GÉOMÉTRIE ALGÉBRIQUE. — *Isogénies entre courbes elliptiques.*

Note (*) de M. **Jacques Vélu**, transmise par M. Henri Cartan.

Connaissant l'équation d'une courbe elliptique E sur un corps k et les coordonnées des points d'un sous-groupe fini F de E, nous donnons les équations de la courbe isogène E/F et de l'isogénie $f : E \to E/F$.

1. Rappels. — Soit E une courbe elliptique définie sur un corps k que nous supposerons algébriquement clos. A tout point P de E est associée une valuation v_P sur le corps $k(E)$ des fonctions définies sur k, et pour toute fonction $t \in k(E)$ on note $t(P)$ la valeur de t au point P. Si O est un point de E, il existe x et y appartenant à $k(E)$ vérifiant les conditions

$$(1)\qquad \begin{cases} v_O(x) = -2; \quad v_O(y) = -3; \quad \dfrac{y^2}{x^3}(O) = 1; \\ v_P(x) \geqq 0 \quad \text{et} \quad v_P(y) \geqq 0 \quad \text{pour } P \neq O. \end{cases}$$

Ces conditions entraînent que $k(E)$ est égal à $k(x, y)$ et que x et y sont liées par une relation non singulière du troisième degré que l'on peut établir de la façon suivante : posons $z = -x/y$ de sorte que $v_O(z) = 1$; développons x et y

$$(2)\qquad \begin{cases} x = z^{-2} - \alpha_1 z^{-1} - \alpha_2 - \alpha_3 z - \alpha_4 z^2 - \alpha_5 z^3 - \alpha_6 z^4 - \ldots, \\ y = -\dfrac{x}{z} = -z^{-3} + \alpha_1 z^{-2} + \alpha_2 z^{-1} + \alpha_3 + \alpha_4 z + \alpha_5 z^2 + \alpha_6 z^3 + \ldots; \end{cases}$$

alors x et y sont liées par la relation

$$(3)\qquad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

avec

$$(4)\qquad \begin{cases} \alpha_1 = a_1, \quad & \alpha_4 = a_1 a_3 + a_4, \\ \alpha_2 = a_2, \quad & \alpha_5 = a_2 a_3 + a_1^2 a_3 + a_1 a_4, \\ \alpha_3 = a_3, \quad & \alpha_6 = a_1^2 a_4 + a_1^3 a_3 + a_2 a_4 + 2 a_1 a_2 a_3 + a_3^2 + a_6. \end{cases}$$

On a l'habitude de poser

$$(5)\qquad \begin{cases} b_2 = a_1^2 + 4 a_2, \quad b_4 = a_1 a_3 + 2 a_4, \quad b_6 = a_3^2 + 4 a_6, \\ b_8 = a_1^2 a_6 - a_1 a_3 a_4 + 4 a_2 a_6 + a_2 a_3^2 - a_4^2, \quad \text{d'où} \quad 4 b_8 = b_2 b_6 - b_4^2, \\ \Delta = -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6. \end{cases}$$

La non-singularité de la relation (3) se traduit par $\Delta \neq 0$. Réciproquement, si l'on se donne cinq éléments a_1, a_2, a_3, a_4, a_6 de k, tels que $\Delta \neq 0$, l'équation (3) ci-dessus (rendue homogène) définit une courbe elliptique dans $\mathbf{P}_2$, et, si l'on prend pour point O le point à l'infini, les fonctions x et y satisfont aux conditions (1).

Désignons par G le polynôme

$$G(\xi, \eta) = \xi^3 + a_2 \xi^2 + a_4 \xi + a_6 - \eta^2 - a_1 \xi \eta - a_3 \eta;$$

alors la différentielle de première espèce :

$$\omega(x, y) = \frac{dx}{2y + a_1 x + a_3} = \frac{dx}{G'_\xi(x, y)} = \frac{-dy}{G'_\eta(x, y)} = \frac{dy}{3x^2 + 2a_2 x + a_4 - a_1 y},$$

admet le développement

$$\begin{aligned}\omega(x, y) = dz\,[1 + a_1 z + (a_1^2 + a_2) z^2 + (a_1^3 + 2a_1 a_2 + a_3) z^3 \\ + (a_1^4 + 3a_1^2 a_2 + 6a_1 a_3 + a_2^2 + 2a_4) z^4 + \ldots].\end{aligned} \tag{6}$$

2. Isogénies. — Soit F un sous-groupe fini de E et soit f l'isogénie de noyau F de E dans la courbe elliptique $E' = E/F$. Pour tout point P de E on pose $P' = f(P)$. Le corps des fonctions $k(E')$ s'identifie à un sous-corps de $k(E)$. Considérons les fonctions X et Y qui prennent au point P les valeurs

$$\left\{\begin{aligned} X(P) &= x(P) + \sum_{Q \in F - \{0\}} [x(P + Q) - x(Q)]; \\ Y(P) &= y(P) + \sum_{Q \in F - \{0\}} [y(P + Q) - y(Q)]. \end{aligned}\right. \tag{7}$$

Il est clair que X et Y appartiennent à $k(E')$ et que X et Y satisfont à $v_{O'}(X) = -2$; $v_{O'}(Y) = -3$; $Y^2/X^3(O') = 1$; $v_{P'}(X) \geq 0$ et $v_{P'}(Y) \geq 0$ pour $P' \neq O'$. Par conséquent, $k(E')$ est isomorphe à $k(X, Y)$ et l'isogénie f s'identifie à la transformation $(x, y) \mapsto (X, Y)$. On peut écrire X et Y comme fractions rationnelles en x et y, ce sera les « équations » de l'isogénie f, et la relation liant X et Y, sera l'équation de E'.

3. Résultats. — Désignons par F_2 l'ensemble des points d'ordre 2 de $F - \{0\}$, par R une partie de $F - \{0\} - F_2$ telle que

$$F - \{0\} - F_2 = R \cup (-R) \quad \text{et} \quad R \cap (-R) = \emptyset;$$

enfin par S l'union de F_2 et R. L'isogénie f admet les équations

$$\left\{\begin{aligned} X &= x + \sum_{Q \in S} \left[\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2}\right], \\ Y &= y - \sum_{Q \in S} \left[u_Q \frac{2y + a_1 x + a_3}{(x - x_Q)^3} + t_Q \frac{a_1 (x - x_Q) + y - y_Q}{(x - x_Q)^2} + \frac{a_1 u_Q - g_Q^\xi g_Q^\eta}{(x - x_Q)^2}\right], \end{aligned}\right. \tag{8}$$

avec les notations :

$$\left\{\begin{aligned} & Q = (x_Q, y_Q), \\ & g_Q^\xi = \frac{\partial G}{\partial \xi}(x_Q, y_Q) = 3x_Q^2 + 2a_2 x_Q + a_4 - a_1 y_Q, \\ & g_Q^\eta = \frac{\partial G}{\partial \eta}(x_Q, y_Q) = -2y_Q - a_1 x_Q - a_3, \\ & t_Q = \begin{cases} g_Q^\xi & \text{si } Q \in F_2, \\ 2g_Q^\xi - a_1 g_Q^\eta = 6x_Q^2 + b_2 x_Q + b_4 & \text{si } Q \notin F_2, \end{cases} \\ & u_Q = (g_Q^\eta)^2 = 4x_Q^3 + b_2 x_Q^2 + 2b_4 x_Q + b_6. \end{aligned}\right. \tag{9}$$

On obtient ces formules en utilisant les formules d'addition. En effet, si $Q \in F_2$, on a

$$x(P+Q) - x(Q) = \frac{t_Q}{x - x_Q};$$

$$y(P+Q) - y(Q) = -\frac{a_1(x - x_Q) + y - y_Q}{(x - x_Q)^2} t_Q \qquad \text{et} \qquad u_Q = 0,$$

et si $Q \notin F_2$ on a

$$x(P+Q) - x(Q) + x(P-Q) - x(-Q) = \frac{t_Q}{(x-x_Q)^2} + \frac{u_Q}{(x-x_Q)^3},$$

$$\begin{aligned} & y(P+Q) - y(Q) + y(P-Q) - y(-Q) \\ & \quad = -u_Q \frac{2y + a_1 x + a_3}{(x-x_Q)^3} - t_Q \frac{a_1(x-x_Q) + y - y_Q}{(x-x_Q)^2} - \frac{a_1 u_Q - g_Q^x g_Q^y}{(x-x_Q)^2}. \end{aligned}$$

Passons maintenant à la relation liant X et Y. Posons

$$(10) \qquad t = \sum_{Q \in S} t_Q, \qquad w = \sum_{Q \in S} (u_Q + x_Q t_Q).$$

On obtient

$$(11) \qquad \left\{ \begin{array}{l} Y^2 + A_1 XY + A_3 Y = X^3 + A_2 X^2 + A_4 X + A_6, \\ \quad \text{avec} \\ \qquad A_1 = a_1, \qquad A_2 = a_2, \qquad A_3 = a_3, \\ \quad A_4 = a_4 - 5t, \qquad A_6 = a_6 - b_2 t - 7w. \end{array} \right.$$

Pour obtenir cette relation, on reporte (2) dans (8), ce qui donne

$$(12) \qquad \left\{ \begin{array}{l} X = z^{-2} - a_1 z - a_2 - a_3 z \\ \qquad - (\alpha_4 - t) z^2 - (\alpha_5 - a_1 t) z^3 - (\alpha_6 - a_1^2 t - a_2 t - w) z^4 - \ldots, \\ Y = -z^{-3} + a_1 z^{-2} + a_2 z^{-1} + a_3 + (\alpha_4 + t) z + \alpha_5 z^2 + (\alpha_6 + a_1^2 t + 2w) z^3 + \ldots. \end{array} \right.$$

On pose $Z = -X/Y$ et on tire de (12) :

$$(13) \qquad \left\{ \begin{array}{l} Z = z + 2t z^5 + 3 a_1 t z^6 + (4 a_1^2 t + 4 a_2 t + 3w) z^7 + \ldots, \\ z = Z - 2t Z^5 - 3 a_1 t Z^6 - (4 a_1^2 t + 4 a_2 t + 3w) Z^7 + \ldots. \end{array} \right.$$

On reporte à nouveau z dans (12), on trouve

$$\begin{aligned} X = {} & Z^{-2} - a_1 Z^{-1} - a_2 - a_3 Z \\ & - (\alpha_4 - 5t) Z^2 - (\alpha_5 - 5 a_1 t) Z^3 - (\alpha_6 - 9 a_2 t - 6 a_1^2 t - 7w) Z^4 - \ldots, \end{aligned}$$

ce qui donne les formules (11).

Remarques. — 1° On pourrait prendre d'autres fonctions pour jouer le rôle de X et Y. Celles qui ont été choisies sont telles que les uniformisantes Z et z coïncident jusqu'à l'ordre 5, ce qui est le plus grand ordre possible.

2° Si l'on pose $\omega(X, Y) = dX/(2Y + a_1 X + a_3)$, on a $\omega(x, y) = \omega(X, Y)$.

3° Si E est définie sur un sous-corps k_0 de k, si F est séparable sur k_0, et stable par conjugaison sur k_0, la courbe elliptique E/F ainsi que l'isogénie f sont définies de façon naturelle sur k_0, et les formules ci-dessus sont valables sur k_0.

4. Application. — Considérons la courbe elliptique définie sur Q par l'équation

$$y^2 + xy + y = x^3 - x^2 - 3x + 3.$$

Elle a un sous-groupe F d'ordre 7 formé des points O, $Q = (1, 0)$, $2Q = (-1, -2)$, $3Q = (3, -6)$, $4Q = (3, 2)$, $5Q = (-1, 2)$, $6Q = (1, -2)$. On a

$$(14)\quad \left\{\begin{array}{lllll} x_Q = 1, & t_Q = -2, & u_Q = 4, & g^x_Q = -4, & g^y_Q = -2, \\ x_{2Q} = -1, & t_{2Q} = 4, & u_{2Q} = 16, & g^x_{2Q} = 4, & g^y_{2Q} = 4, \\ x_{3Q} = 3, & t_{3Q} = 40, & u_{3Q} = 64, & g^x_{3Q} = 24, & g^y_{3Q} = 8, \\ b_2 = -3, & b_4 = -5, & b_6 = 13, & t = 42, & w = 198, \end{array}\right.$$

la courbe $E' = E/F$ a pour équation $y^2 + xy + y = x^3 - x^2 - 213x - 1257$, et l'isogénie $f : E \to E'$ est donnée en reportant les valeurs (14) dans (8).

(*) Séance du 12 juillet 1971.

3, *Résidence du Parc*,
91-*Palaiseau*,
Essonne.