

Rapports I. Soit $(E, \mathcal{O})$ une courbe elliptique. L'application d'Abel-Jacobi:

$$E \longrightarrow \mathbb{P}^2(\mathbb{C}), \quad P \longmapsto [P] - [\mathcal{O}]$$

est un isomorphisme.

Par transport de structure, on en a déduit une loi de groupe sur les points de E .

II. Il existe un plongement $\iota: E \longrightarrow \mathbb{P}_k^2$ dont l'image est la courbe définie par une équation de Weierstrass:

$$(W): \quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

envoyant $\mathcal{O}$ sur le point $[0:1:0]$.

De plus, les fonctions $x = \frac{X}{Z}$ et $y = \frac{Y}{Z}$ sont tels que

$$\bullet \quad (1, x) \text{ soit une base de } \mathcal{L}(2[\mathcal{O}])$$

$$(1) \quad \bullet \quad (1, x, y) \text{ soit une base de } \mathcal{L}(3[\mathcal{O}])$$

L'objectif de ce cours est de démontrer que la loi de groupe

$$E \times E \longrightarrow E$$

est un morphisme de k -variétés.

Proposition: Soient $P, Q, R \in E$. Les assertions suivantes sont équivalentes:

(i) On a $P+Q+R = \mathcal{O}$.

(ii) Il existe une droite $L \subset \mathbb{P}^2$ par laquelle

$$[L \cap E] = [P] + [Q] + [R]$$

(diviseur des points d'intersection, compte avec multiplicités)

Démonstration: Montrons (i) $\Rightarrow$ (ii). Si $P+Q+R = \mathcal{O}$, alors il existe $f \in k(E)^\times$

$$\text{vérifiant } (f) = [P] - [\mathcal{O}] + [Q] - [\mathcal{O}] + [R] - [\mathcal{O}] = [P] + [Q] + [R] - 3[\mathcal{O}].$$

Une telle fonction s'annule en P, Q, R et appartient à $\mathcal{L}(3[\mathcal{O}])$.

Par (1), on peut l'écrire $f = ax + by + c$ ($a, b, c \in k$)

Soit $L \subset \mathbb{P}^2$ la droite d'équation $aX + bY + cZ = 0$. On prétend que L fait le job.

On calcule le diviseur d'intersection:

• Si $S \in E \setminus \{\mathcal{O}\}$, alors on "déhomogénéise" (W) en Z (i.e. on pose $x = \frac{X}{Z}, y = \frac{Y}{Z}$) pour obtenir:

$$E \setminus \{\mathcal{O}\}: y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

$$L \setminus \{Z=0\}: f = ax + by + c = 0$$

L'anneau des fonctions régulières sur cette intersection correspond à

$$k[x, y] / (f, y^2 + a_1xy + a_3y - \dots)$$

En localisant en un point S de $E \setminus \{\mathcal{O}\}$, on obtient $\mathcal{O}_S / (f)$

le diviseur $[L \cap E]$ sur l'hypersurface $\{Z \neq 0\}$ est donc de la forme

$$\sum_{S \in E \setminus \{\mathcal{O}\}} \text{ord}_S(f) \cdot [S]$$

• Si $S = \mathcal{O}$, alors on "déhomogénéise" (W) en Y (i.e. on pose $u = \frac{X}{Y}, v = \frac{Z}{Y}$) pour obtenir:

$$E \setminus \{Y=0\}: v + a_1uv + a_3v^3 - u^3 - a_2u^2v - a_4uv^2 - a_6v^3 = 0$$

$$L \setminus \{Y=0\}: au + b + cv = 0$$

L'anneau des fonctions régulières sur l'intersection correspond à

$$(2) \quad k[u, v] / (au + b + cv, v + a_1uv + a_3v^3 - \dots)$$

$$\text{Or } au + b + cv = a\left(\frac{X}{Y} \cdot \frac{Y}{Z}\right) + b + c\left(\frac{Z}{Y}\right) = a\frac{X}{Y} + b + \frac{c}{Y} = Y^{-1}f, \text{ donc (2)}$$

se résout:

$$(2)' \quad k[u, v] / (Y^{-1}f, v + a_1uv + a_3v^3 - \dots)$$

En localisant en $\mathcal{O}$, on trouve que le diviseur $[L \cap \iota(E)]$ est supporté

en $\mathcal{O}$, de contribution $\text{ord}_{\mathcal{O}}(Y^{-1}f) \cdot [\mathcal{O}]$

$$\text{Au total: } [L \cap E] = \sum_{S \in E} \text{ord}_S(f) \cdot [S] - \text{ord}_{\mathcal{O}}(y)$$

$$= [P] + [Q] + [R] - 3[\mathcal{O}] + 3[\mathcal{O}]$$

$$= [P] + [Q] + [R] \quad \text{ce que l'on cherchait.}$$

Réciproquement, montrons (ii) $\Rightarrow$ (i). Il existe une telle droite, notons son équation:

$$aX + bY + cZ = 0$$

De même, posons $f = ax + by + c$. Le même calcul que celui effectué ci-dessus

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

$$= [P] + [Q] + [R] \quad \text{d'après (2).}$$

d'où l'égalité $\text{div}(f) = [P] + [Q] + [R] - 3[\mathcal{O}]$ ce qui assure $P+Q+R = \mathcal{O}$. $\square$

Théorème: La loi de groupe $E \times E \longrightarrow E$ est un morphisme de k -variétés.

On commence par deux lemmes pour préparer le terrain.

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

De plus, y_0 et y_0' sont racines d'un polynôme de la forme

$$Y^2 + (a_1x_0 + a_3)Y + \text{terme de degré } 0.$$

Démonstration: Soit $0 = aX + bY + cZ$ l'équation de la droite L dans $\mathbb{P}^2$

passant par P et $\mathcal{O}$. Comme elle passe par $\mathcal{O}$ on a $b = 0$, et

comme elle passe par P , on a $ax_0 + c = 0$. On peut alors choisir

$$a = 1 \text{ et } c = -x_0. \text{ Ainsi } L: X - x_0 = 0.$$

Comme $-P$ est un point de L , sa première coordonnée est x_0 .

Par le second assertion, il suffit de considérer l'équation de Weierstrass. $\square$

Lemme 2: (i) L'application inverse $E \longrightarrow E, R \longmapsto -R$ est ses-jacente

à un automorphisme involutif et défini sur k de la variété E .

(ii) Pour tout $Q \in E$, l'application de translation

$$E \longrightarrow E, \quad R \longmapsto R + Q$$

est ses-jacente à un automorphisme de variétés, qui est défini

sur k si Q l'est.

Démonstration: On commence par un fait général: si P et Q sont deux points

de E (éventuellement égaux), alors $[P] + [Q]$ est un diviseur de degré $2 \geq 2g-1$

et donc $\mathcal{L}([P] + [Q])$ est de dimension 2. On peut donc trouver $f \in \mathcal{L}([P] + [Q])$

non constante. Comme $\mathcal{L}([P]) = \mathcal{L}([Q]) = k$, on remarque que f a bien

un pôle simple en P et Q .

En particulier, le morphisme $\phi_f: E \longrightarrow \mathbb{P}_k^1$ est tel que

$$\phi_f^*([\infty]) = \text{diviseur polaire de } f = [P] + [Q]$$

le morphisme ϕ_f est donc de degré 2. Il est aussi séparable car son

$$k(E) = k(f^{1/2}) \text{ et } 1 = g(E) = g(\mathbb{P}^1) = 0. \text{ Ainsi, } \phi_f \text{ est Galois}^*$$

* Une extension de degré 2 séparable est nécessairement normale car

la conjugaison correspond à l'opposée.

• Comme la catégorie des corps de fonctions sur k équipée des extensions de

corps est catégoriquement équivalente à la catégorie des courbes projectives lisses équipées

des morphismes de variétés, l'élément non trivial $\sigma \in \text{Gal}(k(E)/k(f))$

provient d'un automorphisme $\sigma_{P,Q}$ de E en tant que k -variété.

• Comme ϕ_f est galoisien, l'action de $\sigma_{P,Q}$ agit transitivement sur les fibres de

$$\phi_f. \text{ Ainsi: } \sigma(P) = Q.$$

Soit $R \in E \setminus \{P, Q\}$.

La fonction $f - f(R) \in k(f)$ possède un zéro en R , donc aussi en $\sigma(R)$, et comme

seules pôles de simples en P et en Q . Comme $\deg(f - f(R)) = 0$, on trouve:

$$(*) \quad \text{div}(f - f(R)) = [R] + [\sigma(R)] - [P] - [Q] \sim 0.$$

(i) Si l'on applique (*) à $P = Q = \mathcal{O}$, on trouve $\sigma_{\mathcal{O}, \mathcal{O}}(R) = -R$ pour tout

$R \in E \setminus \{\mathcal{O}\}$.

(ii) Si l'on applique (*) à $P = \mathcal{O}$ et Q comme dans l'énoncé, on trouve

$$\sigma_{\mathcal{O}, Q}(R) = Q - R = -t_Q(R) \text{ et donc } t_Q = \sigma_{\mathcal{O}, \mathcal{O}} \circ \sigma_{Q, Q} \circ \sigma_{\mathcal{O}, \mathcal{O}} \square$$

On est prêt à démontrer le théorème principal.

Démonstration du théorème: Dans un premier temps, on considère deux points

$P, Q \neq \mathcal{O}$ tels que $P \neq \pm Q$.

• Comme $P \neq Q$, la droite (PQ) est bien définie et elle ne contient pas $\mathcal{O}$

car sinon $P = -Q$. En particulier, en écartant $R = [x(R):y(R):z(R)]$

on a $z(P), z(Q) \neq 0$ que l'on peut donc supposer $= 1$.

• Soit $(PQ): aX + bY + cZ = 0$ l'équation de cette droite dans $\mathbb{P}^2$.

$$\text{En écartant } ax(P) + by(P) + c = ax(Q) + by(Q) + c = 0$$

on va trouver, par exemple,

$$a = y(P) - y(Q), \quad b = x(P) - x(Q) \text{ et } c = x(Q)y(P) - x(P)y(Q)$$

Comme $\mathcal{O} \notin (PQ)$, $[0:1:0]$ n'est pas solution, et donc $b \neq 0$.

• Si $(x, y, 1)$ est un point de l'intersection entre la courbe E et la

droite (PQ) , alors en substituant (3) $y_0 = -\frac{a}{b}x_0 - \frac{c}{b}$ dans l'équation

de Weierstrass admette, on trouverait un polynôme de degré 3:

$$(4) \quad 0 = x_0^3 + (a_2 - \frac{a^2}{b^2} + \frac{a}{b}a_1)x_0^2 + \text{terme de degré } \leq 1$$

les seuls tels points étant P, Q et $-(P+Q)$, on trouverait comme

solutions de (4) $x(P), x(Q)$ et $x(-(P+Q)) = x(P+Q)$ d'après le

lemme 1. Comme le second coefficient d'un polynôme unitaire n'est autre que

la somme de ses racines, on trouve:

$$(5) \quad x(P+Q) = -a_2 + \frac{(y(P) - y(Q))^2}{(x(P) - x(Q))^2} + a_1 \frac{y(P) - y(Q)}{x(P) - x(Q)} - x(P) - x(Q)$$

En utilisant (3), on trouve aussi:

$$y(-(P+Q)) = \frac{y(P) - y(Q)}{x(P) - x(Q)} x(P+Q) - \frac{y(P)x(Q) - y(Q)x(P)}{x(P) - x(Q)}$$

Le lemme 1 donne aussi $y(P+Q) + y(-(P+Q)) = a_1x(P+Q) + a_3$

d'où l'on tire

$$(6) \quad y(P+Q) = -\left(a_1 + \frac{y(P) - y(Q)}{x(P) - x(Q)}\right)x(P+Q) - a_3 + \frac{y(P)x(Q) - y(Q)x(P)}{x(P) - x(Q)}$$

• Les équations (5) & (6) donne alors que

$$U \longrightarrow E, \quad (P, Q) \longmapsto P+Q$$

est algébrique, où $U \subset E \times E$ est l'ouvert de Zariski

$$U := \{(P, Q) \in E \setminus \{\mathcal{O}\} \times E \setminus \{\mathcal{O}\} \mid P \neq \pm Q\}$$

• Par traiter le cas général, on observe que $P+Q = t_{-R}(t_R(P) + Q)$

et donc que la loi de groupe est donnée par

$$t_{-R} \circ \oplus \circ (t_R \times \text{id})$$

sur l'ouvert $V_R := (t_R \times \text{id})^{-1}(U)$. Les V_R recouvrent $E \times E$, et donc

l'addition est bien donnée par un morphisme sur $E \times E$. $\square$

Exemple: On considère la courbe elliptique $E/\mathbb{Q}$ d'équation affine:

$$E: y^2 = x^3 + 17$$

1. On vérifie que les points $P_1 = (-2, 3), P_2 = (-1, 4), P_3 = (2, 5), P_4 = (4, 9),$

$P_5 = (8, 23)$ sont bien sur E .

D'autres: $P_6 = (43, 282), P_7 = (52, 375), P_8 = (5234, 378661) \dots$

2. Vérifier que $P_5 = -2 \cdot P_1, P_4 = P_1 - P_3, 3P_1 - P_3 = P_7$.

$$2P_2 = \left(\frac{137}{64}, -\frac{2651}{512}\right), \quad P_2 + P_3 = \left(-\frac{8}{9}, -\frac{109}{27}\right)$$

grâce aux formules (5) et (6).

3. En fait, tout point rationnel peut s'écrire sur la forme

$$P = nP_1 + mP_3 \quad \text{par des } n, m \in \mathbb{Z}.$$

Mieux, $E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}$.