, w) de F tels que $w = 1$:
Regardons un exemple :
Soit C la courbe projective définie par le polynôme

$$F(x, y, w) = x^2y + xyw + w^3 \tag{4}$$

On choisit la matrice $\phi = \begin{pmatrix} 1 & 0 & -x_0 \\ 0 & 1 & -y_0 \\ 0 & 0 & 1 \end{pmatrix}$

on verifie que $\phi(x_0, y_0, 1) = (0, 0, 1)$ et que $\phi^{-1} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} x + x_0 \\ y + y_0 \\ 1 \end{pmatrix}$

$$\begin{aligned} f(x,y) &= F(x+x_0, y+y_0, 1) \in k[x,y] \\ &= (x_0^2 y_0 + x_0 y_0 + 1) + (x_0^2 y + 2x_0 y_0 x + x_0 y + y_0 x) \\ &\quad + (y_0 x^2 + 2x_0 xy + xy) + (x^2 y) \\ &= f_0(x,y) + f_1(x,y) + f_2(x,y) + f_3(x,y) \end{aligned}$$

où f_i est homogène de degré i.

Le point $(x_0, y_0, 1)$ est un point *non-singulier* si f_1 n'est pas nulle dans $K[x,y]$.

Dans notre exemple (w_0=1) :

$$f_1(x,y) = (2x_0 y_0 + y_0)x + (x_0^2 + x_0)y. \tag{5}$$

Pour que $(x_0, y_0, 1)$ soit un point singulier de $C(K)$ il faut et il suffit que les coefficients de x et y soient nuls tous les deux, on résout le systeme :

$$\begin{cases} 2x_0 y_0 + y_0 = 0 \\ x_0^2 + x_0 = 0 \end{cases}$$

et on obtient $(x_0, y_0) = (0,0)$ et $(x_0, y_0) = (-1, 0)$.
Dans $\mathbb{P}_2$(K) ces points sont $(0,0,1)$ et $(-1,0,1)$, mais aucun d'eux n'annule F. Et par suite C est non-singulière en tout point de $C(K)$ pour $w_0 = 1$.
(NB : La notion de non-singularité ne dépend pas du choix de la matrice ϕ).

Exemple 2. Recherche de *points d'inflexion*

Soit C une courbe donnée par un polynôme F, nous voulons savoir si $(x_0, y_0, 1)$ est un *point d'inflexion* de $F(K)$.

On peut prendre $\phi = \begin{pmatrix} 1 & 0 & -x_0 \\ 0 & 1 & -y_0 \\ 0 & 0 & 1 \end{pmatrix}$ et alors

$f(x,y) = F(\phi^{-1}(x,y,1)) = F(x+x_0, y+y_0, 1) = f_0 + f_1 + f_2 + .. + f_d$.

Le point $p = (x_0, y_0, 1)$ est un *point d'inflexion* de C si

1. $p \in C$ (ie. si le terme constant $f_0 = 0$)
2. p est non-singulier (ie. $p \in C$ et $f_1(x,y) \neq 0$)
3. $f_2(x,y)$ satisfait $f_2(a,b) = 0$ pour a, b définis par $f_1(x,y) = bx - ay$.

Remarque : La dernière condition est équivalente à : $f_1(x,y)$ divise $f_2(x,y)$.

Démonstration. (de la remarque) Soit $f_2(x,y) = cx^2+dxy+ey^2$ et $f_1(x,y) = bx-ay$, supposons que $f_2(x,y) = cx^2+dxy+ey^2 = (bx-ay)(rx+sy)$. Alors on a
$c = br, d = -ar+bs, e = -as$ d'où $ca^2+dab+eb^2 = 0$.
Réciproquement, si $ca^2+dab+eb^2 = 0$ on définit $r = c/b$ et $s = -e/a$, et on conclut en séparant les cas où $b = 0$ ou $a = 0$. □

Exemple **:** Soit $F(x,y,w) = x^2y+xyw+w^3$. Quels sont les points $(x,y,1)$ qui sont des points d'inflexions ?
Nous avons déjà vu pour $(x_0,y_0,1)$ que

$$\begin{aligned} f(x,y) &= F(x+x_0, y+y_0, 1) \in k[x,y] \\ &= (x_0^2y_0 + x_0y_0 + 1) + (x_0^2y + 2x_0y_0x + x_0y + y_0x) \\ &\quad + (y_0x^2 + 2x_0xy + xy) + (x^2y) \\ &= f_0(x,y) + f_1(x,y) + f_2(x,y) + f_3(x,y) \end{aligned}$$

Le point $(x_0,y_0,1)$ est sur la courbe cela implique que $f_0(x,y) = 0$.
Si on pose $b = 2x_0y_0 + y_0$ et $a = -(x_0^2+x_0)$, la condition pour que $(x_0,y_0,1)$ soit un point d'inflexion est

$$0 = f_2(a,b) = y_0a^2 + (2x_0y_0)ab.$$

Si le corps K n'est pas de caractéristique 2, il y a une autre méthode plus élégante pour trouver les points d'inflexions sans passage au coordonnées affines.

Introduisons la *Matrice Hessienne* qui nous servira pour la suite :

La *matrice hessienne* d'une fonction polynômiale F est la matrice carrée, notée H(F), de ses dérivées partielles secondes :

$$H = H(x_0,y_0,w_0) = \begin{pmatrix} \frac{\partial^2 F}{\partial x^2} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial w} \\ \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial y^2} & \frac{\partial^2 F}{\partial y \partial w} \\ \frac{\partial^2 F}{\partial x \partial w} & \frac{\partial^2 F}{\partial y \partial w} & \frac{\partial^2 F}{\partial w^2} \end{pmatrix}_{(x_0,y_0,w_0)} \tag{6}$$

Proposition 1.2. *Soit K est un corps de caractéristique $\neq 2$ et soit C une courbe plane sur K définie par le polynôme F de degré ≥ 2. Soit (x_0,y_0,w_0) un point non-singulier de la courbe C, alors (x_0,y_0,w_0) est un* point d'inflexion *si et seulement si la matrice Hessienne de F satisfait* $\det H(x_0,y_0,w_0) = 0$ *(ce determinant s'appelle aussi Hessien).*

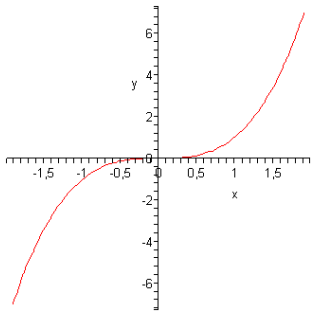


FIGURE 4 – Courbe possédant un point d'inflexion en (0,0).

Exemple : Soit $F(x, y, w) = x^2y + xyw + w^3$, la matrice Hessienne au point $(x_0, y_0, 1)$ est

$$\begin{pmatrix} 2y_0 & 2x_0+1 & y_0 \\ 2x_0+1 & 0 & x_0 \\ y_0 & x_0 & 6 \end{pmatrix}$$

d'après la proposition précedente $(x_0, y_0, 1)$ est un point d'inflexion si et seulement si le Hessien $\mathrm{H}(x_0, y_0, 1)$=0, c'est à dire

$$2y_0(x_0^2 + x_0) - 6(2x_0 + 1)^2 = 0. \tag{7}$$

en utilisant le fait que $f_0(x, y) = 0$, cette equation devient :

$$3(2x_0 + 1)^2 = -1. \tag{8}$$

1.6 Tangente

Définition 1.8. *Soit K un corps et E un courbe projective plane définie par le polynôme F sur K. L'équation de la* tangente *L en (x_0, y_0, w_0) est*

$$\left[\frac{\partial F}{\partial x}\right]_{(x_0,y_0,z_0)} x + \left[\frac{\partial F}{\partial y}\right]_{(x_0,y_0,z_0)} y + \left[\frac{\partial F}{\partial w}\right]_{(x_0,y_0,z_0)} w = 0. \tag{9}$$

1.7 Définition d'une courbe elliptique

Une *courbe elliptique* sur un corps K est une courbe projective plane non-singulière E définie par une équation homogène irréductible de degré 3 sur K, munie d'un point $\mathrm{O} \in E(K)$.

2 Courbes elliptiques sous forme de Weierstrass

Dans tout cette partie on note K un corps.

2.1 Équation générale d'une cubique

Une cubique C est définie par un polynôme F (sur K) dont la forme générale est

$$\begin{aligned} F(x,y,w) = c_{yyy}y^3 + c_{xyy}xy^2 + c_{xxy}x^2y + c_{yyw}y^2w + c_{xyw}xyw \\ +c_{yww}yw^2 + c_{xxx}x^3 + c_{xxw}x^2w + c_{xww}xw^2 + c_{www}w^3. \end{aligned} \tag{10}$$

Réductions possibles :

Condition 1 : Par une transformation linéaire de K^3 on peut se ramener au cas où la courbe passe par le point (0,1,0) ce qui equivaut à dire que

$$c_{yyy} = 0. \tag{11}$$

Condition 2 : De même, par une transformation linéaire on peut se ramener au cas où le point (0,1,0) soit un *point non-singulier*, pour le vérifier nous allons utiliser la méthode de l'exemple ci-dessus, pour cela prenons $\phi = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ (on a bien $\phi(0,1,0) = (0,0,1)$)

$$\begin{aligned} f(x,y) = F(\phi^{-1}(x,y,1)) &= F(y,1,x) \\ &= c_{xyy}y + c_{xxy}y^2 + c_{yyw}x + c_{xyw}xy + c_{yww}x^2 \\ &\quad + c_{xxx}y^3 + c_{xxw}y^2 + c_{xww}yx^2 + c_{www}x^3 \end{aligned}$$

d'où

$$f_1(x,y) = c_{xyy}y + c_{yyw}x. \tag{12}$$

il faut qu'un des coefficients de x et y soit non nul, ce qui veut dire que

$$c_{xyy} \neq 0 \quad \text{ou} \quad c_{yyw} \neq 0. \tag{13}$$

Condition 3 : De même, par une transformation linéaire on peut se ramener au cas où « *la droite à l'infini* »$L(x,y,w) = w$ soit tangente à la courbe en (0,1,0), en appliquant la relation de la définition 1.8 on obtient

$$\left[\frac{\partial F}{\partial x}\right]_{(0,1,0)} x + \left[\frac{\partial F}{\partial y}\right]_{(0,1,0)} y + \left[\frac{\partial F}{\partial w}\right]_{(0,1,0)} w = c_{yyw}x + c_{xyy}y. \tag{14}$$

d'où

$$L(x, y, w) = c_{yyw}w + c_{xyy}x. \tag{15}$$

La condition est que

$$c_{xyy} = 0$$

et alors la tangente est w.

Condition 4 : En utilisant un autre type de transformation du plan on peut se ramener au cas où la courbe ait un *point d'inflexion* en (0,1,0), d'après les équations de f_1 et de f_2 donné par l'équation de la condition 2, on a

$$f_2(x, y) = c_{yww}x^2 + c_{xyw}xy + c_{xxy}y^2$$

et

$$f_1(x, y) = c_{yyw}x,$$

pour que f_1 divise f_2 il faut que

$$c_{xxy} = 0.$$

La condition pour que $(0, 1, 0)$ soit dans l'intersection de w avec C est que w ne divise pas F, d'où

$$c_{xxx} \neq 0.$$

Donc finalement l'équation de la cubique devient

$$F(x, y, w) = c_{yyw}y^2w+c_{xyw}xyw+c_{yww}yw^2+c_{xxx}x^3+c_{xxw}x^2w+c_{xww}xw^2+c_{www}w^3. \tag{16}$$

$$\text{avec } c_{yyw} \neq 0 \text{ et } c_{xxx} \neq 0. \tag{17}$$

Nous pouvons encore faire des réductions en se ramenant au cas où $c_{yyw} = c_{xxx} = 1$, nous le prouverons dans la proposition qui suit.

Proposition 2.1. *Soit K un corps et soit C une cubique définie par le polynôme F sur K telle que C(K) admette un point d'inflexion en (x_0, y_0, w_0), alors il existe une transformation projective ϕ de sorte que l'équation de F^ϕ soit équivalente à l'équation*

$$y^2w + a_1xyw + a_3yw - x^3 - a_2x^2w - a_4xw^2 - a_6w^3 = 0 \tag{18}$$

Démonstration. On peut choisir ϕ_1 telle que $\phi_1(x_0, y_0, w_0) = (0, 1, 0)$, alors F^{ϕ_1} possède un point d'inflexion en $(0, 1, 0)$ (car la transformation projective ϕ_1 préserve les points d'inflexion). Soit $L(x, y, w) = \alpha x + \beta y$ la tangente à F^{ϕ_1} en (0,1,0), choisissons une matrice non-singulière $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $\alpha a + \beta c = 0$, et définissons

$$\phi_2^{-1} = \begin{pmatrix} a & 0 & b \\ 0 & 1 & 0 \\ c & 0 & d \end{pmatrix}.$$

Grâce à ce ϕ_2, L^{ϕ_2} est la même droite que w. Donc $(F_1^{\phi})^{\phi_2} = F^{\phi_2\phi_1}$ admet la droite w comme tangente et le point $(0, 1, 0)$ comme point d'inflexion, d'après les ce qui vient d'être dit plus haut $F^{\phi_2\phi_1}$ a la même équation que (16). En prenant la matrice ϕ^3 dont l'inverse est

$$\phi_3^{-1} = \begin{pmatrix} t & 0 & 0 \\ 0 & t & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

L'équation de $(F^{\phi_2\phi_1})^{\phi_3} = F^{\phi_3\phi_2\phi_1}$ est

$$\begin{aligned} F^{\phi_3\phi_2\phi_1}(x, y, w) =& F^{\phi_2\phi_1}(tx, ty, w) \\ =& c_{yyw}t^2y^2w + c_{xyw}t^2xyw + c_{yww}tyw^2 + c_{xxx}(t^3x^3) \\ &+ c_{xxw}t^2x^2w + c_{xww}txw^2 + c_{www}w^3 \end{aligned}$$

En prenant $t = c_{yyw}/c_{xxx}$ ($c_{xxx} \neq 0$) on voit que y^2w et x^3 ont le même coefficient dans l'équation de $F^{\phi_3\phi_2\phi_1}$ et (puisque $c_{yyw} \neq 0$) en factorisant l'équation par ce coefficient on obtient l'équation (18). Donc la matrice $\phi = \phi_3\phi_2\phi_1$ est la matrice définissant la transformation recherchée.

□

2.2 Courbe elliptique sous forme de Weierstrass

Définition 2.1. *Une* courbe elliptique (E, O) *sur un corps K est dite sous Forme de Weierstrass si et seulement si son équation est de la forme*

$$Y^2w + a_1XYW + a_3YW^2 = X^3 + a_2X^2W + a_4XW^2 + a_6W^3 \quad (a_i \in K) \tag{19}$$

On note car(K) la caractéristique de K.

Proposition 2.2. *Si la caractéristique de K est différente de 2 et de 3, il est toujours possible de travailler avec des courbes elliptiques de la forme :*

$$y^2 = x^3 + ax + b \tag{20}$$

Notation 2.1. *Soient les quantités* $b_2, b_4, b_6, b_8, c_4, c_6$ *définis par :*

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

Et

$$\begin{aligned} c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 - 36b_2b_4 - 216b_6 \end{aligned}$$

b_8 *sera utilisé plus tard dans la suite.*

Démonstration. (de la proposition)

- Si $W = 0$, la solution de l'équation est le point à l'infini O=(0,1,0) qui est non-singulier car $\left(\frac{\partial F}{\partial W}\right)_{(0,1,0)} = 1 \neq 0$.
- Si $W \neq 0$, alors on passe de l'espace projectif à l'espace affine par $(x, y) = (\frac{X}{W}, \frac{Y}{W})$ et l'équation (17) devient :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in K) \tag{21}$$

  et donc on peut travailler dans l'espace affine.
- Si car$(K) \neq 2$, dans (21) on peut faire le changement de variable suivant :
  remplacer y par $\frac{1}{2}(y - a_1x - a_3)$ et l'equation devient :

$$\begin{aligned} (21) \Leftrightarrow 0 = &\frac{1}{4}\left[y^2 + a_1^2x^2 + a_3^2 - 2a_1xy - 2a_3y + 2a_1a_3x\right] + \\ &\frac{1}{2}\left[a_1xy - a_1^2x^2 - a_3a_1x + a_3y - a_1a_3x - a_3^2\right] \\ \Rightarrow &\frac{1}{4}y^2 - \frac{1}{4}a_1^2x^2 - \frac{1}{4}a_3^2 - \frac{1}{2}a_1a_3x = x^3 + a_2x^2 + a_4x + a_6 \\ \Rightarrow &y^2 - a_1x^2 - a_3^2 - 2a_1a_3x = 4x^3 + 4a_2x^2 + 4a_4x + 4a_6 \\ \Rightarrow &y^2 = 4x^3 + x^2(a_1 + 4a_2) + x(2a_1a_3 + 4a_4) + (4a_6 + a_3^2) \end{aligned}$$

  alors la première réduction donne

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \tag{22}$$

avec $b_2,\ b_4$ et b_6 comme dans la Notation 2.1

– Si en plus la caractéristique de K est différente de 3, on remplace (x, y) par $\left(\frac{x-3b_2}{36}, \frac{y}{108}\right)$ on obtient après calcul,

$$y^2 = x^3 - 27c_4x - 54c_6 \tag{23}$$

avec c_4 et c_6 comme dans la Notation 2.1

□

2.3 Discriminant et j-invariant d'une forme de Weierstrass

Nous avons besoin de trois notions pour définir le discriminent :

Définition 2.2. *Soit deux polynôme P et Q de degrés p et q respectivement,*

$$P(x) = a_0 + a_1x + \cdots + a_px^p \text{ et } Q(x) = b_0 + b_1x + \cdots + b_qx^q$$

On appelle Matrice de Sylvester *la matrice $(p+q)$ suivante :*

$$S_{p,q} = \begin{pmatrix}
a_0 & & & 0 & b_0 & & & & 0 \\
a_1 & a_0 & & & b_1 & b_0 & & & \\
\vdots & \ddots & \ddots & & \vdots & \ddots & \ddots & & \\
\vdots & \ddots & \ddots & a_0 & b_{q-1} & \ddots & \ddots & \ddots & \\
a_q & \ddots & \ddots & a_1 & b_q & b_{q-1} & \ddots & & \ddots \\
\vdots & & \ddots & \vdots & & b_q & \ddots & & b_0 \\
a_p & \ddots & & \vdots & & & \ddots & & \vdots \\
 & a_p & & \vdots & & & & \ddots & \vdots \\
 & & \ddots & a_{p-1} & & & & \ddots & \vdots \\
0 & & & a_p & 0 & & & & b_q
\end{pmatrix}$$

Définition 2.3. *On appelle* ***résultant*** *de deux polynômes P et Q le déterminant de la matrice de Sylvester de P et Q, on le note R(P,Q).*

Proposition 2.3. *Soit A un anneau factoriel. Soient F et G dans $A[X]$ tels que,*

$$F(X) = a_0 + a_1X + \cdots + a_mX^m$$
$$G(X) = b_0 + b_1X + \cdots + b_nX^n$$

il y a équivalence entre

1. *F et G ont un facteur commun de degré >0.*
2. *$aF + bG = 0$ pour certain a et b non nuls dans $A[X]$ avec* $\deg(a) < n$ *et* $\deg(b) < m$.
3. *$R(F, G) = 0$.*

Démonstration.
(1) $\Rightarrow$ (2). Si $u|F$ et $u|G$, on écrit $F = bu$ et $G = -au$, cela donne $aF + bG = abu - bau = 0$.
(2) $\Rightarrow$ (1). Supposons que $aF + bG = 0$, alors aF divise bG mais aF ne divise pas b (car $\deg(b) < \deg(F)$, et donc $\deg(\text{pgcd}(F, G)) > 1$ (contraposé de Gauss) et donc F et G ont un facteur en commun.
(2) $\Leftrightarrow$ (3). Dans la matrice résultant de F et G nous avons $m + n - 1$ lignes, appelons L_i la i-ème ligne. En ajoutant à L_0 chaque ligne L_i multipliée par X^i $(i > 0)$ le résultant $R(F, G)$ ne change pas, et L_0 devient

$$(F(X) \;\; XF(X) \;\; \cdots \;\; X^{n-1}F(X) \;\; G(X) \;\; XG(X) \;\; X^{p-1}G(X))$$

On calcule le determinant en dévéloppant par rapport à L_0 et on obtient

$$R(F(X), G(X)) = a(X)F(X) + b(X)G(X)$$
$$\text{où } a, b \in A[X] \text{ avec } \deg(a) \leq \deg(F), \;\; \deg(b) \leq \deg(G).$$

□

Définition 2.4. *Le **discriminant** d'un polynôme de degré n et de coefficient dominant a est donné par la formule*

$$\Delta(P) = \frac{(-1)^{\frac{n(n-1)}{2}}}{a} R(P, P'). \tag{24}$$

Revenons à notre sujet et cherchons le discriminant de l'équation (23) qu'on note pour la suite Δ tout simplement,

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

en appliquant la formule (24) on obtient

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \tag{25}$$
$$= a_1^6a_6 + a_1^5a_3a_4 + a_1^4a_2a_3^2 + a_1^4a_4^2 + a_3^4 + a_1^3a_3^3. \tag{26}$$

pour b_2, b_4, b_6, b_8 comme dans la Notation 2.1.

Remarque. Dans le cas où $a_1 = a_3 = a_2 = 0$, le discriminant se simplifie en

$$\Delta = -2^4(27a_6^2 + 4a_4^3).$$

Proposition 2.4. *Soit K un corps de caracteristique différente de 2. Alors la courbe plane d'équation*

$$y^2 = x^3 - \alpha x^2 + \beta x - \gamma \tag{27}$$

est non-singulière si et seulement si $f(x) = x^3 - \alpha x^2 + \beta x - \gamma$ a toutes ses racines distinctes dans $\overline{K}$.

Démonstration. Notons que d'après le paragraphe 2.1 on peut avoir non-singularité sur la droite à l'infini. La courbe C définie par l'équation (27) est non-singulière si et seulement si (27) vérifie les conditions du deuxième point de la définition 1.6 : tout point $(x_0, y_0, 1)$ de C n'est pas singulier. On va montrer que C admet un point singulier $(x_0, y_0, 1)$ si et seulement si $(x_0, y_0, 1)$ est une racine multiple de f. Supposons que $(x_0, y_0, 1)$ est un point singulier, il vérifie alors les équations suivantes

$$3x_0^2 - 2\alpha x_0 + \beta = 0 \tag{28}$$

$$2y_0 = 0 \tag{29}$$

$$y_0^2 = -\alpha x_0^2 + 2\beta x_0 - 3\gamma \tag{30}$$

L'équation (28) donne que $f'(x_0)$=0, les équation (29) et(30) donnent que $0 = y_0 = y_0^2 = f(x_0)$ donc $f(x_0) = f'(x_0) = 0$. Les seuls points singuliers sur $\overline{K}$ sont $(x_0, 0, 1)$ où x_0 est une racine de f, un tel point est singulier si et seulement si x_0 est racine multiple de f. □

Proposition 2.5. *Une courbe d'équation*

$$y^2w + a_1xyw + a_3yw^2 = x^3 + a_2x^2w + a_4xw^2 + a_6w^3 \tag{31}$$

est non-singulière si et seulement si $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \neq 0$ (courbe sous forme de Weierstrass cf. définition 2.1).

Démonstration.
- Si $\mathrm{car}(K) \neq 2$ alors l'équation (31) est singulière si et seulement si l'équation (22) l'est, si et seulement si la partie droite de l'équation (22) a une racine multiple (par la Proposition 2.4) si et seulement si le discriminant de cette même partie est nul si et seulement si $\Delta = 0$.
- Si $\mathrm{car}(K) = 2$ l'équation (31) peut avoir des points singuliers seulement dans le cas des points $\overline{K}$ rationnels $(x_0, y_0, 1)$ sur la courbe, un tel point est singulier si et seulement si

$$0 = a_1y_0 + x_0^2 + a_4 \tag{32}$$

$$0 = a_1x_0 + a_3 \tag{33}$$

$$0 = y_0^2 + a_1x_0y_0 + a_2x_0^2 + a_6 \tag{34}$$

L'équation (34) est redondante étant la somme de x_0(32) et de y_0(33).

1. Supposons que $a_1 = 0$, alors $\Delta = 0$ si et seulement si $a_3 = 0$ (d'après l'équation (26)) donc l'équation (33) est vérifiée, reste à montrer que l'équation (32) l'est également.
   cela revient à trouver une solution dans $\overline{K}$ pour le système

$$y_0^2 = x_0^3 + a_2x_0^2 + a_4x_0 + a_6 \tag{35}$$
$$0 = x_0^2 + a_4 \tag{36}$$

   ((36) est en fait (32) pour $a_1 = 0$, (35) est (21) pour $a_1 = a_3 = 0$) il suffit pour cela de prendre un x_0 dans $\overline{K}$ verifiant (36), l'insérer dans (35) et choisir un y_0 dans $\overline{K}$ verifiant alors (33).

2. Si $a_1 \neq 0$, dans ce cas

   (33) donne $x_0 = a_1^{-1}a_3$ et alors (32) donne $y_0 = a_1^{-3}a_3^2 + a_1^{-1}a_4$

   On remplace dans (21) et on obtient

$$(a_1^{-6}a_3^4 + a_1^{-2}a_4^2) + (a_1^{-3}a_3^3 + a_1^{-1}a_3a_4) + (a_1^{-3}a_3^3 + a_1^{-1}a_3a_4)$$
$$+a_1^{-3}a_3^3 + a_1^{-2}a_2a_3^2 + a_1^{-1}a_3a_4 + a_6$$

   et cela est égale à $a_1^{-6}\Delta$ et donc (x_0, y_0) satisfait (21), et par suite $(x_0, y_0, 1)$ est un point singulier si et seulement si $\Delta = 0$.

□

Remarque. Nous donnons une démonstration directe de cette proposition. En définissant de manière plus générale la notion de multiplicité d'intersection de deux courbes, on pourrait la déduire du théorème de Bezout.

Définition 2.5. *Le* j-invariant *d'une courbe élliptique est définie par*

$$j = c_4^3/\Delta.$$

3 Loi de Groupe

Dans cette partie nous adésignons par K un corps et $\overline{K}$ une extension algébrique de K.

3.1 Théoreme de Bezout et règle de la sécante-tangente

Proposition 3.1. *Si $A = K[x_1, \cdots, x_r]$, soient f et g des polynômes de $A[X]$ de degré respectifs m et n,*

$$f(X) = a_0 + a_1X + \cdots + a_mX^m$$
$$g(X) = b_0 + b_1X + \cdots + b_nX^n$$

avec a_j homogène de degré $m - j$, et b_j homogène de degré n-j, alors le résultant $R(f, g)$ est homogène de degré mn.

Démonstration. $R(f, g)(tX) = R(f(tX), g(tX))=$

$$\det \begin{pmatrix}
a_0 & & & 0 & b_0 & & & & 0 \\
a_1t & a_0 & & & b_1t & b_0 & & & \\
\vdots & a_1t & \ddots & & \vdots & \ddots & \ddots & & \\
\vdots & \ddots & \ddots & a_0 & b_{n-1}t^{n-1} & \ddots & \ddots & \ddots & \\
a_nt^n & \ddots & \ddots & a_1t & b_nt^n & b_{n-1}^{n-1} & \ddots & \ddots & \\
\vdots & & \ddots & \vdots & & b_n & \ddots & & b_0 \\
a_mt^m & \ddots & & \vdots & & & \ddots & & b_1t \\
 & a_mt^m & & \vdots & & & & \ddots & \vdots \\
 & & \ddots & a_{m-1}t^{m-1} & & & & \ddots & \vdots \\
0 & & & a_mt^m & 0 & & & & b_n^n
\end{pmatrix}$$

Pour $i \in [1, n]$ multiplions la $i-$ème colonne par t^{i-1} et pour $j \in [1, m]$ multiplions la $(n + j)-$ème colonne par t^{j-1}, nous obtenons :

$$\begin{pmatrix}
a_0 & & & 0 & b_0 & & & & 0 \\
a_1t & a_0t & & & b_1t & b_0t & & & \\
a_2t^2 & a_1t^2 & \ddots & & \vdots & b_1t^2 & \ddots & & \\
\vdots & \ddots & \ddots & a_0t^{n-1} & \vdots & \ddots & \ddots & \ddots & \\
a_nt^n & \ddots & \ddots & a_1t^n & b_nt^n & b_{n-1}t^n & \ddots & \ddots & \\
\vdots & & \ddots & \vdots & & b_nt^{n+1} & \ddots & & b_0t^{m-1} \\
a_mt^m & \ddots & & \vdots & & & \ddots & & b_1t^m \\
 & a_mt^{m+1} & & \vdots & & & & \ddots & \vdots \\
 & & \ddots & a_{m-1}t^{m+n-2} & & & & \ddots & \vdots \\
0 & & & a_mt^{m+n-1} & 0 & & & & b_nt^{n+m-1}
\end{pmatrix}$$

$$= t^u R(f(tX), g(tX))$$

$$= t^v R(f(X), g(X))$$

-la première égalité est obtenue en factorisant des colonnes, ie pour $i \in [2, n]$, on a multiplié la i-ème colonne par t^{i-1}, et pour $j \in [n+2, n+m]$, on a multiplié la j-ème colonne par t^{j-1}, et donc

$$u = 1 + 2 + \cdots + (m-1) + 1 + 2 + \cdots + (n-1) = \frac{m(m-1)}{2} + \frac{n(n-1)}{2}$$

-la deuxième égalité est obtenue en mettant t^i en facteur dans la $(i+1)$-ème ligne pour $i \geq 2$, il y a $(m+n-1)$ lignes à factoriser, donc

$$v = 1 + 2 + \cdots + (m+n-1) = \frac{(m+n)(m+n-1)}{2}$$

En remarquant que $v - u = mn$ on en déduit que

$$R(f(tX), g(tX)) = t^{v-u} R(f(X), g(X)) = t^{mn} R(f(X), g(X))$$

□

Théorème 3.1. *(de Bezout) Soient C et E des courbes projectives planes définies par $F \in K[x, y, w]_m$ et $G \in K[x, y, w]_n$. Alors*

1. *$C(\bar{K}) \cap E(\bar{K})$ est non vide.*
2. *Si $C(\bar{K}) \cap E(\bar{K})$ contient plus que mn points comptés avec leur multiplicité, alors F et G ont comme facteur commun un polynôme homogène de degré >0.*

Démonstration. Dans notre sujet nous avons besoin surtout de la deuxieme partie du théorème.
2. Supposons que $C(\overline{K})\cap E(\overline{K})$ contient au moins $mn+1$ points. Joignons ces points par des droites et prenons un point P définit sur $\overline{K}$ qui n'appartient à aucune de ces droites (existe car $\overline{K}$ est infini et le nombre des droites est fini). Grâce à une transformation projective nous pouvons considérer que ce point est $P=(0,0,1)$, et regardons F et G comme des polynôme en w,

$$F(x,y,w) = a_0 + a_1 w + \cdots + a_m w^m \quad avec \quad a_j \in \overline{K}[x,y]_{m-j}$$
$$G(x,y,w) = b_0 + b_1 w + \cdots + b_n w^n \quad avec \quad a_j \in \overline{K}[x,y]_{n-j}$$

on calcule $R(F,G)$ par rapport à w qui, d'après la proposition 3.1, est un polynôme de degré mn dans $\overline{K}[x,y]$ (ie $R(F,G)\in\overline{K}[x,y]_{mn}$). Pour (x_0,y_0) fixé, d'après la proposition 2.3 on a $R(F,G)(x_0,y_0)=0$ si et seulement si $F(x_0,y_0,w)$ et $G(x_0,y_0,w)$ ont un facteur commun (c'est nécessairement $w-w_0$ pour un certain w_0 car $\overline{K}$ est algébriquement clos) si et seulement si $F(x_0,y_0,w_0)=G(x_0,y_0,w_0)=0$.

On choisit une famille $\Im=((x_i,y_i,w_i))_{1\leq i\leq mn+1}$ de $mn+1$ points distincts parmi les points d'intersection de F avec G, on a alors $R(F,G)(cx_i,cy_i)=0$ pour tout c. Le polynôme $y_ix-x_iy=0$ divise alors $R(F,G)(x,y)$, (en fait la multiplicité d'intersection est la puissance de (y_ix-x_iy) divisant le résultant).

Supposons qu'il existe deux points (x_i,y_i) et (x_i,y_i) de la famille $\Im$ différents tels que $(x_i,y_i)=\lambda(x_j,y_j)$, les points (x_i,y_i,w_i) et (x_j,y_j,w_j) satisfont tout les deux l'équation $y_ix-x_iy=0$, mais $P=(0,0,1)$ satisfait aussi cette équation, donc P est aussi sur la droite reliant ces deux point, cela contredit le fait que P n'appartient à aucune droite reliant deux points parmi les $mn+1$ points d'intersection.
Alors les $mn+1$ facteurs de $y_ix-x_iy=0$ sont premiers entre eux deux à deux dans $\overline{K}[x,y]$, et par l'unicité de la factorisation leur produit divise $R(F,G)$. Mais $\deg(R(F,G))=mn$, on en déduit que $R(F,G)=0$. et par la proposition 2.3 nous savons que F et G ont un facteur en commun dans $\overline{K}[x,y][w]=\overline{K}[x,y,w]$. Par le lemme 3.1 suivant, puisque ce facteur divise F (homogène), il est homogène. □

Lemme 3.1. *En utilisant les mêmes notations que dans le théorème, si F est homogène de degré d, et si G de degré $K\leq d$ est un polynôme divisant F, alors G est homogène.*

Démonstration. Ecrivons $F=GM$, F est par définition une somme de monômes de degré d, supposons que G n'est pas homogène, alors il possède des monômes de degrés différents, soit d_1 le plus petit des degrés et d_2 le plus

grand. De même pour M, soit e_1 le plus petit des degrés des monôme de M et e_2 le plus grand. Le produit des monômes de degré d_1 de G avec ceux de degré e_1 de M donne un monôme de degré d_1e_1 qui est le plus bas des degré des monômes du polynôme produit (donc de F). de même le plus grand des degrés des monômes du polynôme produit (donc de F) est d_2e_2. Alors $d_1e_1 = d_2e_2$ car F est homogène, cela donne forcément $d_1 = d_2$ et $e_1 = e_2$, autrement dit G est homogène. □

Proposition 3.2. *(de Bezout) Si C est une courbe plane définie par $F \in K[x, y, w]_d$ et L une droite définie par un polynôme $D \in K[x, y, w]_1$telle que $\sum_p i(p, L, C) > d$,alors D divise F.*

Démonstration. Sans perte de généralité nous pouvons supposer que K est un corps algébriquement clos, en particulier K est infini. Supposons par l'absurde que D ne divise pas F donc D et F n'ont aucun facteur non constant en commun, donc admet un nombre fini de points communs, ce qui signifie que $\sum_{p\in L} i(p, L, C)$ est fini. Par une transformation projective nous pouvons supposer que L est la droite a l'infini $w = 0$. Alors les points P_i de l'intersection entre L et C sont de la forme $(x_i, y_i, 0)$. En appliquant une autre transformation projective, une translation de y, nous pouvons supposer que tout les points d'intersection ont la coordonnée en y non nulle. Alors on peut écrire $P_i = (r_i, 1, 0)$ avec $r_i \in K$ les points d'intersection de $F(x, 1, 0)$ avec $L : w = 0$. Ainsi $F(x, 1, 0)$ est un polynôme en x ayant au plus d racines comptées avec leur miltiplicité, par conséquent $\sum_{p\in L} i(p, L, C) \leq d$, contradiction avec l'hypothèse. □

Remarque 3.1. *Nous donnons une démonstration directe de cette proposition. En définissant de manière plus générale la notion de multiplicité d'intersection de deux courbes, on pourrait la déduire du théorème de Bezout.*

Proposition 3.3. (Règle de la Sécante-tangente) : *Si C est une cubique non-singulière et L une droite. Si C a deux points d'intersection (comptés avec leur multiplicité) avec L, alors C a 3 points d'intersection (comptés avec leur multiplicité) avec L.*

Démonstration. C est non-singulière, donc le polynôme F définissant C est irréductible, donc F et D n'ont pas de facteurs commun donc (d'apres le point 2 du théoreme 3.1 de Bezout) $C \cap L$ admet un nombre fini de points. Soit la droite $L : ax + by + cw = 0$ où, par symétrie, nous pouvons supposer que $c \neq 0$. Les points d'intersection de C et de L sont les racines du polynôme

$$q(x, y) = p(x, y, -\frac{ax + by}{c}) \in K[x, y]_3$$

Soient $P_1 = (x_1, y_1, w_1)$ et $P_2 = (x_2, y_2, w_2)$ deux points d'intersection de C avec L, alors $q(x_1, y_1)$=$q(x_2, y_2) = 0$, il vient que

$$q(x, y) = v(x, y)(y_1x - x_1y)(y_2x - x_2y) \quad \text{où } v(x, y) \in K[x, y]_1$$

le troisième point d'intersection de C avec L est alors donné par

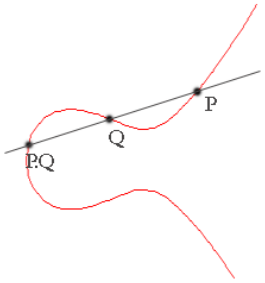
$$P_3 = (x_3, y_3, -\frac{xx_3 + yy_3}{c})$$

où (x_3, y_3) est l'unique racine de $v(x, y)$. □

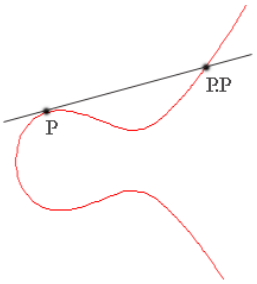
3.2 Construction de la loi

Soient K un corps et E une courbe elliptique sur K, soient deux points P et Q de $E(K)$, et soit L la droite passant par P et Q, par la proposition précédente nous savons qu'il existe un troisième point appartenant à $E(k) \cap L(k)$ (en comptant les multiplicités).

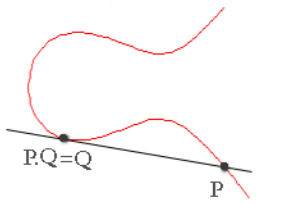
1. Si $P \neq Q$, on notera $P.Q$ le troisieme point.



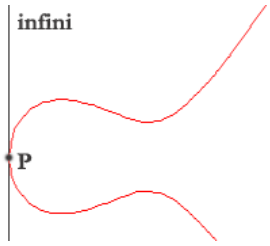
2. Si $P = Q$, alors $P.Q$ est l'intersection de la tangente en P à la courbe C, au lieu de $P.Q$ on le notera $P.P$.



3. Si la droite passant par P et Q est tangente à E en Q alors $P.Q = Q$.



4. Si la droite passant par P est verticale (tangente en P et verticale), le troisième point est le point à l'infini.



Pour une courbe elliptique (E, O) on définit

$$\forall (P, Q) \in E(k)^2 \quad P + Q = O.(P.Q)$$

Cela signifie que $P + Q$ est le troisième point d'intersection entre E et la droite passant par $P.Q$ et O.

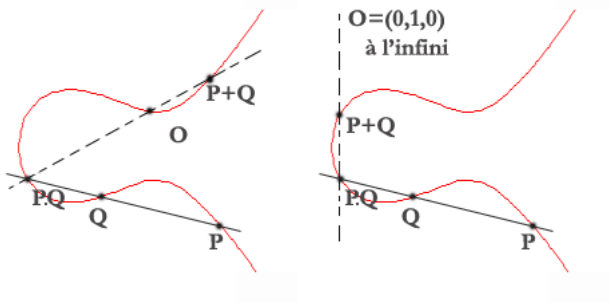


FIGURE 5 – Loi du Groupe pour différents points O.

Dans la suite nous allons démontrer que cette construction forme un groupe abélien (théoreme de Poincaré).

3.3 Théorème de Poincaré

Théorème 3.2. *(Poincaré) 1.Soit K un corps et soit C une cubique non-singulière et soit $O \in C(K)$, alors l'opération $P + Q = O.(P.Q)$ définit une structure de groupe abélien avec O comme élément neutre et $P' = (O.O).P$ comme élément opposé.*
2.Notons $\overline{K}$ une extension du corps K, alors l'application $F(K) \longrightarrow F(\overline{K})$ est un homomorphisme de groupe. Si un point différent O' a été choisit alors deux opérations sont liées par $P +' Q = P + Q - O'$ et les structures de groupe sont isomorphes.

Démonstration.

- **Commutativité :** Cette construction ne dépend pas de l'ordre de P et Q, donc $P + Q = Q + P$.
- **Elément neutre :** $P + O = O.(P.O) = P$, O est l'élément neutre.
- **Opposé :** On fixe un point P et un point O, on appelle $P' = P.(O.O)$ (i.e si la tangente en O passe par R $(= O.O)$ alors on appelle P' le troisieme point d'intersection de C avec de la droite passant par P et R), alors $P.P' = O.O$ et alors

$$P + P' = O.(P.P') = O.(O.O) = O + O = O$$

(Le graphe explique bien ce qui vient d'être dit dans le point (3))

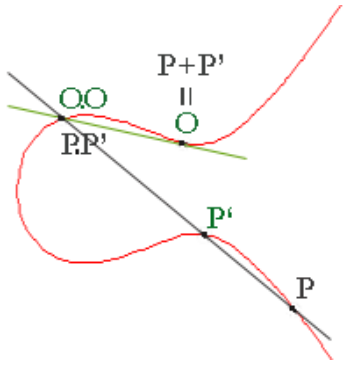


FIGURE 6 – Calcul de l'inverse de P.

Nous allons noter $-P$ l'opposé au lieu de P' dans la suite.

- **Associativité :** L'associativité est le point le plus difficile a démontrer, avant de la démontrer nous avons besoin d'énoncer un lemme..

Lemme 3.2. *Soit K un corps comlutatif et C une cubique sur K. Pour tout P, Q, P', Q' dans $C(K)$,*

$$(P.P').(Q.Q') = (P.Q).(P'.Q').$$

Avant de donner une preuve, regardons comment ce lemme implique le théorème de Poincaré. En fait, il suffit de faire le calcul,
on a

$$P + (Q + R) = O.(P.(Q + R)) \text{ et } (P + Q) + R = O.((P + Q)R)$$

et donc il suffit de prouver que $P(Q + R) = (P + Q)R$,

$$\begin{aligned}
\text{Or } P.(Q + R) &= P.(O.(Q.R)) \\
&= ((P.Q).Q).(O.(Q.R)) \text{ car P=((P.Q).Q)} \\
&= ((P.Q).O).(Q.(Q.R)) \text{ par le lemme 3.2} \\
&= ((P.Q).O).R \text{ car (Q.(Q.R))=R} \\
&= (O.(P.Q)).R \\
&= (P + Q).R
\end{aligned}$$

on a obtenu ce qu'on cherchait, et finalement $P + (Q + R) = (P + Q) + R$.
et donc nous avons démontré l'associativité !

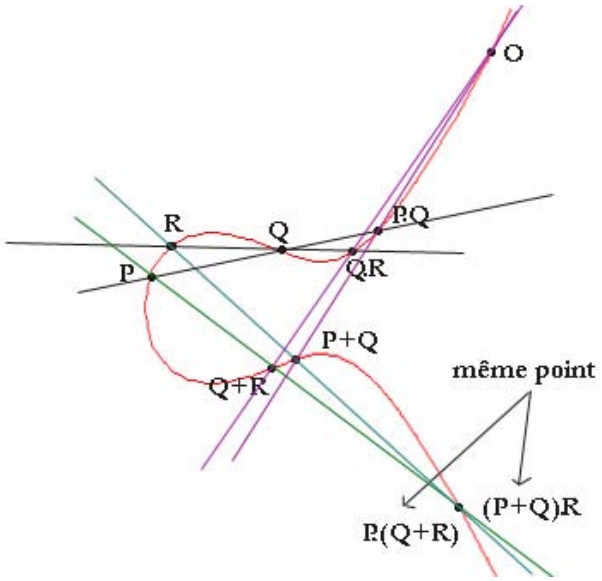


FIGURE 7 – Associativite P+(Q+R)=(P+Q)R.

2. Or $F(K)$ est un groupe abélien pour la loi + alors on a clairement que $F(K) \subset F(\overline{K})$, lapplication $F(K) \to F(\overline{K})$est un morphisme de groupe. Soit O un point donné, on a

$$\begin{aligned}(P+Q)-O' &= O[(O.(P.Q)).((O.O).O')] \\ &= O[(O.(O.O)).((P.Q).O')] \text{ (par le lemme 3.2)} \\ &= O[O.(P+'Q)] = P+'Q\end{aligned}$$

Soit l'application bijective

$$\begin{aligned}\varphi : (F(K),+) &\longrightarrow (F(K),+') \\ P &\longrightarrow P-O'\end{aligned}$$

alors,

$$\begin{aligned}\varphi(P+Q) &= (P+Q)-O' = P+'Q \\ &= \varphi(P)+'\varphi(Q).\end{aligned}$$

φ est donc un isomorphise.

□

Reste à prouver le Lemme 3.2.

Démonstration. (du lemme 3.2) Il va falloir distinguer le cas dégénéré du cas non-dégénéré, la distinction entre ces deux cas revient à regarder si deux des huit points ci-dessous sont égaux

$$P, P', Q, Q', P.Q, P'.Q', P.P', Q.Q'$$

mettons ces points dans une matrice 3×3

$$\begin{pmatrix} P & P' & P.P' \\ Q & Q' & Q.Q' \\ P.Q & P'.Q' & \end{pmatrix} \tag{37}$$

On dit qu'on est dans le cas non-dégénéré si aucun éléments de la matrice est égal à un élément qui n'appartient pas à sa ligne ni à sa colonne, (par exemple P ne doit pas être égale à $Q', Q.Q', P'.Q'$). Dans le cas contraire nous dirons que nous somme dans le cas dégénéré.

Preuve dans le cas non dégénéré :
Soient L'_1, L'_2, L'_3 les droites qui rencontrent la cubique C en les points respectifs des lignes de la matrice précédante, avec la convention que si un point apparaît deux fois dans une ligne alors la droite est tangente à la courbe en ce point.
Soient L''_1, L''_2, L''_3 les droites déterminées par les colonnes de la matrice.

Dans la preuve, nous désignons par F le polynôme définissant la cubique C, d_i celui définissant la droite L_i, d'_i celui définissant la droite L'_i et d''_i celui définissant la droite L''_i.

Pour le moment la dernière case de la matrice est vide, si on regarde par les ligne on pense que cette case contient $(P.Q).(P'.Q')$, et si on regarde du côté colonne on voit que cette case doit contenir $(P.P').(Q.Q')$. nous allons démontrer que ces deux valeurs sont égales. Puisque nous sommes dans le cas non-dégénéré nous avons forcément $L'_i \neq L''_j$, cela implique que ces deux droites se coupent seulement en le (i, j)-ème point de la matrice sauf pour $i = j = 3$.

Dans la preuve nous devons supposer que K est un corps algébriquement clos (nous allons utiliser le fait qu'il est infini).
Soient d' et d'' telles que

$$d' = d'_1 d'_2 d'_3 \text{ et } d'' = d''_1 d''_2 d''_3 \tag{38}$$

Soient C' et C'' les courbes corréspondantes à d' et d''. Soit un point $R' \in L'_1(K)$ autre que P, P', PP' (existe car K est infini) et soit R'' un point qui n'appartient pas à $C'(K)$ on choisit a, a', a'' non tous nuls tels que

$$\begin{cases} aF(R') + a'd'(R') + a''d''(R') & = 0 \\ aF(R'') + a'd'(R'') + a''d''(R'') & = 0 \end{cases} \tag{39}$$

Montrons que

$$F_0 = aF + a'd' + a''d'' = 0 \tag{40}$$

Nous allons utiliser les deux remarques suivantes :

1. Soient L une droite, p un point, C_1 et C_2 deux courbes planes définies respectivement par les polynômes G_1 et G_2, alors on a

$$i(p, L, G_1G_2) = i(p, L, G_1) + i(p, L, G_2). \tag{41}$$

2. Si en plus G_1 et G_2 sont du même degré et si $G_1 + G_2 \neq 0$, alors

$$i(p, L, G_1 + G_2) \geq \min\{i(p, L, G_1), i(p, L, G_2)\}. \tag{42}$$

Ces deux remarques sortent directement de la définition.

Supposons maintenant que $F_0 \neq 0$ et appelons C_0 la courbe définie par F_0, C_0 est donc une cubique.

Opérations sur la première ligne :
Soit p_{1t} un élément de la premiere ligne, à savoir L'_1, de la matrice avec $t \in [1, 3]$.

$$\begin{aligned} i(p_{1t}, L'_1, C''') &= i(p_{1t}, L'_1, d''_1d''_2d''_3) \\ &= i(p_{1t}, L'_1, L''_1) + i(p_{1t}, L'_1, L''_2) + i(p_{1t}, L'_1, L''_3) \text{ (par la remarque 1)} \\ &\geq 1. \\ i(p_{1t}, L'_1, C_0) &= i(p_{1t}, L'_1, aF + a'd' + a''d'') \\ &\geq \min\{i(p_{1t}, L'_1, C_F), i(p_{1t}, L'_1, d'), i(p_{1t}, L'_1, d'')\} \text{ (par la remarque 2)} \\ &\geq 1. \end{aligned}$$

par (39) $R' \in C_0$, mais $R' \in L'_1$ donc $i(R', L'_1, C_0) \geq 1$ donc

$$i(p_{11}, L'_1, C_0) + i(p_{12}, L'_1, C_0) + i(p_{13}, L'_1, C_0) + i(R', L'_1, C_0) \geq 4.$$

finalement $\sum_{p \in L'_1} i(p, L'_1, C_0) \geq 4 \geq 3 \times 1$ et donc par la proposition 3.2 d'_1 divise F_0, on en déduit que

$$F_0 = Md'_1.$$

où M est un polynôme de degré 3 représentant une conique C_M.

Opérations sur la deuxième ligne :
Soit p_{2t} une élément de la deuxième ligne de la matrice

$$\begin{aligned} i(p_{2t}, L'_2, C_0) &= i(p_{1t}, L'_2, aF + a'd' + a''d'') \\ &\geq \min\{i(p_{2t}, L'_2, C_F), i(p_{2t}, L'_2, C'), i(p_{2t}, L'_2, C''')\} \\ &\geq 1. \end{aligned}$$

D'autre part, par la remarque 1 nous pouvons écrire

$$\begin{aligned} i(p_{2t}, L'_2, C_0) &= i(p_{2t}, L'_2, Md'_1) \\ &= i(p_{2t}, L'_2, C_M) + i(p_{2t}, L'_2, L'_1) \\ &\geq 1. \end{aligned}$$

- Si $p_{2t} \notin L'_1$ alors $i(p_{2t}, L'_2, L'_1) = 0$ et par suite $i(p_{2t}, L'_2, C_M) \geq 1$.
- Si $p_{2t} \in L'_1$, il existe j tel que $p_{2t} = p_{1j}$ et donc $p_{2t} \in L''_j$. $L'_2 \cap L''_j = p_{2t}$ (un seul point commun car nous sommes dans le cas non-dégénéré) et par conséquent $j = t$ mais nous avons que $p_{2t} = p_{1j}$, cela signifie que $p_{2j} = p_{1j}$ et alors le point p_{2t} apparaît deux fois dans la colonne L''_j et puisque $d'' = d''_1 d''_2 d''_3$ alors $i(p_{2j}, L''_j, L'') \geq 2$ et par suite

$$\begin{aligned} i(p_{2t}, L''_j, F_0) &\geq min\{i(p_{2t}, L''_j, C_F), i(p_{2t}, L''_j, d'), i(p_{2t}, L''_j, d'')\} \\ &\geq 2. \\ &\Rightarrow i(p_{2t}, L''_j, F_0) = i(p_{2t}, L''_j, C_M) + i(p_{2t}, L''_j, L_1) \geq 2 \\ &\Rightarrow i(p_{2t}, L''_j, C_M) \geq 1 \text{ (car } i(p_{2t}, L''_j, L'_1) = 1 \text{ (cas non-dégénéré))} \\ &\Rightarrow p_{2t} \in C_M \\ &\Rightarrow i(p_{2t}, L'_2, C_M) \geq 1 \end{aligned}$$

Cela marche pour tout t$\in [1, 3]$ et alors $\sum_{p \in L_2} i(p, L'_2, C_M) \geq 3$, par suite (par la proposition 3.2) $M = Td'_2$ où T est un polynôme définissant une droite D.
On peut alors écrire

$$F_0 = Td'_1 d'_2.$$

où T est un polynôme de degré 1.

Opérations sur la troisième ligne :
Dans la troisième ligne il y a deux éléments $P.Q$ et $P'.Q'$.

1. Supposons que $P.Q = P'.Q'$, et notons p le point commun. Or nous somme dans le cas non-dégénéré cela implique que $i(p, L'_3, L'_1) = i(p, L'_3, L'_2) = 0$. Or $d' = d'_1 d'_2 d'_3$ alors $i(p, L'_3, C') = +\infty$ (car d'_3 divise d'), et $i(p, L'_3, C_F) \geq 2$ car $P.Q = P'.Q' \in C$, on a alors,

$$i(p, L'_3, C_0) \geq \min\{i(p, L'_3, C_F), i(p, L'_3, C'), i(p, L'_3, C'')\} \geq 2.$$

et alors,

$$i(p, L'_3, C_0) = i(p, L'_3, D) + i(p, L'_3, L'_2) + i(p, L'_3, L'_1) \geq 2,$$

et donc $i(p, L'_3, D) \geq 2$, et alors d'_3 divise T (par la proposition 3.2), ie $T = cd'_3$ où c est une constante non nulle.

2. Supposons maintenant que $P.Q \neq P'.Q'$ et soit p l'élément de la troisième ligne appartenant à la $j-$ème colonne, si p apparaît n fois dans cette colonne alors

$$i(p, L''_j, C_0) \geq n$$

on voit directement (ou par la remarque 2) que

$$i(p, L''_j, d_1 d_2) = n - 1,$$

et puisqu'on a (par la remarque 2)

$$i(p, L''_j, C_0) = i(p, L''_j, D) + i(p, L''_j, d_1 d_2)$$

cela implique $i(p, L''_j, D) \geq 1$ cela signifie que $p \in D$.
de même on démontre que l'autre point de la troisième ligne est sur D, on voit que L'_3 et D ont 2 points distincts en commun , alors d'_3 divise T, ie $T = cd'_3$ où c est une constante non nulle.

Alors dans tout les cas $T = cd'_3$ et on conclut que,

$$F_0 = cd'_1 d'_2 d'_3 = cd'.$$

Mais $F_0(R'') = 0$ et $d'(R'') \neq 0$, cela est une contradiction avec le fait que c soit non nulle, alors $F_0 = 0$ et cela démontre la relation (40).

Reste à prouver que dans (40) $a \neq 0$.
Démontrons le par l'absurde, supposons que $a = 0$, alors on a $a' \neq 0$ ou $a'' \neq 0$, nous pouvons supposer par symétrie que $a' \neq 0$, alors d' divise d'', ainsi d'_1 divise $d''_1 d''_2 d''_3$ et par unicité de la factorisation L'_1 est l'une des L''_j ce

qui contredit le fait qu'on soit dans le cas non-dégénéré. On en déduit que $a \neq 0$, alors on peut diviser (40) par a, d'où

$$F = c'd' + c''d'' \tag{43}$$

Soit N le point d'intersection de L'_3 et de L''_3. Cela donne $d'(N) = d''(N) = 0$ et par suite $F(N) = 0$, on en déduit que $N \in C_F(K) \cap L'_3(K)$ alors N est $(P.Q)$ ou $(P'.Q')$ ou $(P.Q).(P'.Q')$, mais $N \in C_F(K) \cap L''_3(K)$ aussi alors N est PP' ou $Q.Q'$ ou $(P.P').(Q.Q')$.
Or nous sommes dans le cas non-dégénéré alors les deux points du premier cas sont différents des deux points du deuxième cas, on en déduit que,

$$(P.Q).(P'.Q') = N = (P.P').(Q.Q') \tag{44}$$

Mais aussi nous avons les cas :

$$P.Q = N = (P.P').(Q.Q') \tag{45}$$
$$P'.Q' = N = (P.P').(Q.Q') \tag{46}$$
$$P.P' = N = (P.Q).(P'.Q') \tag{47}$$
$$Q.Q' = N = (P.Q).(P'.Q'). \tag{48}$$

Les quatres dernières équations sont symétriques et il suffit d'étudier la première.

Supposons que l'équation (45) est vérifiée.
Soit p_{33} le point $(P.Q).(P'.Q')$, p_{33} appartient à L'_3 donc à C'. p_{33} est aussi sur C. Puisque $c'' \neq 0$ dans (43) (car sinon F serait égale à $cd'_1d'_2d'_3$, or C est non-singulière), donc d'après l'équation (43) p_{33} doit être sur C'', c'est à dire sur au moins une des L''_1, L''_2, L''_3.

1. Si $p_{33} \in L''_1$. Puisque $p_{33} \in L'_3$ on doit forcément avoir

   $$p_{33} = P.Q. \tag{49}$$

   En combinant ce résultat à celui de (45) on obtient (44) et on termine la démonstration.

2. Si $p_{33} \in L''_2$. Puisque $p_{33} \in L'_3$ on doit forcément avoir

   $$p_{33} = P'.Q'. \tag{50}$$

   -Si $P.Q = P'.Q'$ on combine ce résultat avec (45) et on obtient (44), et la démonstration se termine.
   -Si $P.Q \neq P'.Q'$, par (50)

   $$i(P'.Q', L'_3, C_F) = 2.$$

(P.Q) est sur L''_3 par (45), mais (P.Q) est sur L''_1, (on sait aussi que $(P.Q)$ est sur L'_3) cela donne

$$i(P.Q, L'_3, C'') = i(P.Q, L'_3, L''_1) + i(P.Q, L'_3, L''_2) + i(P.Q, L'_3, L''_3) \geq 2,$$

donc

$$\sum_{p \in L'_3} i(p, L'_3, C) \geq 4,$$

donc d'_3 divise F, ce qui contredit la non-singularité de C_F.

3. On en déduit alors que p_{33} est sur L''_3, mais $p_{33} \in L'_3$, et puisque nous sommes dans la cas non-dégénéré (un seul point commun pour chaque ligne et colonne) on en déduit que $p_{33} = N$. Mais dans (45) $P.Q = N$ donc $p_{33} = P.Q$ et alors $p_{33} = (P.P').(Q.Q')$, cela est exactement (44). Fin de la démonstration pour le cas non-dégénéré.

Preuve dans le cas dégénéré : Dans ce cas on suppose que une ligne L'_i et une colonne L''_j ont deux points en commun, ces deux droites sont alors égales. Par symétrie, les seuls cas qu'on doit étudier sont

$$\begin{aligned} P &= Q' \\ P &= Q.Q' \text{ (et donc } P.Q = Q') \\ P.P' &= P.Q \text{ (et donc } P' = Q) \end{aligned}$$

La relation du Lemme 3.2 (on rappelle $(P.P').(Q.Q') = (P.Q).(P'.Q')$) devient

$$\begin{aligned} (P.P').(Q.P) &= (P.Q).(P'.P) \\ (P.P').P &= Q'.(P'.Q') \\ (P.Q).(Q'.Q') &= (P.Q).(Q.Q') \end{aligned}$$

La première est la troisième sont trivialement vraie, la deuxième est aussi vraie car les deux côtés valent P'.

□

3.4 Expression explicite de la loi de groupe

On suppose que la courbe E est sous forme de Weierstrass. Son équation est donc de la forme

$$Y^2W + a_1XYW + a_3YW^3 = X^3 + a_2X^2W + a_4XW^2 + a_6W^3$$

en coordonnées affine cela donne

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{51}$$

Notons que $O = (0 : 1 : 0)$ est l'unique point à l'infini de la courbe E et que l'opposé d'un point P de coordonnées affines (x_p, y_p) est donné par l'intersection de la droite verticale d'équation $X = x_p$ avec E, en effet on sait que $-P = (O.O).P$ et puisque O est un point d'inflexion (point à l'infini) on a $O.O = O$ et par suite $-P = OP$. Notons (x_{-p}, y_{-p}) les coordonnées affines de $-P$. Nous venons de montrer que $x_{-p} = x_p$, reste à trouver y_{-p}. D'après l'équation (51) on a

$$\begin{aligned} f(x_p, y) &= y^2 + a_1x_py + a_3y - x_p^3 - a_2x_p^2 - a_4x_p - a_6 \\ &= y^2 + y(a_1x_p + a_3) - a_2x_p^2 - a_4x_p - a_6 \end{aligned}$$

C'est une équation de degré deux en y, elle possède deux racines distinctes, à savoir y_p et y_{-p}, et alors on peut écrire, pour une constante c

$$\begin{aligned} f(x_p, y) &= c(y - y_p)(y - y_{-p}) \\ &= cy^2 + cy(-y_{-p} - y_p) + cy_py_{-p} \end{aligned}$$

En comparant le coefficient de y^2 de cette équation avec celui l'équation précédente on trouve $c = 1$ et en comparant les coefficients de y on trouve $y_{-p} = -y_p - a_1x_p - a_3$, donc le point $-P$ est de coordonnées $(x_p, -y_p - a_1x_p - a_3)$.

Proposition 3.4. *Soient $M = (x_1, y_1)$ et $N = (x_2, y_2)$ deux points de la courbe E. On suppose que $M \neq -N$. La somme $M + N$ est alors un point de coordonnées (x_3, y_3) donné par*

$$\begin{aligned} x_3 &= p^2 + a_1p - a_2 - x_1 - x_2 \\ y_3 &= -(p + a_1)x_3 - q - a_3 \end{aligned}$$

avec

$$p = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & si\ M \neq N\ (cas\ secant) \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & si\ M = N\ (cas\ tangent) \end{cases}$$

et

$$q = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1} & si\ M \neq N\ (cas\ secant) \\ \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} & si\ M = N\ (cas\ tangent) \end{cases}$$

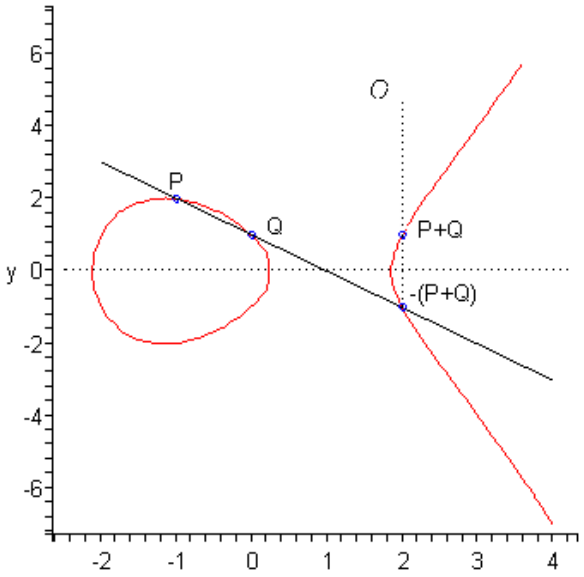


FIGURE 8 – Exemple de calcul de somme et d'inverse pour le point O à l'infini.

Remarque. La droite (MN) est la droite d'équation $Y = pX + q$.

Démonstration. Posons

$$F(X,Y,T) = Y^2T + a_1XYT + a_3YT^2 - X^3 - a_2X^2T - a_4XT^2 - a_6T^3.$$

Si le droite (MN) est verticale, alors $O \in (MN) \cap E$ et $O = (M.N)$, donc

$$M + N = (O.(M.N)) = (O.O) = O$$

cas exclu par l'hypothèse. Donc la droite (MN) n'est pas verticale et elle a une équation affine de la forme

$$Y = pX + q.$$

Calculons les coefficients p et q. Supposons $M \neq N$. Comme, par hypothèse, $M \neq -N$ on a $x_1 \neq x_2$ et

$$\begin{aligned} p =& \frac{y_2 - y_1}{x_2 - x_1} \\ q =& y_1 - px_1 = y_1 - \frac{y_2 - y_1}{x_2 - x_1}x_1 = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}. \end{aligned}$$

Si $M = N$, l'équation de la tangente à E en $M = N$ s'écrit

$$\frac{\partial F}{\partial X}(x, y, 1)X + \frac{\partial F}{\partial Y}(x, y, 1)Y + \frac{\partial F}{\partial T}(x, y, 1) = 0,$$

c'est-à-dire

$$Y = -\frac{\frac{\partial F}{\partial X}(x, y, 1)}{\frac{\partial F}{\partial Y}(x, y, 1)}X - \frac{\frac{\partial F}{\partial T}(x, y, 1)}{\frac{\partial F}{\partial Y}(x, y, 1)}.$$

On en déduit les expressions suivantes pour p et q :

$$\begin{aligned} p =& \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \\ q =& y_1 - px_1 = y_1 - \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}x_1 \\ =& \frac{2y_1^2 + a_1x_1y_1 + a_3y_1 - 3x_1^3 - 2a_1x_1^2 - a_4x_1 + a_1x_1y_1}{2y_1 + a_1x_1 + a_3} \end{aligned}$$

Mais le point (x_1, y_1) étant sur la courbe, on a

$$y_1^2 = x_1^3 + a_2x_1^2 + a_4x_1 + a_6 - a_1x_1y_1 - a_3y_1.$$

En définitive, on obtient

$$q = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

Le point $M+N$ a pour coordonnées (x_3, y_3). Comme $M+N = (O.(M.N))$, le point (M.N) a pour coordonnées $(x_3 : y_3')$ avec

$$y_3 = y_3' - a_1x_3 - a_3. \tag{52}$$

L'intersection de la droite (MN) avec E est donnée par le système d'équations

$$\begin{cases} Y & = pX + q \\ Y^2 + a_1XY + a_3Y & = X^3 + a_2X^2 + a_4X + a_6 \end{cases}$$

De manière plus précise, x_1, x_2 et x_3 sont les racines comptées avec multiplicité du polynôme $F(X, pX + q, 1)$. On a donc la relation

$$\begin{aligned} (pX + q)^2 + a_1(pX + q)X + a_3(pX + q) - X^3 - a_2X^2 - a_4X - a_6 \\ = -(X - x_1)(X - x_2)(X - x_3). \end{aligned}$$

En regardant le coefficient de X^2 dans cette égalité, on obtient

$$p^2 + a_1 p - a_2 = x_1 + x_2 + x_3.$$

Donc

$$x_3 = p^2 + a_1 p - a_2 - x_1 - x_2$$

et, comme $y'_3 = px_3 + q$, on obtient, compte tenu de (52), la relation

$$y_3 = -px_3 - q - a_1 x_3 - a_3$$

.

□

4 Cryptographie à base de courbes elliptiques

4.1 Introduction

Les courbes ellptiques sont utilisées dans plusieurs domaines, elles ont été très utiles pour la preuve du dernier théorème de Fermat (par Andrew Wiles), on peut aussi utiliser les courbes elliptiques pour des tests de primalité et pour la factorisation. En outre, les courbes elliptiques permettent d'implémenter des systemes cryptographiques semblables à celui proposé par ElGamal. La sécurité de tels systèmes dépend de la difficulté de calculer un logarithme discret sur la courbe elliptique.

4.2 Courbes elliptiques sur un corps fini

Les courbes elliptiques définies sur un corps fini sont très importantes en cryptographie à clef publique.

Soit p est un nombre premier strictement plus grand que 3 et prenons le corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Pour simplifier nous allons considérer des corps de caractéristique différente de 2 et de 3, et alors d'après la proposition 2.2 nous pourrons toujours travailler avec des courbes elliptiques de la forme

$$E : y^2 = x^3 + ax + b \tag{53}$$

avec $4a^3 + 27b^2 \neq 0 \bmod p$.

Avant de donner des exemples nous avons besoin d'énoncer quelques définitions et théorèmes utiles pour les cacluls.

Définition 4.1. *Soit p un nombre premier. On dit qu'un entier a est un* résidu quadratique modulo p *si $a \not\equiv 0 \bmod p$ et l'équation $y^2 \equiv a \bmod p$ admet une solution $y \in \mathbb{F}_p$*

Exemple 4.1. *Dans* $\mathbb{Z}/7\mathbb{Z}$, $1^2 = 1$, $2^2 = 4$, $3^2 = 2$, $4^2 = 2$, $5^2 = 4$, $6^2 = 1$. $\{1, 2, 4\}$ *est l'ensemble des résidus quadratiques de* $\mathbb{F}_7$.

On va étudier maintenant comment savoir si un entier a est un *résidu quadratique* ou pas.

Théorème 4.1. (Critère d'Euler) *Soit p un nombre premier. a est un* résidu quadratique *modulo p si et seulement si*

$$a^{(p-1)/2} \equiv 1 \bmod p.$$

Démonstration. Si a est un résidu quadratique il s'écrit $a \equiv y^2 \ mod\ p$. On a alors

$$\begin{aligned} a^{(p-1)/2} &\equiv (y^2)^{(p-1)/2} \bmod p \\ &\equiv y^{p-1} \bmod p \\ &\equiv 1 \bmod p \text{ (grâce au théorème de Fermat : } a^{p-1} \equiv 1 \bmod p). \end{aligned}$$

Réciproquement, supposons que $a^{(p-1)/2} \equiv 1 \ mod\ p$ et soit b un élément primitif modulo p, alors $a \equiv b^i \ mod\ p$ pour un entier positif i. Cela donne :

$$\begin{aligned} a^{(p-1)/2} &\equiv (b^i)^{(p-1)/2} \bmod p \\ &\equiv b^{i(p-1)/2} \bmod p. \end{aligned}$$

L'ordre $(p-1)$ de b divise nécessairement $i(p-1)/2$, par suite i est pair et les racines carrées de a sont $\pm b^{i/2} \ mod\ p$. □

Le critère d'Euler ne calcule pas les racines carrés, mais il nous aide à savoir qui sont les résidus quadratiques.

Vous trouverez plus bas un algorithme en C de calcul des point d'une courbe E.

4.3 Chiffrement et déchiffrement ElGamal elliptiques

Prenons un exemple.

Soit E une courbe elliptique définie sur $\mathbb{F}_{11} = \mathbb{Z}/11\mathbb{Z}$ par l'équation

$$y^2 = x^3 + x + 6$$

(E est bien définie sur $\mathbb{F}_{11}$ et nous avons bien $\Delta = -2^4(4 + 27 \times 36) \neq 0$).

E admet 13 points. Le groupe est d'ordre premier donc cyclique. Donc E est isomorphe à $\mathbb{F}_{13}$ et tout point autre que celui à l'infini est générateur du

groupe. Ceci permet de calculer tout les points de E à partir de n'importe quel point m. Or nous sommes dans un groupe additif, les éléments se calculent alors en faisant $p-2=11$ additions.

Prenons par exemple $m=(2,4)$. Or pour $a_1=a_2=a_3=0$, si M et N sont deux points de E de coordnnées respectifs (x_1,y_1) et (x_2,y_2) la proposition 3.4 devient :

$M+N$ est de coordonnées (x_3,y_3) telle que

$$\begin{aligned} x_3 &= p^2-x_1-x_2 \\ y_3 &= p(x_1-x_3)-y_1. \end{aligned}$$

avec

$$p=\begin{cases} \frac{y_2-y_1}{x_2-x_1} & si\ M\neq N. \\ \frac{3x_1^2+a}{2y_1} & si\ M=N. \end{cases}$$

Pour calculer $2m=m+m=(2,4)+(2,4)$ on calcul

$$\begin{aligned} p &= \frac{3\times 2^2+1}{2\times 4} \bmod 11 \\ &= \frac{13}{8}=2\times 7=3 \text{ dans } \mathbb{F}_{11} \end{aligned}$$

et par suite

$$\begin{aligned} x_3 &= p^2-2x_1=9-4=5 \\ y_3 &= p(x_1-x_3)-y_1=24-4=9 \end{aligned}$$

donc $2m=(5,9)$, on fait pareil pour $3m,\cdots,10m$ et on obtient

$m=[2,4]$	$2m=[5,9]$	$3m=[8,8]$	$4m=[10,9]$
$5m=[3,5]$	$6m=[7,2]$	$7m=[7,9]$	$8m=[3,6]$
$9m=[10,2]$	$10m=[8,3]$	$11m=[5,2]$	$12m=[2,7]$

Chiffrement et déchiffrement :

Alice et Bob sont en contact. Alice veut envoyer un message à Bob. Bob choisit une courbe elliptique E, par exemple $E: y^2=x^3+x+6$, il choisit également un élément $g=(2,4)$ de E et un entier aléatoire $0\leq a\leq 12$ prenons par exemple $a=3$. Il calcule

$$A=a\times g=3\times(2,4)=(8,8)\in E.$$

La clef publique de Bob est alors (E,g,A) et sa clef privée est a.

Alice récupère la clef publique de Bob, elle choisit un entier $0 \leq b \leq 12$ (clef secondaire) prenons $b = 7$ par exemple, Alice calule

$$C = b \times A + m = 7(8,8) + (10,9) = (3,6) + (10,9) = (2,7)$$
$$B = b \times g = 7(2,4) = (7,9)$$

Le message crypté (transmis par le réseau) est $(C, B) = ((2,7),(7,9))$.

Bob reçoit le message crypté d'Alice et veut le décrypter, il calcule

$$-aB + C = -3(7,9) + (2,7) = -(3,6) + (2,7) = (3,5) + (2,7) = (10,9)$$

Bob retrouve bien le message clair d'Alice.

4.4 Cryptographie ECDSA (signature et authentification)

l'ECDSA (*Elliptic curve digital signature algorithm*) est l'analogue du DSA sauf qu'au lieu de travailler avec des sous-groupes d'ordres q dans $\mathbb{F}_p^*$, on travaille avec des courbes elliptiques $E(\mathbb{F}_p)$.

Alice choisit une courbe elliptique E sur $\mathbb{F}_p$ que le nombre de points de $E(\mathbb{F}_p)$ soit divisible par un eniter n(premier) très grand. Elle choisit un point g de $E(\mathbb{F}_p)$ et un entier $a \in [1, n-1]$, elle calcule $A = ag$.
La clef publique d'Alice est alors (E, g, n, A), sa clef privée est a.

Calcule de la signature pour ECDSA :
Soit m le message en clair. Pour calculer la signature, Alice procède comme suit

1. Elle choisit une entier $1 \leq k \leq n-1$ (clef secondaire), et calcule $B = kg = (x_1, y_1)$. Si x_1=0 pour des raisons de sécurité on revient à l'étape 1 (en effet si x_1=0 la signature $d = k^{-1}(h(m) + ax_1) \bmod n$ n'utilise pas la clef privée a).
2. Alice calcule $k^{-1} \bmod n$.
3. Elle calcule $d = k^{-1}\{h(m) + ax_1\} \bmod n$, où h est une fonction de hachage sécurisée (SHA-1).
4. Si $d = 0$ (alors d^{-1}, qui va être utilisée dans la vérification de la signature, n'existe pas) alors on retourne à l'étape 1.
5. la signature du message m est le couple des entiers (x_1, d).

Vérification de la signature pour ECDSA : Bob reçoit la signature (x_1, d) d'Alice et veut savoir si elle est valide, alors il fait les étapes suivantes :

1. En utilisant la clef publique d'Alice (E, g, n, A) Bob vérifie que c et d sont bien des entiers apartenant à $[1, n-1]$.
2. Bob calcule $h(m)$.
3. Il calcule $w = d^{-1} \bmod n$.
4. Il calcule ensuite $u_1 = h(m)w \bmod n$ et $u_2 = x_1 w \bmod n$.
5. Bob calcule ensuite $u_1 g + u_2 A = (x_0, y_0)$.
6. Si $x_0 = x_1$ la signature serait en effet bien valide.
   En effet,

$$\begin{aligned} u_1 P + u_2 Q = h(m)wg + x_1 wA = h(m)d^{-1}g + x_1 d^{-1}ag \\ = \frac{kg}{h(m) + ax_1}(h(m) + x_1 a) \\ = kg = (x_1, y_1) \end{aligned}$$

Côté sécurité : l'ECDSA, comme tout les cryptosystemes de l'ECDLP (*elliptic curve discrete logarithm problem*), est difficile à casser : pour une courbe elliptique E définie sur $\mathbb{F}_p$, un point $P \in \mathbb{F}_p$ d'ordre n, et un point $Q \in \mathbb{F}_p$, trouver l'entier l, $0 \leq l \leq n-1$, tel que $Q = lP$ est très difficile.

4.5 Conclusion

La plus grande utilité des cryptosystèmes à base de courbes elliptiques est le fait qu'on puisse utiliser des clefs plus courtes et aussi fortes (même plus forte) que pour d'autres cryptosystèmes. Une clef de 160 bits pour un système à base de courbes elliptiques offre le même niveau de sécurité qu'une clef de 1024 bits d'un système comme le DSA ou le RSA.

4.6 Remerciements

Je tiens à remercier mon tutteur M. Peyre Emmanuel pour le soutien qu'il m'a apporté. Son éxigence m'a fait comprendre et m'a appris beaucoup de nouvelles choses, non seulement sur les bases des courbes elliptiques mais aussi sur la manière dont on rédige un mémoire..

4.7 Références

[KNA] ELLIPTIC CURVES by Anthony W. Knapp
Mathematical notes (Princeton University Press) 1993.

[PEY] CORPS FINIS ET COURBES ELLIPTIQUES par Emmanuel Peyre
(Institut Fourier, Université de Grenoble 1 et CNRS) 2007.

[STI] CRYPTOGRAPHIE par Douglas Stinson 2-ème édition-
(Université de Waterloo (Ontorio) 2003.