ENSIBS Cyber & Info

Année universitaire 2019 / 2020

Introduction aux courbes elliptiques

Responsable : A. RIDARD

Table des matières

I. Fonctions à deux variables

1. Rappels sur les fonctions à une variable

Dans ces rappels, on considère une fonction réelle à une variable réelle $f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & f(x) \end{array}$.

Il s'agit d'un "procédé d'association" qui à tout réel x associe au plus un réel noté alors $f(x)$.
Plus rigoureusement, f est une relation binaire sur $\mathbb{R}$ telle que tout réel x soit en relation avec au plus un réel noté alors $f(x)$.

On note $\mathscr{D}_f$ l'ensemble de définition de f c'est à dire l'ensemble des réels x en relation avec un réel noté $f(x)$ (son image par f) :

$$\mathscr{D}_f = \{x \in \mathbb{R} \mid f(x) \text{ existe}\}$$

Définition (Courbe représentative)**.**

On appelle courbe représentative de f l'ensemble :

$$\mathscr{C}_f = \left\{\big(x, f(x)\big) \in \mathbb{R}^2 \mid x \in \mathscr{D}_f\right\}$$

C'est tout simplement la représentation graphique de la relation binaire f sur $\mathbb{R}$, et donc une partie du plan $\mathbb{R}^2$.

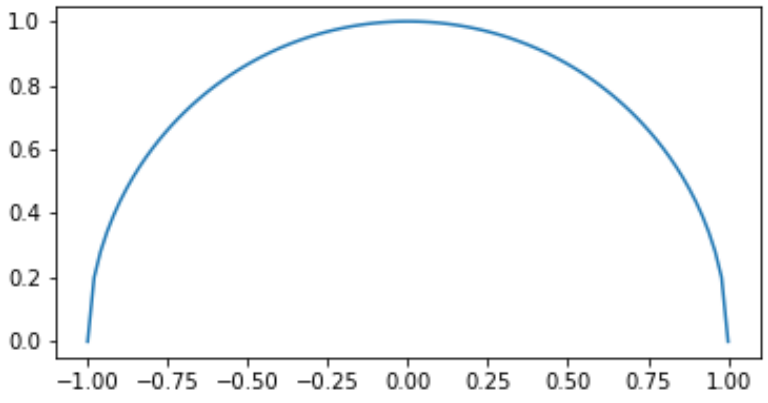
Une courbe représentative

```python
# Importation des modules
import numpy as np
import pylab as pl

# Définition de la fonction de R vers R
def f(x):
    return np.sqrt(1-x**2)

# Représentation graphique
x = np.linspace(-1,1,100)
y = f(x)

pl.subplot(1,1,1,aspect='equal')
pl.plot(x,y)
pl.savefig('courbeRep.png')
```



Pour étudier localement une telle fonction, on utilise les notions suivantes :

Définition (Limite)**.**

On dit que f tend vers $l \in \mathbb{R}$ en $x_0 \in \mathbb{R}$ et on note $\lim\limits_{x \to x_0} f(x) = l$ ou plus simplement $\lim\limits_{x_0} f = l$ si :

$$\forall \epsilon > 0,\ \exists \eta > 0,\ \forall x \in \mathscr{D}_f,\ |x - x_0| < \eta \Longrightarrow |f(x) - l| < \epsilon$$

- On peut aussi faire l'étude asymptotique de f c'est à dire étudier f "au voisinage" de l'infini
- La limite de f peut être infinie ou ne pas exister (les deux cas de divergence)

Définition (Continuité)**.**

On dit que f est continue en $x_0 \in \mathscr{D}_f$ si :

$$\lim_{x \to x_0} f(x) = f(x_0)$$

- "Au voisinage de x_0, $f(x)$ est proche de $f(x_0)$"
- Lorsque x_0 n'appartient pas à $\mathscr{D}_f$, on peut essayer de prolonger par continuité f en x_0

Considérons la fonction $f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \frac{\sin x}{x} \end{array}$.

1. Déterminer $\mathscr{D}_f$ et $\lim\limits_{x \to 0} f(x)$.
2. En déduire le prolongement par continuité de f en 0.

Définition (Dérivabilité)**.**

On dit que f est dérivable en $x_0 \in \mathscr{D}_f \setminus \partial\mathscr{D}_f$ si :

$$\lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0} \quad \text{existe et est réelle}$$

Dans ce cas, on note $f'(x_0)$ cette limite.

- $\partial\mathscr{D}_f$ désigne "le bord" de $\mathscr{D}_f$ donc $\mathscr{D}_f \setminus \partial\mathscr{D}_f$ représente "l'intérieur" de $\mathscr{D}_f$
- On définit ainsi la fonction dérivée f' que l'on calcule en général à l'aide de formules
- En posant $x = x_0 + h$, on obtient :

$$\lim_{h \to 0} \frac{f(x_0 + h) - f(x_0)}{h} \quad \text{existe et est réelle}$$

Propriété (DL à l'ordre 1)**.**

Si f est dérivable en x_0, alors "au voisinage de x_0" :

$$f(x) = f(x_0) + f'(x_0)(x - x_0) + (x - x_0)\epsilon(x) \quad \text{avec } \lim_{x \to x_0} \epsilon(x) = 0$$

- "Au voisinage de x_0, $f(x)$ est proche de $f(x_0)+f'(x_0)(x-x_0)$"
- Une fonction dérivable en un réel "ressemble" à une fonction affine au voisinage de ce réel
- En posant $x = x_0 + h$, on obtient :

$$f(x_0+h) = f(x_0) + f'(x_0)h + h\epsilon(h) \quad \text{avec} \lim_{h\to 0} \epsilon(h) = 0$$

- Cette condition est même suffisante pour que f soit dérivable en x_0

Propriété (Tangente)**.**

Si f est dérivable en x_0, alors la courbe $\mathscr{C}_f$ admet une tangente au point $\big(x_0, f(x_0)\big)$ d'équation :

$$y = f'(x_0)(x-x_0) + f(x_0)$$

- C'est la droite de coefficient directeur $f'(x_0)$ et passant par le point $\big(x_0, f(x_0)\big)$
- La courbe représentative d'une fonction dérivable en un réel "ressemble" à une droite au voisinage de ce réel
- Par définition, une tangente d'une courbe représentative ne peut pas être verticale

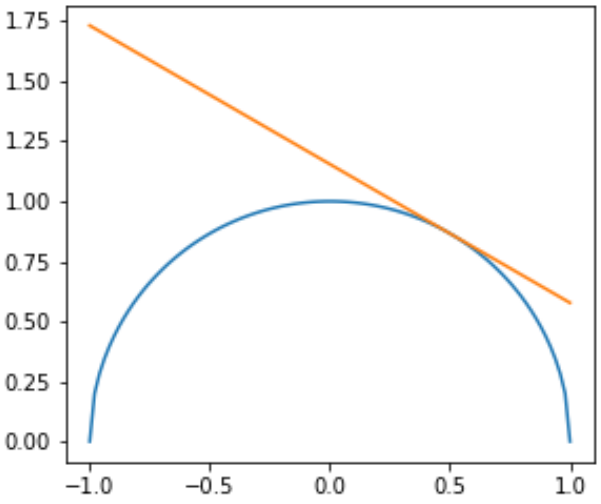
Une tangente

```
# Importation des modules
import numpy as np
import pylab as pl

# Définition de la fonction de R vers R
def f(x):
    return np.sqrt(1-x**2)

# Représentation graphique
x = np.linspace(-1,1,100)
y1 = f(x)
y2 = (-1/np.sqrt(3))*(x-1/2)+f(1/2)

pl.subplot(1,1,1,aspect='equal')
pl.plot(x,y1)
pl.plot(x,y2)
pl.savefig('tangente.png')
```



Toutes les courbes du plan sont-elles des courbes représentatives de fonctions à une variable ?

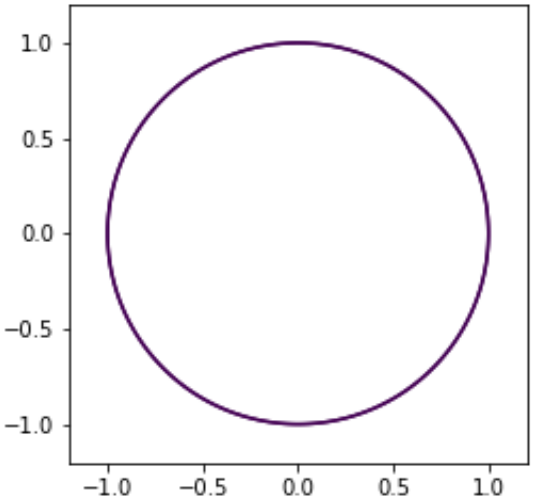
Une courbe "non représentative"

```
# Importation des modules
import numpy as np
import pylab as pl

# Définition de la fonction de R^2 vers R
def f(x,y):
    return x**2+y**2-1

# Représentation graphique
x = np.linspace(-1.2,1.2,100)
y = np.linspace(-1.2,1.2,100)
X,Y = np.meshgrid(x,y)
Z = f(X,Y)

pl.subplot(1,1,1,aspect='equal')
pl.contour(X,Y,Z,[0])
pl.savefig('courbeNonRep.png')
```



2. Surface représentative et courbes de niveaux

On considère maintenant une fonction réelle à deux variables réelles $f : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & f(x,y) \end{array}$.

On note encore $\mathscr{D}_f$ l'ensemble de définition de f :

$$\mathscr{D}_f = \{(x,y) \in \mathbb{R}^2 \mid f(x,y) \text{ existe}\}$$

Définition (Surface représentative)**.**

On appelle surface représentative de f l'ensemble :

$$\mathscr{S}_f = \left\{\left(x,y,f(x,y)\right) \in \mathbb{R}^3 \mid (x,y) \in \mathscr{D}_f\right\}$$

C'est tout simplement la représentation graphique de la relation binaire f de $\mathbb{R}^2$ vers $\mathbb{R}$, et donc une partie de l'espace $\mathbb{R}^3$.

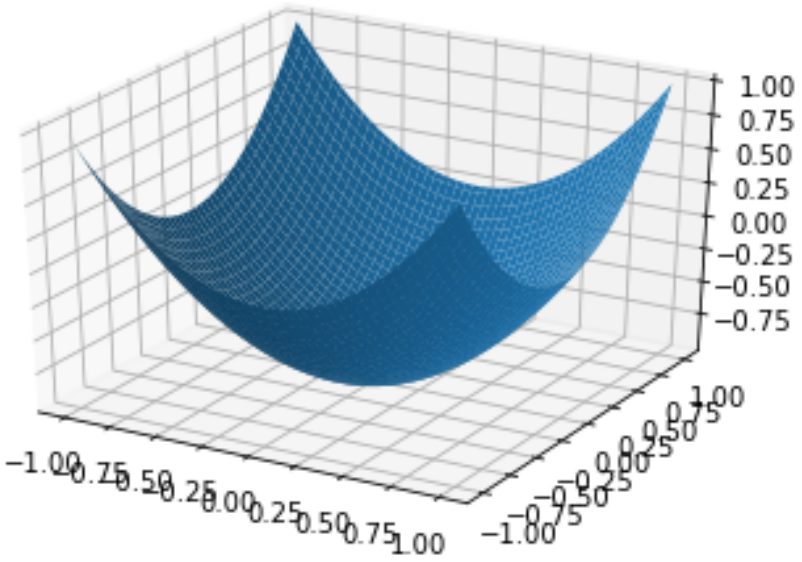
Une surface représentative

```python
# Importation des modules
import numpy as np
import pylab as pl
from mpl_toolkits.mplot3d import Axes3D

# Définition de la fonction de R^2 vers R
def f(x,y):
    return x**2+y**2-1

# Représentation graphique
x = np.linspace(-1,1,100)
y = np.linspace(-1,1,100)
X,Y = np.meshgrid(x,y)
Z = f(X,Y)

fig = pl.figure()
ax = fig.gca(projection='3d')
ax.plot_surface(X,Y,Z)
pl.savefig('surfRep.png')
```



Définition (Courbes de niveaux)**.**

On appelle courbe de niveau k de f l'ensemble :

$$\mathscr{C}_{f,k} = \{(x,y) \in \mathbb{R}^2 \mid f(x,y) = k\}$$

C'est tout simplement l'ensemble des antécédents de k par f, et donc une partie de $\mathbb{R}^2$.

Comparer $\mathscr{C}_{f,k}$ et $\mathscr{S}_f \cap \{(x,y,z) \in \mathbb{R}^3 \mid z = k\}$.

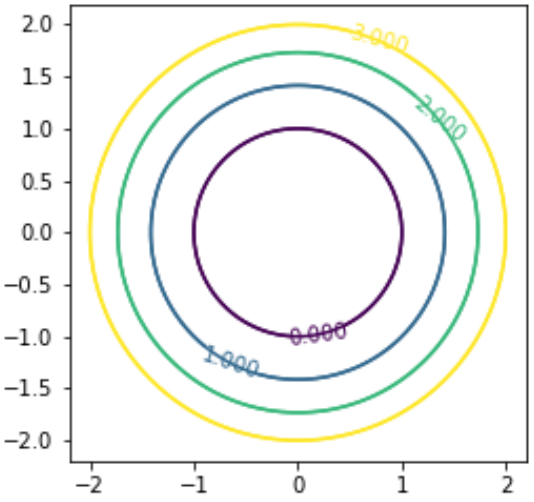
Des courbes de niveaux

```
# Importation des modules
import numpy as np
import pylab as pl

# Définition de la fonction de R^2 vers R
def f(x,y):
    return x**2+y**2-1

# Représentation graphique
x = np.linspace(-2.2,2.2,100)
y = np.linspace(-2.2,2.2,100)
X,Y = np.meshgrid(x,y)
Z = f(X,Y)

pl.subplot(1,1,1,aspect='equal')
pl.contour(X,Y,Z,[0,1,2,3])
ln = pl.contour(X,Y,f(X,Y),[0,1,2,3])
pl.clabel(ln)
pl.savefig('courbesNiv1.png')
```



Étudier les courbes de niveaux de f permet de mieux "comprendre" f

Comment peut-on généraliser à $\mathbb{R}^2$ (et même à n'importe quel ev) la notion de valeur absolue ?

3. Norme

Définition (norme et evn)**.**

Une norme sur un ev E est une application N de E dans $\mathbb{R}$ vérifiant :

1. $\forall u \in E,\ \forall \lambda \in \mathbb{R},\ N(\lambda u) = |\lambda| N(u)$ (homogénéité)
2. $\forall (u,v) \in E^2,\ N(u+v) \leq N(u) + N(v)$ (inégalité triangulaire)
3. $\forall u \in E,\ N(u) \geq 0$ (positivité)
4. $\forall u \in E \setminus \{0_E\},\ N(u) > 0$ (stricte positivité)

L'ev E muni d'une norme N est un espace vectoriel normé (evn) noté (E, N).

- Les normes sont souvent notées $\|.\|$, elles servent à définir la longueur d'un vecteur
- La valeur absolue est une norme sur $E = \mathbb{R}$
- Sur $E = \mathbb{R}^2$, on peut définir plusieurs normes :
  — $\|(x,y)\|_1 = |x| + |y|$
  — $\|(x,y)\|_2 = \sqrt{|x|^2 + |y|^2}$ (norme euclidienne vue au lycée)
  — $\|(x,y)\|_\infty = \max\{|x|, |y|\}$

Définition (normes équivalentes)**.**

On dit que deux normes N_1 et N_2 sont équivalentes s'il existe deux réels strictement positifs α et β tels que :

$$\forall u \in E,\ \alpha N_2(u) \leq N_1(u) \leq \beta N_2(u)$$

- Dans $\mathbb{R}^2$, les trois normes définies précédemment sont équivalentes
- En fait, dans un evn de dimension finie, toutes les normes sont équivalentes

Soit $(E, \|.\|)$ un evn, a un vecteur de E et R un réel strictement positif.
La boule ouverte de centre a et de rayon R, notée $B(a,R)$, est définie par :

$$B(a,R) = \{u \in E \mid \|u - a\| < R\}$$

Représenter la boule unité (de centre 0_E et de rayon 1) dans :

1. $(\mathbb{R}, |.|)$
2. $(\mathbb{R}^2, \|.\|_2)$
3. $(\mathbb{R}^2, \|.\|_1)$
4. $(\mathbb{R}^2, \|.\|_\infty)$

Boule unité dans $(\mathbb{R}^3, \|.\|_2)$

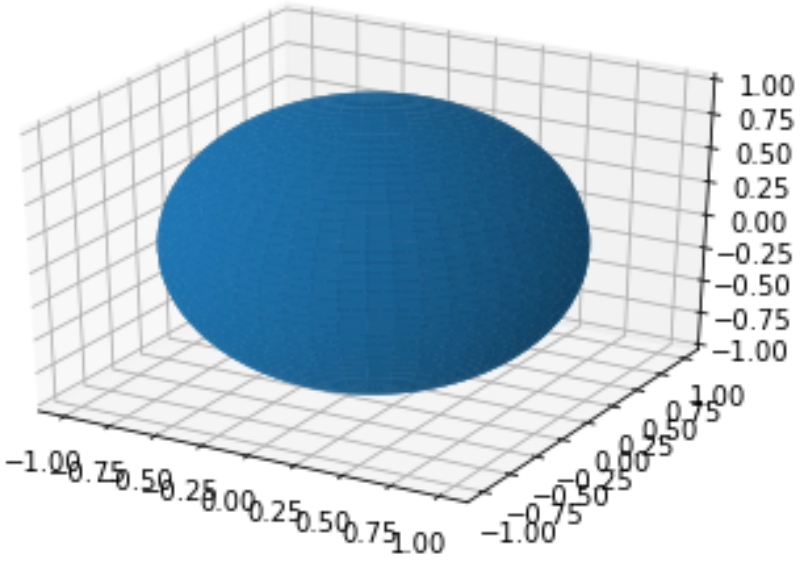
```python
# Importation des modules
import numpy as np
import pylab as pl
from mpl_toolkits.mplot3d import Axes3D
from itertools import product, combinations

# Représentation graphique de la surface paramétrée
fig = pl.figure()
ax = fig.add_subplot(111, projection='3d')

u = np.linspace(0, 2 * np.pi, 100) # longitude
v = np.linspace(0, np.pi, 100) # colatitude

# Coordonnées sphériques
x = np.outer(np.cos(u), np.sin(v))
y = np.outer(np.sin(u), np.sin(v))
z = np.outer(np.ones(np.size(u)), np.cos(v))

ax.plot_surface(x, y, z)
pl.savefig('boule.png')
```



On peut maintenant généraliser la continuité et la dérivabilité aux fonctions à deux variables.

4. Limite et continuité

Définition (Limite)**.**

On dit que f tend vers $l \in \mathbb{R}$ en $(x_0, y_0) \in \mathbb{R}^2$ et on note $\lim\limits_{(x,y)\to(x_0,y_0)} f(x,y) = l$ ou plus simplement $\lim\limits_{(x_0,y_0)} f = l$ si :

$$\forall \epsilon > 0,\ \exists \eta > 0,\ \forall (x,y) \in \mathscr{D}_f,\ \|(x,y) - (x_0,y_0)\| < \eta \Longrightarrow |f(x,y) - l| < \epsilon$$

- Cette propriété est dite topologique car elle ne dépend pas de la norme utilisée
- Pour montrer $\lim\limits_{(x,y)\to(x_0,y_0)} f(x,y) = l$, on majore $|f(x,y) - l|$ par une quantité qui tend vers 0 quand $(x,y) \to (x_0,y_0)$
- Pour montrer $\lim\limits_{(x,y)\to(x_0,y_0)} f(x,y) \neq l$, on prend un "chemin" selon lequel $f(x,y)$ ne tend pas vers l quand $(x,y) \to (x_0,y_0)$

Définition (Continuité)**.**

On dit que f est continue en $(x_0, y_0) \in \mathscr{D}_f$ si :

$$\lim_{(x,y)\to(x_0,y_0)} f(x,y) = f(x_0,y_0)$$

On considère la fonction $f : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & \begin{cases} \frac{xy^2}{x^2+y^2} & \text{si } (x,y) \neq (0,0) \\ 0 & \text{si } (x,y) = (0,0) \end{cases} \end{array}$.

Montrer que f est continue en $(0,0)$.

5. Dérivées partielles et différentiabilité

Définition (Dérivées partielles).

On dit que f admet une première dérivée partielle en $(x_0, y_0) \in \mathscr{D}_f \setminus \partial\mathscr{D}_f$ si :

$$\lim_{h\to 0} \frac{f(x_0+h, y_0) - f(x_0, y_0)}{h} \quad \text{existe et est réelle}$$

Dans ce cas, on la note $\dfrac{\partial f}{\partial x}(x_0, y_0)$.

De même, on dit que f admet une deuxième dérivée partielle en $(x_0, y_0) \in \mathscr{D}_f \setminus \partial\mathscr{D}_f$ si :

$$\lim_{h\to 0} \frac{f(x_0, y_0+h) - f(x_0, y_0)}{h} \quad \text{existe et est réelle}$$

Dans ce cas, on la note $\dfrac{\partial f}{\partial y}(x_0, y_0)$.

On définit ainsi les fonctions dérivées pratielles $\dfrac{\partial f}{\partial x}$ et $\dfrac{\partial f}{\partial y}$ que l'on calcule en général à l'aide de formules

On considère la fonction $f : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & \begin{cases} \frac{xy^2}{x^2+y^2} & \text{si } (x,y) \neq (0,0) \\ 0 & \text{si } (x,y) = (0,0) \end{cases} \end{array}$.

Montrer que f admet les deux dérivées partielles en $(0,0)$.

Pour généraliser la notion de dérivabilité, il nous faut plus que ces dérivées partielles.

Définition (Différentiabilité).

On dit que f est différentiable en $(x_0, y_0) \in \mathscr{D}_f \setminus \partial\mathscr{D}_f$ si "au voisinage de (x_0, y_0)",
il existe une application linéaire de $\mathbb{R}^2$ dans $\mathbb{R}$, notée $df(x_0, y_0)$, vérifiant :

$$f(x_0+h_1, y_0+h_2) = f(x_0, y_0) + df(x_0, y_0).(h_1, h_2) + \|(h_1, h_2)\|\epsilon(h_1, h_2) \quad \text{avec} \lim_{(h_1,h_2)\to(0,0)} \epsilon(h_1, h_2) = 0$$

Dans ce cas, $df(x_0, y_0)$ est appelée la différentielle de f en (x_0, y_0) et on a :

$$df(x_0, y_0).(h_1, h_2) = h_1 \frac{\partial f}{\partial x}(x_0, y_0) + h_2 \frac{\partial f}{\partial y}(x_0, y_0)$$

Il s'agit en fait du DL à l'ordre 1 de f en (x_0, y_0)

On considère la fonction $f : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & \begin{cases} \frac{x^2y^2}{x^2+y^2} & \text{si } (x,y) \neq (0,0) \\ 0 & \text{si } (x,y) = (0,0) \end{cases} \end{array}$.

Montrer que f est différentiable en $(0,0)$.

Ce n'est pas parce que f admet les deux dérivées partielles en (x_0, y_0) que f est différentiable en (x_0, y_0).
Considérer en $(0,0)$ la fonction $f : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & \begin{cases} \frac{xy^2}{x^2+y^2} & \text{si } (x,y) \neq (0,0) \\ 0 & \text{si } (x,y) = (0,0) \end{cases} \end{array}$

Définition (Jacobienne).

On appelle jacobienne de f en (x_0, y_0), la matrice (dans les bases canoniques) de l'application linéaire $df(x_0, y_0)$:

$$\mathcal{J}f(x_0, y_0) = \begin{pmatrix} \frac{\partial f}{\partial x}(x_0, y_0) & \frac{\partial f}{\partial y}(x_0, y_0) \end{pmatrix}$$

Les formules connues de dérivées restent vraies sur la jacobienne.
Par exemple, $(uv)'(x_0) = u'(x_0) \times v(x_0) + u(x_0) \times v'(x_0)$ devient :

$$\mathcal{J}(fg)(x_0, y_0) = \mathcal{J}f(x_0, y_0) \times g(x_0, y_0) + f(x_0, y_0) \times \mathcal{J}g(x_0, y_0)$$

De la même manière que l'on note $(uv)' = u' \times v + u \times v'$, on pourra noter tout simplement :

$$\mathcal{J}(fg) = \mathcal{J}f \times g + f \times \mathcal{J}g$$

On considère les fonctions $f : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & xy \end{array}$ et $g : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & x^2+y^2 \end{array}$.
Déterminer $\mathcal{J}(fg)(x,y)$ pour tout $(x,y) \in \mathbb{R}^2$.

Définition (Point critique).

On dit que (x_0, y_0) est un point critique de f si $\frac{\partial f}{\partial x}(x_0, y_0) = \frac{\partial f}{\partial y}(x_0, y_0) = 0$

6. Tangente à une courbe définie implicitement

On considère la courbe de niveau 0 de f d'équation $f(x,y) = 0$.

A l'inverse de ce qui a été fait précédemment [1], on va étudier f pour mieux comprendre cette courbe de niveau.

Heuristique

Si f est différentiable en (x_0, y_0), on a "au voisinage de (x_0, y_0)" :

$$f(x_0 + h_1, y_0 + h_2) \simeq f(x_0, y_0) + h_1 \frac{\partial f}{\partial x}(x_0, y_0) + h_2 \frac{\partial f}{\partial y}(x_0, y_0)$$

c'est à dire (en posant $x = x_0 + h_1$ et $y = y_0 + h_2$) :

$$f(x,y) \simeq f(x_0, y_0) + (x - x_0) \frac{\partial f}{\partial x}(x_0, y_0) + (y - y_0) \frac{\partial f}{\partial y}(x_0, y_0)$$

Si $f(x_0, y_0) = 0$ et si $\frac{\partial f}{\partial y}(x_0, y_0) \neq 0$, alors "au voisinage de (x_0, y_0)" :

$$f(x,y) = 0 \Longleftrightarrow y \simeq y_0 - (x - x_0) \frac{\frac{\partial f}{\partial x}(x_0, y_0)}{\frac{\partial f}{\partial y}(x_0, y_0)}$$

[1]. Rappelez-vous, étudier les courbes de niveaux de f pour mieux "comprendre" f

Propriété (Théorème des fonctions implicites)**.**

Soit f une fonction différentiable en (x_0, y_0) telle que $f(x_0, y_0) = 0$.
Si $\frac{\partial f}{\partial y}(x_0, y_0) \neq 0$, alors "au voisinage de (x_0, y_0)" :

$$f(x, y) = 0 \Longleftrightarrow y = \phi(x)$$

avec ϕ dérivable vérifiant $\phi'(x) = -\frac{\frac{\partial f}{\partial x}(x,\phi(x))}{\frac{\partial f}{\partial y}(x,\phi(x))}$

Si c'est $\frac{\partial f}{\partial x}(x_0, y_0)$ qui est non nulle, il suffit d'échanger les rôles de x et y

Propriété (Équation de la tangente)**.**

Soit f une fonction différentiable en (x_0, y_0).
Si (x_0, y_0) n'est pas un point critique de f, alors la courbe d'éq. $f(x, y) = 0$ admet une tangente au point (x_0, y_0) d'éq. :

$$(x - x_0)\frac{\partial f}{\partial x}(x_0, y_0) + (y - y_0)\frac{\partial f}{\partial y}(x_0, y_0) = 0$$

Démontrer cette propriété.

II. Polynômes de degré 3

1. Rappels sur les polynômes de degré 2

On considère dans cette partie $P = aX^2 + bX + c$ un polynôme (à coefficients réels) du second degré ($a \neq 0$).

Propriété (Racines et discriminant)**.**

On note $\Delta = b^2 - 4ac$ le discriminant de P.

- Si $\Delta > 0$, alors P admet deux racines réelles (simples) :

$$x_1 = \frac{-b - \sqrt{\Delta}}{2a} \quad \text{et} \quad x_2 = \frac{-b + \sqrt{\Delta}}{2a}$$

  De plus, $P = a(X - x_1)(X - x_2)$
- Si $\Delta = 0$, alors P admet une racine réelle (double) :

$$x_1 = \frac{-b}{2a}$$

  De plus, $P = a(X - x_1)^2$
- Si $\Delta < 0$, alors P n'admet pas de racine réelle [a].

a. En revanche, P admet deux racines complexes (conjuguées) :

$$z_1 = \frac{-b - i\sqrt{-\Delta}}{2a} \quad \text{et} \quad z_2 = \frac{-b + i\sqrt{-\Delta}}{2a}$$

De plus, $P = a(X - z_1)(X - z_2)$

- On ne fera pas la différence entre le polynôme $P = aX^2 + bX + c$ et la fonction polynomiale $P : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & ax^2 + bx + c \end{array}$
- P a toujours deux racines complexes z_1 et z_2 (éventuellement confondues) vérifiant :

$$\Delta = a^2(z_1 - z_2)^2$$

- Un polynôme a toujours autant de racines complexes que son degré (théorème de D'Alembert), il est alors scindé :

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = a_n(X - z_1)(X - z_2)\ldots(X - z_n)$$

2. CNS de racine multiple

On considère dans cette partie $P = a_3X^3 + a_2X^2 + a_1X + a_0$ un polynôme (à coefficients réels) de degré 3 ($a_3 \neq 0$).
On note z_1, z_2, z_3 ses trois racines complexes (éventuellement confondues) :

$$P = a_3(X - z_1)(X - z_2)(X - z_3)$$

Définition (Racine multiple)**.**

On dit que z_1 est racine multiple de P si $(X - z_1)^2$ divise P :

$$P = (X - z_1)^2 Q \quad \text{avec } Q \text{ un polynôme de degré 1}$$

- On rappelle que z_1 est racine de P c'est à dire $P(z_1) = 0$ si $(X - z_1)$ divise P (division euclidienne)
- On remarque que $(X - z_1)^2$ divise P si et seulement si $z_1 = z_2$ ou $z_1 = z_3$

Propriété (CNS à l'aide de la dérivée)**.**

z_1 est racine multiple de P si et seulement si $P(z_1) = P'(z_1) = 0$

Définition (Discriminant)**.**

On appelle discriminant de P, noté Δ, le nombre défini par :

$$\Delta = a_3^4(z_1 - z_2)^2(z_1 - z_3)^2(z_2 - z_3)^2$$

En notant $z_1, z_2, \ldots, z_n$ les n racines complexes de $a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$, on peut définir :

$$\Delta = a_n^{2n-2} \prod_{i<j} (z_i - z_j)^2$$

Propriété (CNS à l'aide du discriminant)**.**

P admet une racine multiple si et seulement si $\Delta = 0$

3. Discriminant de $X^3 + aX + b$

On considère dans cette partie $P = X^3 + aX + b$ et on note z_1, z_2, z_3 ses trois racines complexes.

Propriété (Relations entre coefficients et racines)**.**

On note $\sigma_1 = z_1 + z_2 + z_3$, $\sigma_2 = z_1z_2 + z_1z_3 + z_2z_3$ et $\sigma_3 = z_1z_2z_3$.
On peut alors exprimer les σ_i à l'aide des coefficients de P :

$$\sigma_1 = 0,\ \sigma_2 = a \text{ et } \sigma_3 = -b$$

- En fait, pour $a_3X^3 + a_2X^2 + a_1X + a_0$ avec z_1, z_2, z_3 ses trois racines complexes, on a :

$$\sigma_1 = -\frac{a_2}{a_3},\ \sigma_2 = \frac{a_1}{a_3} \text{ et } \sigma_3 = -\frac{a_0}{a_3}$$

- Rappelez-vous les relations entre coefficients et racines pour $aX^2 + bX + c$ avec z_1, z_2 ses racines complexes :

$$z_1 + z_2 = \frac{-b}{a} \text{ et } z_1z_2 = \frac{c}{a}$$

Propriété (Discriminant de $X^3 + aX + b$)**.**

Le discriminant de P s'exprime à l'aide de ses coefficients :

$$\Delta = -(4a^3 + 27b^2)$$

Preuve. Cf. feuille de TD 2

III. Courbes elliptiques

1. Définition et caractérisation

Définition (Point singulier)**.**

On considère une courbe $\mathscr{C} : f(x,y) = 0$.
On dit que (x,y) est un point singulier de $\mathscr{C}$ si c'est un point critique de f **et un point de** $\mathscr{C}$.

Un point critique de f n'est pas forcément un point singulier de $\mathscr{C} : f(x,y) = 0$.
Considérer par exemple $\mathscr{C} : y^2 = x^3 + x^2$

Définition (Courbe elliptique)**.**

On dit que la courbe $\mathscr{C} : f(x,y) = 0$ est elliptique si $f(x,y) = y^2 - x^3 - ax - b$ et si elle n'admet aucun point singulier.

Les courbes suivantes sont-elles elliptiques ?

1. $\mathscr{C}_1 : y^2 = x^3 - x$
2. $\mathscr{C}_2 : y^2 = x^3 - x + 1$
3. $\mathscr{C}_3 : y^2 = x^3 + b$ avec $b \in \mathbb{R}$

Propriété (CNS à l'aide des coefficients)**.**

Une courbe d'équation (courte de Weirstrass) $y^2 = x^3 + ax + b$ est elliptique si et seulement si $4a^3 + 27b^2 \neq 0$

Démontrer cette propriété.

2. Loi de groupe

Définition (Groupe)**.**

Un groupe est un ensemble G muni d'une loi interne [a] $*$ vérifiant :

- $\forall x,y,z \in G,\ (x*y)*z = x*(y*z)$ (associativité)
- $\exists e \in G,\ \forall x \in G,\ x*e = e*x = x$ (élément neutre)
- $\forall x \in G,\ \exists y \in G,\ x*y = y*x = e$ (symétrique)

a. Une application $GxG \to G$

- L'élément neutre est unique, tout comme le symétrique d'un élément
- Si la loi $*$ est commutative [a], le groupe G est dit commutatif (abélien). Dans ce cas,
  - — la loi $*$ est (souvent) notée $+$ et appelée addition
  - — l'élément neutre est noté 0
  - — le symétrique de x est noté $-x$ et appelé opposé

a. $\forall x,y \in G,\ x*y = y*x$

Les courbes elliptiques sont un formidable outil de cryptographie asymétrique tant elles apportent d'usages intéressants et variés. On les retrouve dans de nombreux protocoles utilisés quotidiennement sur Internet comme TLS (RFC 4492 : « Elliptic Curve Cryptography Cipher Suites for TLS »), PGP (RFC 6637 : « Elliptic Curve Cryptography in OpenPGP »), ou encore SSH (RFC 5656 : « Elliptic-curve algorithm integration in the Secure Shell transport layer »), souvent à travers l'acronyme générique ECC (« Elliptic Curve Cryptography »).

De célèbres applications ou projets comme Tor, Apple iMessage ou Bitcoin (à travers la courbe elliptique secp256k1, cf. [1]) en font aussi un usage central pour préserver l'authenticité des messages, leur confidentialité ou l'anonymat des parties.

Les courbes elliptiques permettent de multiples usages :

- l'échange de clé avec l'algorithme ECDH (*Elliptic Curve Diffie-Hellman*) ;
- la signature électronique avec l'algorithme ECDSA (*Elliptic Curve Digital Signature Algorithm*) ;
- le test de primalité avec l'algorithme ECPP (*Elliptic Curve Primality Proving*) ;
- la factorisation d'entiers avec l'algorithme ECM (*Elliptic Curve Method*).

Les courbes elliptiques bénéficient en plus d'une meilleure robustesse cryptographique, d'une plus faible empreinte mémoire et d'une plus grande rapidité de calcul que les cryptosystèmes asymétriques non elliptiques.

1. QU'EST-CE QU'UNE COURBE ELLIPTIQUE ?

La cryptographie sur les courbes elliptiques repose non pas sur nos classiques opérations sur les entiers, mais sur l'utilisation astucieuse d'un ensemble de points sur un plan en deux dimensions. On s'intéresse ainsi à l'ensemble des points (x, y) solutions de l'équation cubique $A.x^3 + B.x^2.y + C.x.y^2 + D.y^3 + E.x^2 + F.x.y + G.y^2 + H.x + I.y + J = 0$ pour des constantes $A, B, C, D, E, F, G, H, I, J$ fixées.

Comme cette forme ne garantit pas l'unicité d'une seule équation par courbe, elle est rarement utilisée en pratique, et en procédant à des changements de variables, on trouve les équations simplifiées de Weierstrass. En se restreignant à certaines courbes aux caractéristiques intéressantes, on obtient aussi les équations normalisées de Montgomery et d'Edwards :

Nom de l'équation	Équation
Équation longue de Weierstrass	$y^2 + a.x.y + c.y = x^3 + b.x^2 + d.x + e$
Équation courte de Weierstrass	$y^2 = x^3 + a.x + b$
Équation de Montgomery	$b.y^2 = x^3 + a.x^2 + x$
Équation d'Edwards	$x^2 + y^2 = 1 + a.x^2.y^2$ ou $x^2 + y^2 = a^2.(1 + b.x^2.y^2)$

On prendra bien soin que la courbe n'ait pas de singularité (points doubles ou points de rebroussement), sinon les caractéristiques attendues ne sont pas au rendez-vous. À ce titre, il faut veiller à ce que ce qu'on appelle le discriminant de la courbe soit non nul. Pour l'équation courte de Weierstrass, le discriminant est égal à $-16.(4.a^3 + 27.b^2)$.

On ajoute à cet ensemble un point fictif appelé « point à l'infini », situé arbitrairement loin de la courbe, noté O. Le tout forme un groupe au sens mathématique du terme (**https://fr.wikipedia.org/wiki/Groupe_(math%C3%A9matiques)**) sur lequel on définit une opération d'addition de deux points. En effet, en traçant une droite reliant deux points quelconques sur cette courbe réelle, on intersecte toujours la courbe

en un troisième point. On prend le symétrique de ce point par rapport à l'axe des abscisses pour définir le point résultat de l'addition (voir figure 1). Par extension, l'addition d'un point avec lui-même (appelée doublement) se fait en traçant la tangente en ce point.

L'équivalent de la multiplication dans ce groupe sera l'addition de points et l'équivalent de l'élévation à la puissance, la multiplication d'un point par un entier (l'addition multiple du point avec lui-même). Ainsi, on notera *8. P* le point *P + P + P + P + P + P + P + P*. On peut calculer algébriquement le point résultat à l'aide des formules de la figure 2. Remarquons qu'on peut utiliser les principes de l'exponentiation binaire et calculer *23. P = 1. P + 2. P + 4. P + 16. P* par calcul et addition des doubles successifs utiles.

Il est bien plus intéressant de considérer maintenant l'équation de la courbe elliptique modulo un nombre premier *p*, et de retenir donc uniquement les solutions *(x, y)* modulo *p*. Pourquoi ? Car le nombre d'éléments d'un tel groupe est bien plus diversifié que celui d'un groupe multiplicatif comme *Z / p Z* avec *p* premier (toujours égal à *p – 1*), ce qui nous assure des propriétés très intéressantes. Le nombre d'éléments de ce groupe est d'ailleurs appelé l'ordre de la courbe.

De nombreuses courbes elliptiques ont été étudiées et certaines ont d'ailleurs été normalisées dans des standards, comme celui du NIST américain (*National Institute of Standards and Technology*) ou du SECG (*Standards for Efficient Cryptography Group*). OpenSSL possède d'ailleurs une base de données de quelques courbes répandues, avec lesquelles il sait calculer :

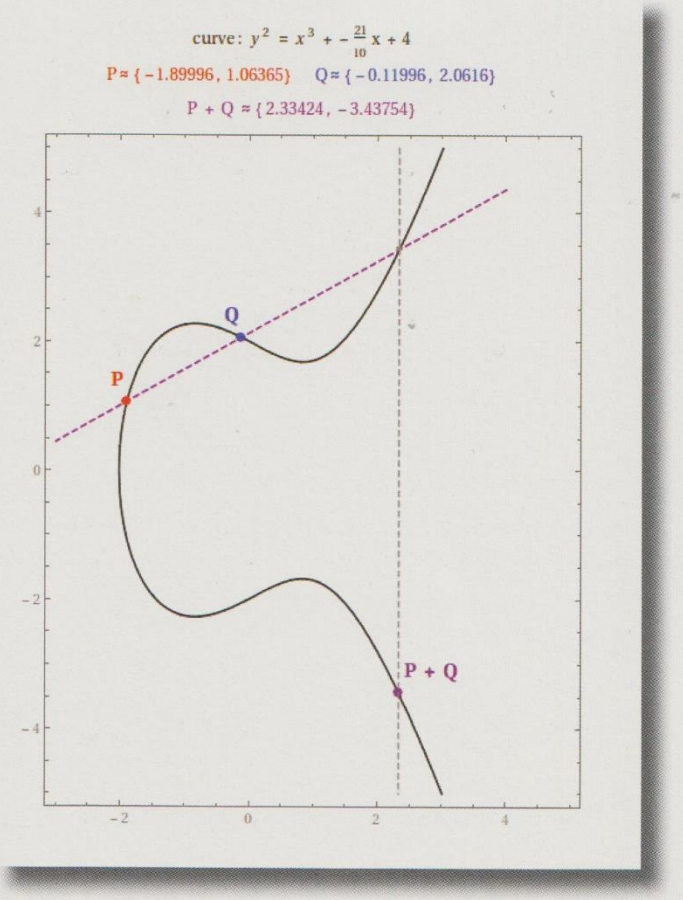


Fig. 1 : Représentation d'une courbe elliptique et addition géométrique de 2 points.

Soit $P : (x_1, y_1)$ et $Q : (x_2, y_2)$ deux points sur la courbe elliptique E d'équation $y^2 = x^3 + ax + b$ avec $4a^3 + 27b^2 \neq 0$.

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

alors $R = P + Q : (x_3, y_3)$ est défini par :

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_3 - x_1) + y_1 \end{cases}$$

Fig. 2 : Addition algébrique de 2 points sur une courbe elliptique.