

① COURBES ELLIPTIQUES

K corps parfait

$\bar{K}$ une clôture algébrique de K

Définition. Une courbe elliptique sur K est une courbe projective lisse E de genre 1 définie sur K munie d'un K -point $O \in E(K)$.

Exemple: Pour tout $\lambda \in K - \{0, 1\}$,

$$E_\lambda = \{[x:y:z] \in \mathbb{P}^2 \mid y^2z = x(x-z)(x-\lambda z)\}$$

est une courbe elliptique avec $O = [0:1:0]$.

Non-exemples:

(1) L'équation $y^2z = x^3$ ne définit pas une courbe elliptique car cette courbe a un point singulier $[0:0:1]$

(2) La courbe projective lisse de genre 1 définie



sur $\mathbb{Q}$ donnée par

$$C = \{ [x:y:z:t] \in \mathbb{P}^3 \mid \begin{cases} y^2 t^2 = x^4 - t^2 \\ zt = x^2 \end{cases} \}$$

n'est pas une courbe elliptique car elle n'a pas de $\mathbb{Q}$ -points : $C(\mathbb{Q}) = \emptyset$.

(3) La courbe projective lisse

$$C = \{ [x:y:z] \in \mathbb{P}^2 \mid x^5 + y^5 = z^5 \}$$

a des points $C(\mathbb{Q})$, par exemple $[0:1:1]$, mais n'est pas une courbe elliptique car elle est de genre 5.

Proposition. Soit $(E, 0)$ une courbe elliptique sur k . L'application dite d'Abel-Jacobi

$$AJ: E(\bar{k}) \longrightarrow \text{Pic}^0(E)$$

$$P \longmapsto \text{classe de } [P] - [0]$$

est une bijection $\text{Gal}(\bar{k}/k)$ -équivariante.

Démonstration. Le point 0 appartient à $E(k) = E(\bar{k})^{\text{Gal}(\bar{k}/k)}$ par définition,

d'où, pour tout $\sigma \in \text{Gal}(\bar{k}/k)$,

$$\begin{aligned} AJ(\sigma(P)) &= [\sigma(P)] - [0] = \sigma([0]) \\ &= \sigma([P] - [0]) \\ &= \sigma(AJ(P)), \end{aligned}$$

c'est-à-dire l'application d'Abel-Jacobi est $\text{Gal}(\bar{k}/k)$ -équivariante.

- Injectivité: soient $P, Q \in E(\bar{k})$ avec $AJ(P) = AJ(Q)$. Alors $[P] - [Q] = 0$ dans $\text{Pic}^0(E)$, ce qui signifie qu'il existe $f \in \bar{k}(E)^\times$ avec

$$\text{div}(f) = [P] - [Q] \geq -[Q].$$

La dernière inégalité implique $f \in \mathcal{L}([Q])$.

Par le théorème de Riemann-Roch,

$$l([Q]) - l(\underbrace{K_E}_{\deg = -1} - [Q]) = \underbrace{\deg [Q]}_1,$$

d'où $l([Q]) = 1$. Mais $\mathcal{L}([Q])$ contient

déjà toutes les fonctions constantes $\bar{k}$, donc $f \in \bar{k}^*$, ce qui veut dire $P = Q$.

• Surjectivité: Soit D un diviseur de degré 0. Par Riemann-Roch,

$$l([0] + D) - l(\cancel{K_E} - [0] - D) = \deg([0] + D)$$

d'où $l([0] + D) = 1$. Soit donc

$f \in \mathcal{L}([0] + D)$ non nulle.

Comme $\text{div}(f) + D + [0] \geq 0$ est effectif de degré 1, il existe un point $P \in E(\bar{k})$ tel que

$$\text{div}(f) + D + [0] = [P],$$

autrement dit

$$\text{div}(f) = D - ([P] - [0]),$$

c'est-à-dire la classe de D dans $\text{Pic}^0(E)$ est égale à $AJ(P)$ $\square$

Théorème. Soit E une courbe elliptique définie sur k . Alors:

(1) Il existe des fonctions $x, y \in k(E)$ induisant un isomorphisme entre E et une courbe d'équation dite de Weierstrass

$$y^2z + a_1xy^2 + a_3y^3 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

avec $a_1, a_2, a_3, a_4, a_6 \in k$ qui envoient le point O sur le point $[0:1:0]$.
(Ici $x = \frac{X}{Z}$ et $y = \frac{Y}{Z}$).

(2) Deux telles équations définissent des courbes elliptiques isomorphes si et seulement si l'on peut passer de l'une à l'autre par un changement de variables de la forme

$$\begin{cases} x' = u^2x + r \\ y' = u^3y + u^2sx + t \end{cases}$$

avec $u, v, s, t \in k$ et $u \neq 0$.

Démonstration. On considère les espaces $\mathcal{L}(n[0])$ pour $n=1, 2, 3, \dots$. Par le théorème de Riemann-Roch,

$$l(n[0]) - l(K_E - n[0]) = \deg(n[0]),$$

d'où $l(n[0]) = n$. Comme le diviseur $n[0]$ est défini sur k , l'espace $\mathcal{L}(n[0])$ admet une base finie d'éléments de $k(E)^X$. Il existe donc des fonctions $x, y \in k(E)^X$ telles que

$\{1, x\}$ est une base de $\mathcal{L}(2[0])$

$\{1, x, y\}$ est une base de $\mathcal{L}(3[0])$,

ce qui implique nécessairement

$$\text{ord}_0(x) = -2$$

$$\text{ord}_0(y) = -3$$

L'espace $\mathcal{L}(6[0])$, de dimension 6, contient les 7 fonctions

(4)

$$1, x, y, x^2, xy, y^2, x^3$$

et donc il existe une relation linéaire

$$0 = A_1 + A_2 x + A_3 y + A_4 x^2 + A_5 xy + A_6 y^2 + A_7 x^3$$

à coefficients $A_1, \dots, A_7 \in K$. Comme les ordres d'annulation

$$\text{ord}_0(1) = 0$$

$$\text{ord}_0(x) = -2$$

$$\text{ord}_0(y) = -3$$

$$\text{ord}_0(x^2) = -4$$

$$\text{ord}_0(xy) = -5$$

$$\text{ord}_0(y^2) = \text{ord}_0(x^3) = -6$$

sont tous distincts, on a $A_6, A_7 \neq 0$

(sinon on aurait une relation de dépendance linéaire entre fonctions ayant des pôles d'ordre différent de 0).

En remplaçant x par $-A_6 A_7 x$
 y par $A_6 A_7^2 y$

et en divisant par $A_6^3 A_7^4$, on trouve

$$0 = \underbrace{\frac{A_1}{A_6^3 A_7^4}}_{-a_6} - \underbrace{\frac{A_2}{A_6^2 A_7^3}}_{a_4} x + \underbrace{\frac{A_3}{A_6^2 A_7^2}}_{a_3} y + \underbrace{\frac{A_4}{A_6^2 A_7^2}}_{-a_2} x^2 - \underbrace{\frac{A_5}{A_6 A_7}}_{-a_1} xy + y^2 - x^3,$$

ce qui donne une équation de la forme

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

• L'application

$$\varphi: E \setminus \{0\} \longrightarrow \mathbb{P}^2$$

$$P \longmapsto [x(P) : y(P) : 1]$$

s'étend en un morphisme de courbes algébriques

$$\varphi: E \longrightarrow C \subset \mathbb{P}^2$$

$$y^2 z + a_1 x y z + a_3 y z^3 = \dots$$

qui envoie 0 sur $[0:1:0]$.

- Il faut maintenant démontrer que $\varphi: E \rightarrow \mathbb{C}$ est de degré 1, c'est-à-dire l'égalité des corps de fonctions

$$K(E) = K(x, y)$$

Pour cela, on regarde les degrés des extensions intermédiaires

$$\begin{array}{c}
 K(E) \\
 \cup \\
 K(x, y) \\
 \swarrow \quad \searrow \\
 K(x) \quad K(y) \\
 \swarrow \quad \searrow \\
 K
 \end{array}$$

On a $[K(E):K(x)] = 2$ car le seul pôle de $x: E \rightarrow \mathbb{P}^1$ est d'ordre 2 en 0, et de même $[K(E):K(y)] = 3$ car le seul pôle de $y: E \rightarrow \mathbb{P}^1$ est d'ordre 3 en 0. Comme

$$2 = [K(E):K(x, y)] [K(x, y):K(x)]$$

$$3 = [K(E):K(x, y)] [K(x, y):K(y)]$$

et que 2 et 3 sont premiers entre eux,
on en déduit $[K(E): K(x, y)] = 1$.

- La courbe C est lisse. En effet, elle n'est pas singulière en $O = [0:1:0]$ car si F désigne le polynôme homogène qui la définit, on a $\frac{\partial F}{\partial z}(O) = 1$. Si elle est singulière, quitte à faire une translation on peut supposer qu'elle est singulière en $(0, 0)$ et le critère jacobien donne alors que l'équation affine est de la forme

$$y^2 + a_1 xy - a_2 x^2 - x^3 = 0$$

Mais dans ce cas la fonction
rationnelle $C \longrightarrow \mathbb{P}^1$ est de
 $(x, y) \longmapsto [x:y]$

degré 1 car elle admet l'inverse

$$[1:t] \longmapsto (t^2 + a_1 t - a_2, t^3 + a_1 t^2 - a_2 t)$$

En effet, on vérifie par un calcul

⑥

direct que $(t^2 + a_1 t - a_2, t^3 + a_1 t^2 - a_2 t)$ est dans la courbe et les relations

$$\left(\frac{y}{x}\right)^2 + a_1 \left(\frac{y}{x}\right) - a_2 = \frac{x^3}{x^2} = x$$

$$\left(\frac{y}{x}\right)^3 + a_1 \left(\frac{y}{x}\right)^2 - a_2 \left(\frac{y}{x}\right) = \frac{y x^3}{x^3} = y$$

Mais alors la composition

$$E \longrightarrow C \longrightarrow \mathbb{P}^1$$


est une application de degré 1 entre courbes projectives lisses, d'où $E \cong \mathbb{P}^1$, ce qui est absurde car E est de genre 1. on en déduit que C est lisse, puis que $E \xrightarrow{\sim} C$ est un isomorphisme, ce qui finit la preuve de (1).

(2) Étant donnée une autre équation de Weierstrass, les fonctions $\{1, x', y'\}$ forment une base de $\mathcal{L}(3[0])$ avec $x' \in \mathcal{L}(2[0])$ et il existe donc

$\lambda, \mu, r, s, t \in K$ tels que

$$x' = \lambda x + r \quad \text{avec } \lambda, \mu \neq 0$$

$$y' = \mu y + s x + t$$

Pour que les coefficients de x'^3 et y'^2 soient égaux, il faut $\lambda^3 = \mu^2$, c'est-à-dire en posant $\mu = \frac{\lambda^3}{\lambda}$, on a $\lambda = \mu^2$ et $\mu = \mu^3$, ce qui démontre (2) $\square$

Remarque. Si $\text{car}(K) \neq 2$, en remplaçant y par $\frac{1}{2}(y - a_1 x - a_3)$ on obtient l'équation

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$$

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

Si $\text{car}(K) \neq 3$, on peut éliminer le terme en x^2 avec

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108} \right)$$

pour obtenir une équation de la forme

$$y^2 = x^3 - 27c_4 x - 54c_6$$

$$\text{avec } \begin{cases} c_4 = -b_2^3 + 36b_2b_4 - 216b_6 \\ c_6 = b_2^2 - 24b_4 \end{cases}$$

équation de Weierstrass courte

Remarque: Toute équation de Weierstrass non singulière comme dans le théorème définit une courbe elliptique sur K , munie du point $[0:1:0]$. En effet, la forme différentielle

$$w = \frac{dx}{2y + a_1x + a_3} \in \Omega_C$$

a diviseur $\text{div}(w) = 0$, d'où $g = 1$.

② LA LOI DE GROUPE

En utilisant la bijection

$$E(K) \longrightarrow \text{Pic}^0(E),$$

on définit la somme de deux points

$P, Q \in E(K)$ comme le seul point

$P+Q \in E(\bar{K})$ tel que

$$\underbrace{[P+Q] - [0]}_{AJ(P+Q)} = \underbrace{[P] - [0]}_{AJ(P)} + \underbrace{[Q] - [0]}_{AJ(Q)}$$

cl est à dire

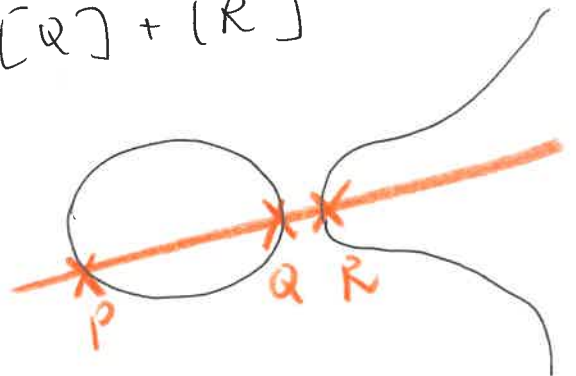
$$[P+Q] \sim [P] + [Q] - [0]$$

Proposition. Soient $P, Q, R \in E(\bar{K})$.

Alors $P+Q+R = 0$ si et seulement si
il existe une droite $L \subset \mathbb{P}^2$ telle

$$\text{que } L \cap E = [P] + [Q] + [R]$$

↑
intersection
avec multiplicité



Démonstration: Si $P+Q+R = 0$, alors

$$[0] \sim [P+Q+R] \sim [P] + [Q] + [R] - 2[0],$$

donc il existe $f \in \bar{K}(E)^{\times}$ telle que

$$\text{div}(f) = [P] + [Q] + [R] - 3[0].$$

Une telle fonction appartient à $\mathcal{L}(3[0])$

(8)

et s'écrivent donc $f = ax + by + c$. Soit $L \subset \mathbb{P}^2$ la droite d'équation $aX + bY + cZ = 0$. Pour un point $s \in L \cap E$ différent de O , la multiplicité de s est $\text{ord}_s(f)$, tandis que pour $s = O$ la multiplicité est $\text{ord}_O(f) + 3$, d'où

$$\begin{aligned} L \cap E &= \text{div}(f) + 3[O] \\ &= [P] + [Q] + [R] \end{aligned}$$

Réciproquement, si L est la droite d'équation $aX + bY + cZ = 0$, en posant $f = ax + by + c$, on a d'un côté

$$L \cap E = \text{div}(f) + 3[O]$$

et de l'autre $L \cap E = [P] + [Q] + [R]$, d'où l'égalité $P + Q + R = O$ selon la loi de groupe définie sur $E(\bar{k})$ $\square$

Théorème. Soit E une courbe elliptique définie sur k . La loi de groupe

$$E \times E \longrightarrow E$$

est un morphisme de k -unités.

Rappelons que E admet une équation de Weierstrass

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

Lemme 1 : Si $P = (x_0, y_0)$ est un point de $E \setminus \{O\}$, alors $-P = (x_0, -y_0 - a_1 x_0 - a_3)$.

Démonstration. Soit $O = aX + bY + cZ$ l'équation de la droite $L \subset \mathbb{P}^2$ passant par P et O . Comme elle passe par $O = [0:1:0]$, on a $b = 0$ et comme elle passe par $P = [x_0:y_0:1]$, on a $a x_0 + c = 0$. On peut alors choisir $a = 1$ et $c = -x_0$. Comme $-P$ est un point de L , sa première coordonnée est x_0 . La deuxième coordonnée est donc une valeur y'_0 de

$$y^2 + (a_1 x_0 + a_3) y - x_0^3 - a_2 x_0^2 - a_4 x_0 - a_6$$

et comme $y_0 + y'_0 = -a_1 x_0 - a_3$, on

trouve $y'_0 = -y_0 - a_1 x_0 - a_3$ □

lemme 2

(1) L'application $E \rightarrow E$ définit
 $P \mapsto -P$

un automorphisme involutif sur k
 de la variété E .

(2) Pour tout point $Q \in E(\bar{k})$, l'application de translation $E \rightarrow E$ définit
 $P \mapsto P + Q$

un automorphisme de variétés, qui est
 défini sur k si le point Q l'est.

Démonstration: Commençons par le fait
 général suivant: pour $P, Q \in E(\bar{k})$,
 l'espace $\mathcal{L}([P] + [Q])$ est de dimension 2
 par Riemann-Roch, et il existe donc
 $f \in \mathcal{L}([P] + [Q])$ non constante. Cette
 fonction a des pôles simples en P et Q
 car $\mathcal{L}([P]) = \mathcal{L}([Q]) = k$. En particulier,
 le morphisme associé $\varphi_f: E \rightarrow \mathbb{P}^1$ satisfait

$$\varphi_f^*([\infty]) = [P] + [Q]$$

et est donc de degré 2. L'extension

$$\bar{k}(f) \subset \bar{k}(E)$$

est séparable car $\sin$ on aurait
 $\bar{k}(E) = \bar{k}(f^{1/2})$ et $E \cong \mathbb{P}^1$. L'extension
est donc galoisienne et $\text{Gal}(\bar{k}(E)/\bar{k}(f))$
est engendré par un élément $\sigma_{f, \alpha}^*$ d'ordre 2.
Puisque E est projective lisse, par la
correspondance entre courbes et corps de
fractions, il existe $\sigma = \sigma_{f, \alpha}$ automorphisme
non trivial de la variété induisant $\sigma_{f, \alpha}^*$
sur les corps de fractions. L'action
de σ sur chaque fibre de $\varphi_f: E \rightarrow \mathbb{P}^1$
est transitive. En effet, soit

$$\varphi_f^{-1}(t) = \{R, S\} \quad R \neq S$$

et soient r et s des uniformisantes
en R et S . Si $\sigma(R) = R$, alors

$$\text{ord}_R(\sigma(r)) = 1 \quad \text{ord}_S(\sigma(r)) = 0,$$

$$\text{donc } \text{ord}_R(r\sigma(r)) = 2 \quad \text{ord}_S(r\sigma(r)) = 0,$$

ce qui est absurde car $r\sigma(r) \in \bar{k}(E)$

et donc $\text{ord}_{\varphi_f(R)}(\sigma(h)) = e_R(\varphi_f)^{-1} \text{ord}_R(\sigma(h))$
 $= e_S(\varphi_f)^{-1} \text{ord}_S(\sigma(h)).$

on obtient $\sigma(R) = S$

La fonction $f - f(R) \in k(f)$ possède un zéro en R , donc aussi en $\sigma(R)$, et des pôles simples en P et Q . On a

$$\text{div}(f - f(R)) = [R] + [\sigma(R)] - [P] - [Q],$$

donc $[R] + [\sigma(R)] \sim [P] + [Q].$

(1) Appliquée à $P=Q=O$, cette relation donne $\sigma(R) = -R.$

(2) Appliquée à $P=O$, cette relation

donne $\sigma_{O,Q}(R) = P - R$, et donc

l'application de translation est un isomorphisme de variétés algébriques $\square$