Introduction aux courbes elliptiques
Cours 2 - Polynômes de degré 3 et courbes elliptiques

2019/2020 - A. RIDARD

A propos de ce document

- Pour naviguer dans le document, vous pouvez utiliser :
  - le menu (en haut à gauche)
  - les différents liens
- Pour signaler une erreur, vous pouvez envoyer un message à l'adresse suivante : anthony.ridard@univ-ubs.fr

Plan du cours

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 :
$$a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = a_n(X - z_1)(X - z_2)\ldots(X - z_n)$$

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 $a_nX^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0$, 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 $\Delta = 0$

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 $\sigma_1 = z_1 + z_2 + z_3$, $\sigma_2 = z_1 z_2 + z_1 z_3 + z_2 z_3$ et $\sigma_3 = z_1 z_2 z_3$.
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 :

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

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

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.

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