Partie IV
Courbes elliptiques

Résumé. Cette partie est le coeur de ce rapport. Elle définira ce qu'est une courbe elliptique et le groupe topologique d'une telle courbe. Il sera également montré qu'une courbe elliptique peut s'écrire sous une forme particulière appelée "équations de Weierstrass".

IV.1 Définition

Définition 46. Une *courbe elliptique* est une paire $(E, \mathcal{O})$, où E est une cubique irréductible non singulière et $\mathcal{O} \in E$. La courbe elliptique E est *définie sur un corps* K si E est une courbe sur K et si $\mathcal{O} \in E(K)$.

IV.2 Équations de Weierstrass

Théorème 47. *Si E est une courbe elliptique définie sur un corps K, alors il existe une application*

$$\phi : E(K) \to \mathbb{P}^2(K)$$

qui fournit un isomorphisme de $E(K)$ sur une courbe $C(K)$ donnée par l'équation de Weierstrass

$$C : F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0,$$

où $a_1, \ldots, a_6 \in K$; et tel que $\phi(\mathcal{O}) = (0,1,0)$.

Preuve. Voir section IV.3. □

Pour alléger les notations, nous allons écrire l'équation de Weierstrass en coordonnées non homogènes : $x = X/Z$ et $y = Y/Z$,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{IV.1}$$

plus le point à l'infini $\mathcal{O} = (0,1,0)$. Remarquons que $\mathcal{O}$ est le seul point à l'infini et qu'il n'est pas singulier car $(\partial F/\partial Z)(0,1,0) = 1 \neq 0$. Nous définissons également les quantités suivantes :

$$\begin{gathered} b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6, \\ b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 = b_2^2 - 24b_4 \quad \text{et} \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \end{gathered}$$

Définition 48. Le *discriminant* Δ de l'équation de Weierstrass est la quantité

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6, \tag{IV.2}$$

et le *j-invariant* de la courbe elliptique E est la quantité

$$j(E) = \frac{c_4^3}{\Delta}. \tag{IV.3}$$

Corollaire 49. *Soit un corps K de caractéristique p. Une courbe E définie sur K donnée par une équation de Weierstrass prend alors une forme simplifiée,*

1. *si $p \neq 2$ et $p \neq 3$,*

$$y^2 = x^3 + a_4 x + a_6, \quad \Delta = -16(4a_4^3 + 27a_6^2),$$
$$j(E) = 1728\frac{4a_4^3}{4a_4^3 + 27a_6^2}; \tag{IV.4}$$

2. *si $p = 2$ et si $j(E) \neq 0$,*

$$y^2 + xy = x^3 + a_2 x^2 + a_6, \quad \Delta = a_6, \quad j(E) = 1/a_6; \tag{IV.5}$$

si $p = 2$ et si $j(E) = 0$,

$$y^2 + a_3 y = x^3 + a_4 x + a_6, \quad \Delta = a_3^4, \quad j(E) = 0; \tag{IV.6}$$

3. *si $p = 3$ et si $j(E) \neq 0$,*

$$y^2 = x^3 + a_2 x^2 + a_6, \quad \Delta = -a_2^3 a_6, \quad j(E) = -a_2^3/a_6; \tag{IV.7}$$

si $p = 3$ et si $j(E) = 0$,

$$y^2 = x^3 + a_4 x + a_6, \quad \Delta = -a_4^3, \quad j(E) = 0. \tag{IV.8}$$

Preuve. (i) Si $p \neq 2$, nous pouvons remplaçer y par $(y - \frac{1}{2}(a_1 x + a_3))$. Nous obtenons alors $y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$. De surcroît, si $p \neq 3$, alors nous remplaçons x par $(x - \frac{b_2}{12})$ pour obtenir $y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$.
(ii) L'invariant (en caractéristique 2) de l'équation générale de Weierstrass $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ vaut $j(E) = a_1^{12}/\Delta$. Si $j(E) = 0$, et donc si $a_1 = 0$, alors la substitution $x \leftarrow (x+a_2)$ donne $y^2+a_3y = x^3+(a_2^2+a_4)x+(a_2^3+a_4a_2+a_6)$; sinon, nous remplaçons (x, y) par $((a_1^2x+\frac{a_3}{a_1}), a_1^3y+\frac{a_1^2a_4+a_3^2}{a_1^3})$ pour avoir $y^2 + xy = x^3 + \frac{a_1a_2+a_3}{a_1^3}x^2 + \frac{a_1^4a_4^2+a_3^4+a_1^5a_3a_4+a_1^3a_3^3+a_1^4a_2a_3^2+a_1^6a_6}{a_1^{12}}$.
(iii) En (i), nous avons montré que si $p \neq 2$, alors $y^2 = x^3 + a_2x^2 + a_4x + a_6$. L'invariant de cette courbe (en caractéristique 3) vaut $j(E) = a_2^2/\Delta$. Si $j(E) = 0$, alors $a_2 = 0$ et nous avons l'expression demandée ; sinon il suffit de remplaçer x par $(x + \frac{a_4}{a_2})$ pour obtenir $y^2 = x^3 + a_2x^2 + \frac{2a_2^2a_4^2+a_2^3a_6+a_4^3}{a_2^3}$. □

Lemme 50. *Soit un corps K et une courbe E donnée par l'équation de Weierstrass :*

$$E : f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

dont le discriminant vaut Δ et le j-invariant, $j(E)$. Le changement de variables

$$(x,y) \leftarrow (u^2x + r, u^3y + u^2sx + t) \quad \textit{avec } r,s,t,u(\neq 0) \in K \tag{IV.9}$$

transforme l'équation précédente en

$$E' : f'(x,y) = y^2 + a_1'xy + a_3'y - x^3 - a_2'x^2 - a_4'x - a_6' = 0,$$

où les coefficients sont donnés par

$$\begin{aligned} ua_1' &= a_1 + 2s, \\ u^2a_2' &= a_2 - sa_1 + 3r - s^2, \\ u^3a_3' &= a_3 + ra_1 + 2t, \\ u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st. \end{aligned}$$

De plus, $u^{12}\Delta' = \Delta$ et $j(E') = j(E)$.

Preuve. Il suffit de remplaçer x et y par leurs nouvelles expressions pour obtenir les relations désirées. □

Il est à noter que toutes les transformations effectuées dans la démonstration du corollaire 49 sont de la forme (IV.9).

Théorème 51. *Soit K un corps de caractéristique p. Deux courbes données par leur équation de Weierstrass dont le discriminant est non nul sont isomorphes si et seulement si elles sont le même j-invariant.*

Preuve. ($\Rightarrow$) Par le lemme précédent.
($\Leftarrow$) Pour simplifier les calculs, nous allons supposer que $p \neq 2, 3$. Soient deux courbes E et E' ayant le même j-invariant dont les équations de Weierstrass sont données par

$$\begin{aligned} E &: y^2 = x^3 + a_4x + a_6, \\ E' &: y'^2 = x^3 + a_4'x + a_6'. \end{aligned}$$

Comme $j(E) = 1728\frac{4a_4^3}{4a_4^3+27a_6^2}$ et $j(E') = 1728\frac{4a_4'^3}{4a_4'^3+27a_6'^2}$ sont égaux, cela implique que $a_6^2a_4'^3 = a_4^3a_6'^2$. Cherchons des isomorphismes de la forme $(x,y) \leftarrow$

(u^2x, u^3y).
1° Si $a_4 = 0$, alors $a_6 \neq 0$ (car $\Delta \neq 0$) et donc $a'_4 = 0$. Nous obtenons un isomorphisme en prenant $u = (a_6/a'_6)^{1/6}$.
2° Si $a_6 = 0$, alors $a_4 \neq 0$ (car $\Delta \neq 0$) et donc $a'_6 = 0$. Nous obtenons un isomorphisme en prenant $u = (a_4/a'_4)^{1/4}$.
3° Si $a_4 a_6 \neq 0$, alors $a'_4 a'_6 \neq 0$. Nous obtenons un isomorphisme en prenant $u = (a_4/a'_4)^{1/6} = (a_6/a'_6)^{1/4}$.
Si $p = 2$ ou 3, la démonstration se fait de la même façon en prenant les équations de Weierstrass correspondantes. □

Théorème 52. *Soit E une courbe donnée par une équation de Weierstrass. Alors E est non singulière si et seulement si $\Delta \neq 0$.*

Preuve. ($\Leftarrow$) Soit l'équation générale de Weierstrass :

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Montrons d'abord que le point à l'infini $\mathcal{O} = (0, 1, 0)$ n'est jamais singulier. Regardons E comme une courbe de $\mathbb{P}^2$:

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0.$$

Comme $(\partial F/\partial Z)(\mathcal{O}) = 1 \neq 0$, $\mathcal{O}$ n'est pas un point singulier de E. Par l'absurde, supposons que E soit singulière en un point $P_0 = (x_0, y_0)$. Par le changement de variables $(x, y) \leftarrow (x - x_0, y - y_0)$, nous ramenons le point P_0 en $(0, 0)$. Par le lemme 50, cette transformation ne modifie pas le discriminant (car $u = 1$). Nous avons alors $a_6 = f(0, 0) = 0$, $a_4 = (\partial f/\partial x)(0, 0) = 0$ et $a_3 = (\partial f/\partial y)(0, 0) = 0$. La courbe E a donc pour équation :

$$E : f(x, y) = y^2 + a_1xy - x^3 - a_2x^2 = 0.$$

Le discriminant de cette équation est nul, ce qui contredit l'hypothèse.
($\Rightarrow$) Pour simplifier les calculs, nous allons supposer que $p \neq 2, 3$. Soit alors la courbe E donnée par l'équation de Weierstrass :

$$E : y^2 = x^3 + a_4x + a_6.$$

Si la courbe est singulière en un point $P_0 = (x_0, y_0)$, alors

$$2y_0 = 0 \Rightarrow y_0 = 0,$$
$$3x_0^2 + a_4 = 0 \Rightarrow x_0^2 = -\frac{a_4}{3}.$$

Or $P_0 = (x_0, y_0)$ est un point de la courbe, par conséquent, $y_0^2 = 0 = x_0^3 + a_4x_0 + a_6 = \frac{2}{3}a_4x_0 + a_6$. Il s'ensuit que $x_0^2 = \frac{9a_6^2}{4a_4^2} = -\frac{a_4}{3}$ et donc $\Delta = -16(4a_4^3 + 27a_6^2) = 0$. Si $p = 2$ ou 3, la démonstration se fait de la même façon en prenant les équations de Weierstrass correspondantes. □

Les théorèmes 47, 51 et 52 permettent de donner une définition alternative d'une courbe elliptique.

Définition 53. Une *courbe elliptique* est une courbe isomorphe à la courbe donnée par une des équations de Weierstrass (IV.4) à (IV.8) où $\Delta \neq 0$ plus le point à l'infini $\mathcal{O} = (0, 1, 0)$.

IV.3 Réduction d'une cubique

Soit un corps K de caractéristique différente de 2. L'équation projective d'une cubique irréductible non singulière est donnée par $f(U, V, W) = 0$ où

$$f(U,V,W) = s_1U^3 + s_2U^2V + s_3UV^2 + s_4V^3 + (s_5U^2 + s_6UV + s_7V^2)W + (s_8U + s_9V)W^2 + s_{10}W^3. \quad \text{(IV.10)}$$

L'équation (IV.10) peut également être vue comme un polynôme de degré 3 en W :

$$f(U,V,W) = c_0W^3 + c_1(U,V)W^2 + c_2(U,V)W + c_3(U,V). \quad \text{(IV.11)}$$

Soit $P_0 = (u_0, v_0, w_0)$ un point de la courbe. La tangente en P_0 intersecte la courbe en un troisième point unique $P_1 = (u_1, v_1, w_1)$. Cette tangente a pour équation

$$\frac{\partial f}{\partial U}(u_0,v_0,w_0)U + \frac{\partial f}{\partial V}(u_0,v_0,w_0)V + \frac{\partial f}{\partial W}(u_0,v_0,w_0)W = 0. \quad \text{(IV.12)}$$

Sans perdre de généralités, nous pouvons supposer que $w_1 \neq 0$ (nous pouvons toujours nous ramener à cette situation en permutant éventuellement W avec U ou avec V). Faisons le changement de variables $(U, V, W) \leftarrow (U - u_1, V - v_1, Z)$. Le point P_1 a maintenant pour coordonnées $(0, 0, 1)$. Étant donné que ce point appartient à la tangente, la dérivée partielle de f par rapport à W en P_0 est nulle. Comme la courbe est non singulière, les dérivées partielles par rapport à U et à V en P_0 ne peuvent pas s'annuler simultanément. Pour fixer les idées, supposons que la dérivée partielle par rapport à V en P_0 soit non nulle (si cette dernière est nulle, nous permutons les variables U et V). Le point $P_1 = (0, 0, 1)$ appartient aussi à la courbe et donc $s_{10} = 0$.

Après changement de variables, les équations (IV.10), (IV.11) et (IV.12) deviennent :

$$f(U,V,W) = s_1U^3 + s_2U^2V + s_3UV^2 + s_4V^3 + (s_5U^2 + s_6UV + s_7V^2)W + (s_8U + s_9V)W^2, \quad \text{(IV.13)}$$

$$f(U,V,W) = c_1(U,V)W^2 + c_2(U,V)W + c_3(U,V), \tag{IV.14}$$

$$V = \lambda U \quad \text{où } \lambda = \frac{\frac{\partial f}{\partial U}\Big|_{P_0}}{\frac{\partial f}{\partial V}\Big|_{P_0}}, \tag{IV.15}$$

de plus, $P_0 = (u_0 - u_1, v_0 - v_1, w_0)$ et $P_1 = (0,0,1)$.

Théorème 54. *Avec les notations précédentes et nos hypothèses de travail, si nous notons*

$$d(U,V) = c_2^2(U,V) - 4c_1(U,V)c_3(U,V)$$

et

$$d(U, \lambda U + 1) = AU^4 + BU^3 + CU^2 + DU + E,$$

et si P_0 n'est pas un point à l'infini, i.e. $w_0 \neq 0$, alors

1. *$A = 0$ et $B \neq 0$;*
2. *la transformation*

$$X = \frac{BU}{V - \lambda U},$$
$$Y = \frac{B}{(V - \lambda U)^2}(2c_3(U,V) + c_2(U,V))$$

est une transformation birationnelle dont l'inverse est donnée par

$$U = X\frac{BY - c_2(X, \lambda X + B)}{2c_3(X, \lambda X + B)},$$
$$V = (\lambda X + B)\frac{BY - c_2(X, \lambda X + B)}{2c_3(X, \lambda X + B)};$$

3. *l'application birationnelle précédente transforme l'équation de la cubique en l'équation de Weierstrass*

$$Y^2 = X^3 + CX^2 + BDX + B^2E.$$

Preuve. (i) Si nous calculons $d(1,\lambda)$ et $\frac{\partial d}{\partial V}(1,\lambda)$, nous obtenons

$$d(1,\lambda) = (s_5 + s_6\lambda + s_7^2\lambda^2)^2 - 4(s_8 + s_9\lambda)(s_1 + s_2\lambda + s_3\lambda^2 + s_4\lambda^3)$$

et

$$\begin{aligned}\frac{\partial d}{\partial V}(1,\lambda) &= 2c_2(1,\lambda)\frac{\partial c_2}{\partial V}(1,\lambda) - 4c_1(1,\lambda)\frac{\partial c_3}{\partial V}(1,\lambda) - 4\frac{\partial c_1}{\partial V}(1,\lambda)c_3(1,\lambda)\\ &= 2(s_5 + s_6\lambda + s_7\lambda^2)(s_6 + 2s_7\lambda) - 4(s_8 + s_9\lambda)(s_2 + 2s_3\lambda + 3s_4\lambda^2)\\ &\quad -4s_9(s_1 + s_2\lambda + s_3\lambda^2 + s_4\lambda^3)\end{aligned}$$

Développons ensuite $d(U, \lambda U + 1)$:

$$\begin{aligned}
&d(U, \lambda U + 1) \\
&\quad = c_2^2(U, \lambda U + 1) - 4c_1(U, \lambda U + 1)c_3(U, \lambda U + 1) \\
&\quad = [(s_5 + s_6\lambda + s_7\lambda^2)U^2 + (s_6 + 2s_7\lambda)U + s_7]^2 - \\
&\qquad 4[(s_8 + s_9\lambda)U + s_9] \cdot [(s_1 + s_2\lambda + s_3\lambda^2 + s_4\lambda^3)U^3 + \\
&\qquad\quad (s_2 + 2s_3\lambda + 3s_4\lambda^2)U^2 + (s_3 + 3s_4\lambda)U + s_4] \\
&\quad = [(s_5 + s_6\lambda + s_7\lambda^2)^2 - 4(s_8 + s_9\lambda)(s_1 + s_2\lambda + s_3\lambda^2 + s_4\lambda^3)]U^4 + \\
&\qquad [2(s_5 + s_6\lambda + s_7\lambda^2)(s_6 + 2s_7\lambda) - 4(s_8 + s_9\lambda)(s_2 + 2s_3\lambda + 3s_4\lambda^2) \\
&\qquad\quad -4s_9(s_1 + s_2\lambda + s_3\lambda^2 + s_4\lambda^3)]U^3 + [\cdots]U^2 + [\cdots]U + [\cdots] \\
&\quad = d(1, \lambda)U^4 + \frac{\partial d}{\partial V}(1, \lambda)U^3 + [\cdots]U^2 + [\cdots]U + [\cdots].
\end{aligned}$$

Le point P_0 est un point de la tangente, il a donc pour coordonnées $(\alpha, \lambda\alpha, 1)$ avec $\alpha \neq 0$ car $P_0 \neq P_1$. Le point P_0 est une racine double de f. En résolvant par rapport à U dans (IV.14), nous avons $c_1(\alpha, \lambda\alpha) + c_2(\alpha, \lambda\alpha) + c_3(\alpha, \lambda\alpha) = \alpha[c_1(1, \lambda) + \alpha c_2(1, \lambda) + \alpha^2 c_3(1, \lambda)] = 0$; $\alpha = 0$ correspond à P_1 et $c_1(1, \lambda) + \alpha c_2(1, \lambda) + \alpha^2 c_3(1, \lambda) = 0$ correspond à la valeur double en P_0. Cette racine étant double, il s'ensuit que le discriminant est nul, i.e. $d(1, \lambda) = 0$ et que $c_3(1, \lambda) \neq 0$. Nous trouvons

$$\alpha = -\frac{c_2(1, \lambda)}{2c_3(1, \lambda)}.$$

Comme $d(1, \lambda) = 0$, nous avons démontré que $A = 0$. Il reste à montrer que $B \neq 0$. Calculons :

$$\begin{aligned}
&\frac{\partial f}{\partial V}(\alpha, \lambda\alpha, 1) \\
&\quad = \frac{\partial c_1}{\partial V}(\alpha, \lambda\alpha) + \frac{\partial c_2}{\partial V}(\alpha, \lambda\alpha) + \frac{\partial c_3}{\partial V}(\alpha, \lambda\alpha) \\
&\quad = \frac{\partial c_1}{\partial V}(1, \lambda) + \alpha\frac{\partial c_2}{\partial V}(1, \lambda) + \alpha^2\frac{\partial c_3}{\partial V}(1, \lambda) \\
&\quad = \frac{4c_3^2(1, \lambda)\frac{\partial c_1}{\partial V}(1, \lambda) - 2c_2(1, \lambda)c_3(1, \lambda)\frac{\partial c_2}{\partial V}(1, \lambda) + c_2^2(1, \lambda)\frac{\partial c_3}{\partial V}(1, \lambda)}{4c_3^2(1, \lambda)} \\
&\qquad\qquad \text{car } \alpha = -\frac{c_2(1, \lambda)}{2c_3(1, \lambda)} \\
&\quad = -\frac{-4c_3(1, \lambda)\frac{\partial c_1}{\partial V}(1, \lambda) + 2c_2(1, \lambda)\frac{\partial c_2}{\partial V}(1, \lambda) - 4c_1(1, \lambda)\frac{\partial c_3}{\partial V}(1, \lambda)}{4c_3(1, \lambda)} \\
&\qquad\qquad \text{car } A = d(1, \lambda) = c_2^2(1, \lambda) - 4c_1(1, \lambda)c_3(1, \lambda) = 0 \\
&\quad = -\frac{\frac{\partial d}{\partial V}(1, \lambda)}{4c_3(1, \lambda)} = -\frac{B}{4c_3(1, \lambda)} \neq 0
\end{aligned}$$

car la dérivée partielle par rapport à V en P_0 est non nulle par hypothèse.
(ii) Par substitution, nous voyons que si $B \neq 0$, les applications $(U, V) \to (X, Y)$ et $(X, Y) \to (U, V)$ sont les inverses l'une de l'autre.
(iii) En remplaçant U et V par leurs expressions respectives, nous obtenons

$$B^2Y^2 = d(X, \lambda X + B).$$

Or, comme $d(U, V)$ est un polynôme homogène de degré 4, nous voyons immédiatement que

$$d(X, \lambda X + B) = B(BX^3) + C(B^2X^2) + D(B^3X) + E(B^4).$$

Pour s'en convaincre, il suffit de regarder le développement de $d(U, \lambda U + 1)$ (voir p. 34). Nous avons finalement

$$B^2Y^2 = B^2(X^3 + CX^2 + DBX + EB^2),$$

ce qui termine la démonstration. □

IV.4 Loi de groupe

IV.4.1 Règle de la "sécante-tangente"

Proposition 55. *Soient une cubique irréductible non singulière C et une droite L définies sur un corps K. Si la cubique C a deux points d'intersection (comptés avec leur multiplicité) avec la droite L, alors C a trois points d'intersection (comptés avec leur multiplicité) avec la droite L.*

Preuve. Comme C est irréductible, $C \cap L$ a un nombre fini de points. Soit la droite $L : aX + bY + cZ = 0$ où, par symétrie, nous supposons $c \neq 0$. Les points d'intersection de C et de L sont les racines du polynôme

$$q(X, Y) = p(X, Y, -\frac{aX + bY}{c}) \in K[X, Y]_3.$$

Notons $P_1 = (a_1, b_1, c_1)$ et $P_2 = (a_2, b_2, c_2)$ (avec éventuellement $P_1 = P_2$), deux points d'intersection de C avec L, alors, comme $q(a_1, b_1) = q(a_2, b_2) = 0$, il vient que

$$q(X, Y) = v(X, Y) \prod_{i=1}^{2} (b_iX - a_iY) \quad \text{où } v(X, Y) \in K[X, Y]_1.$$

Le troisième point d'intersection de C avec L est alors donné par

$$P_3 = (a_3, b_3, -\frac{aa_3 + bb_3}{c})$$

où (a_3, b_3) est l'unique racine de $v(X, Y)$. □

Cette proposition permet de définir la *loi de composition de la sécante-tangente* :

1. Si $P, Q \in C(K)$ et si $P \neq Q$, alors nous définissons $L = PQ$, la droite sécante qui passe par P et Q. Par la proposition précédente, nous savons qu'il existe un troisième point unique (en comptant les multiplicités) qui appartient à $C \cap L$, nous notons ce troisième point $P * Q$.

2. Si $P \in C(K)$, alors nous définissons $L = PP$, la droite tangente à C qui passe par P. Par la proposition précédente, nous savons qu'il existe un troisième point unique (en comptant les multiplicités) qui appartient à $C \cap L$, nous notons ce troisième point $P * P$.

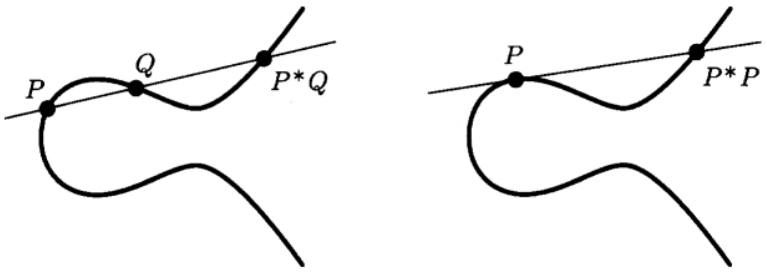

Figure 3: Règle de la sécante-tangente.

Proposition 56. *Soient un corps infini K et une cubique irréductible non singulière C. Pour tous points P_1, P_2, Q_1 et $Q_2 \in C(K)$, nous avons*

$$(P_1 * P_2) * (Q_1 * Q_2) = (P_1 * Q_1) * (P_2 * Q_2). \tag{IV.16}$$

Preuve. Construisons les matrices

$$M = \begin{pmatrix} P_1 & P_2 & P_1 * P_2 \\ Q_1 & Q_2 & Q_1 * Q_2 \\ P_1 * Q_1 & P_2 * Q_2 & (P_1 * Q_1) * (P_2 * Q_2) \end{pmatrix}$$

et

$$\widetilde{M} = \begin{pmatrix} P_1 & Q_1 & P_1 * Q_1 \\ P_2 & Q_2 & P_2 * Q_2 \\ P_1 * P_2 & Q_1 * Q_2 & (P_1 * P_2) * (Q_1 * Q_2) \end{pmatrix},$$

où les éléments de la ligne i de M (respectivement $\widetilde{M}$) sont des points de $C(K)$ de la droite L_i (respectivement $\widetilde{L}_i$) passant par ces éléments. Nous

devons montrer que $M = \widetilde{M}^t$.
(i) Considérons d'abord le cas où L_i et $\widetilde{L}_j$ ont uniquement un point d'intersection (c'est ce que nous appellerons l'hypothèse de travail (i)).
Posons $L = L_1L_2L_3$ et $\widetilde{L} = \widetilde{L}_1\widetilde{L}_2\widetilde{L}_3$. Choisissons ensuite a_1, a_2 et a_3 non tous nuls tels que

$$\begin{cases} a_1C(R_1) + a_2L(R_1) + a_3\widetilde{L}(R_1) = 0 \\ a_1C(R_2) + a_2L(R_2) + a_3\widetilde{L}(R_2) = 0 \end{cases}, \tag{IV.17}$$

avec $R_1(\neq P_1, P_2 \text{ et } P_1 * P_2) \in L_1$ et $R_2 \notin L$. Remarquons que R_1 et R_2 existent car K est infini. Construisons la cubique

$$C_0 = a_1C + a_2L + a_3\widetilde{L}.$$

a) Par l'absurde, supposons que $C_0 \neq 0$.

(1) Notons M_{1j} un élément quelconque de la première ligne de la matrice M. Par le lemme 37,

$$\begin{aligned} I(M_{1j}, L_1, \widetilde{L}) &= I(M_{1j}, L_1, \widetilde{L}_1) + I(M_{1j}, L_1, \widetilde{L}_2) + I(M_{1j}, L_1, \widetilde{L}_3) \\ &\geq 1. \end{aligned}$$

Or, par le lemme 38,

$$\begin{aligned} I(M_{1j}, L_1, C_0) &\geq \min\{I(M_{1j}, L_1, C), I(M_{1j}, L_1, L), I(M_{1j}, L_1, \widetilde{L})\} \\ &\geq 1. \end{aligned}$$

Par (IV.17), R_1 est un point de C_0 et donc $I(R_1, L_1, C_0) \geq 1$ car $R_1 \in L_1$. Nous avons finalement que $\sum_{P \in L_1} I(P, L_1, C_0) \geq 4$ et, par conséquent, par le corollaire 45, $C_0 = FL_1$ où F est une conique.

(2) Notons M_{2k} un élément quelconque de la deuxième ligne de la matrice M.
1° Par le lemme 38,

$$\begin{aligned} I(M_{2k}, L_2, C_0) &\geq \min\{I(M_{2k}, L_2, C), I(M_{2k}, L_2, L), I(M_{2k}, L_2, \widetilde{L})\} \\ &\geq 1. \end{aligned}$$

De plus, par le lemme 37,

$$I(M_{2k}, L_2, C_0) = I(M_{2k}, L_2, F) + I(M_{2k}, L_2, L_1) \geq 1.$$

Si $M_{2k} \notin L_1$, alors $I(M_{2k}, L_2, L_1) = 0$ et donc $I(M_{2k}, L_2, F) \geq 1$.
2° Sinon, si $M_{2k} \in L_1$, alors $\exists j$ tel que $M_{2k} = M_{1j}$ et donc $M_{2k} \in$

$\widetilde{L}_j$. Par l'hypothèse de travail (i), $L_2 \cap \widetilde{L}_j = M_{2j}$ et par conséquent $j = k$. M_{2k} apparaît donc deux fois dans $\widetilde{L}_j$ car $M_{2k} = M_{1j} = M_{1k}$. Nous avons alors, par le lemme 38,

$$\begin{aligned} I(M_{2k}, \widetilde{L}_j, C_0) &\geq \min\{I(M_{2k}, \widetilde{L}_j, C), I(M_{2k}, \widetilde{L}_j, L), I(M_{2k}, \widetilde{L}_j, \widetilde{L})\} \\ &\geq 2. \end{aligned}$$

Par l'hypothèse de travail (i), $I(M_{2k}, \widetilde{L}_j, L_1) = 1$. Par le lemme 37,

$$I(M_{2k}, \widetilde{L}_j, C_0) = I(M_{2k}, \widetilde{L}_j, F) + I(M_{2k}, \widetilde{L}_j, L_1) \geq 2.$$

Nous avons finalement $I(M_{2k}, \widetilde{L}_j, F) \geq 1$; M_{2k} est donc un point de F et $I(M_{2k}, L_2, F) \geq 1$.
3° Comme $I(M_{2k}, L_2, F) \geq 1$ indépendamment du fait que $M_{2k} \in L_1$ ou non, nous avons $\sum_{P \in L_2} I(P, L_2, F) \geq 3$ et, par conséquent, par le corollaire 45, $F = DL_2$ où D est une droite.

(3) 1° Considérons le cas où $P_1 * Q_1 = P_2 * Q_2$. Appelons ce point commun $M_{3\cdot}$. Alors, par l'hypothèse de travail (i), $I(M_{3\cdot}, L_3, L_1) = I(M_{3\cdot}, L_3, L_2) = 0$. En effet, si $P_1 * Q_1 = P_2 * Q_2 = P_1 * P_2$ (les autres cas sont triviaux ou symétriques), alors $Q_1 * Q_2 = P_1 * P_2$ et les droites L_3 et $\widetilde{L}_3$ ont alors deux points communs. Par le lemme 38,

$$\begin{aligned} I(M_{3\cdot}, L_3, C_0) &\geq \min\{I(M_{3\cdot}, L_3, C), I(M_{3\cdot}, L_3, L), I(M_{3\cdot}, L_3, \widetilde{L}) \\ &\geq 2. \end{aligned}$$

Or, par le lemme 37,

$$\begin{aligned} I(M_{3\cdot}, L_3, C_0) &= I(M_{3\cdot}, L_3, D) + I(M_{3\cdot}, L_3, L_2) + I(M_{3\cdot}, L_3, L_1) \\ &\geq 2, \end{aligned}$$

et donc $I(M_{3\cdot}, L_3, D) \geq 2$. Ce qui signifie, par la corollaire 45, que $D = kL_3$ où k est une constante non nulle.
2° Supposons que le point $M_{31} = P_1 * Q_1$ apparaisse n fois dans $\widetilde{L}_j$. Alors, par le lemme 38,

$$\begin{aligned} I(M_{31}, \widetilde{L}_j, C_0) &\geq \min\{I(M_{31}, \widetilde{L}_j, C), I(M_{31}, \widetilde{L}_j, L), I(M_{31}, \widetilde{L}_j, \widetilde{L})\} \\ &\geq n. \end{aligned}$$

De plus, par le lemme 37,

$$I(M_{31}, \widetilde{L}_j, C_0) = I(M_{31}, \widetilde{L}_j, D) + I(M_{31}, \widetilde{L}_j, L_1 L_2).$$

Or, par le lemme 37 et compte tenu de l'hypothèse de travail (i),

$$I(M_{31}, \widetilde{L}_j, L_1 L_2) = n - 1,$$

et donc $I(M_{31}, \widetilde{L}_j, D) \geq 1$. Cela signifie que $M_{31} \in D$. Comme le même argument est valable pour le point $M_{32} = P_2 * Q_2$, nous avons que $M_{32} \in D$. La droite D a par conséquent deux points distincts communs avec L_3 et donc, $D = kL_3$ où k est une constante non nulle.

Finalement, nous avons $C = kL_1L_2L_3 = kL$ où k est une constante non nulle. Or, par hypothèse, $C(R_2) = 0$ et $L(R_2) \neq 0$, ce qui est impossible car $k \neq 0$. Nous avons donc

$$a_1 C + a_2 L + a_3 \widetilde{L} = 0.$$

b) Montrons que $a_1 \neq 0$.
Par l'absurde, supposons que $a_1 = 0$, alors $a_2 \neq 0$ ou $a_3 \neq 0$. Par symétrie, supposons que $a_2 \neq 0$, alors L divise $\widetilde{L}$, et donc $\exists i, j$ tels que L_i est la même droite que $\widetilde{L}_j$, ce qui est contraire à l'hypothèse de travail (i). Nous avons démontré que

$$C = b_1 L + b_2 \widetilde{L}, \tag{IV.18}$$

avec $b_1 = a_2/a_1$ et $b_2 = a_3/a_1$.

c) Notons T le point d'intersection entre L_3 et $\widetilde{L}_3$. Par (IV.18), $C(T) = 0$; T est donc un point de C. Comme $T \in L_3 \cap C$, T est égal à

$$P_1 * Q_1, P_2 * Q_2 \text{ ou } (P_1 * Q_1) * (P_2 * Q_2). \tag{IV.19}$$

Et comme $T \in \widetilde{L}_3 \cap C$, T est égal à

$$P_1 * P_2, Q_1 * Q_2 \text{ ou } (P_1 * P_2) * (Q_1 * Q_2). \tag{IV.20}$$

Par l'hypothèse de travail (i), les deux premiers points de (IV.19) sont différents des deux premiers de (IV.20). En effet, si, par exemple, $P_1 * Q_1 = T = P_1 * P_2$, alors les droites L_1 et $\widetilde{L}_1$ ont deux points communs. Il reste donc les cas

$$(P_1 * Q_1) * (P_2 * Q_2) = T = (P_1 * P_2) * (Q_1 * Q_2), \tag{IV.21}$$
$$P_1 * Q_1 = T = (P_1 * P_2) * (Q_1 * Q_2), \tag{IV.22}$$
$$P_1 * P_2 = T = (P_1 * Q_1) * (P_2 * Q_2),$$
$$P_2 * Q_2 = T = (P_1 * P_2) * (Q_1 * Q_2),$$
$$Q_1 * Q_2 = T = (P_1 * Q_1) * (P_2 * Q_2).$$

Si la relation (IV.21) est vérifiée, alors la démonstration est terminée. Les quatre dernières relations étant symétriques, nous allons uniquement montrer que la relation (IV.22) n'est jamais vérifiée ou implique la relation (IV.21). Considérons le point $M_{33} = (P_1 * Q_1) * (P_2 * Q_2)$. Ce point appartient à $C \cap L_3$. Donc, comme $c_2 \neq 0$ (car sinon C serait réductible), $M_{33} \in \widetilde{L}$, c.-à-d. M_{33} est un point de $\widetilde{L}_1, \widetilde{L}_2$ et/ou $\widetilde{L}_3$.
1° Si $M_{33} \in \widetilde{L}_1$, alors $M_{33} \in L_3 \cap \widetilde{L}_1$ et est donc égal à $P_1 * Q_1$, i.e.

$$(P_1 * Q_1) * (P_2 * Q_2) = P_1 * Q_1.$$

Ce qui, remis dans (IV.22), termine la démonstration.
2° Si $M_{33} \in \widetilde{L}_2$, alors $M_{33} \in L_3 \cap \widetilde{L}_2$ et est donc égal à $P_2 * Q_2$, i.e.

$$(P_1 * Q_1) * (P_2 * Q_2) = P_2 * Q_2. \tag{IV.23}$$

Si $P_2 * Q_2 = P_1 * Q_1$, alors nous avons un cas équivalent à 1°. Sinon, par (IV.18) et par le lemme 38,

$$I(P_1 * Q_1, L_3, C) \geq \min\{I(P_1 * Q_1, L_3, L), I(P_1 * Q_1, L_3, \widetilde{L})\} \geq 2,$$

car, par (IV.22), $I(P_1 * Q_1, L_3, \widetilde{L}) \geq 2$. De plus, comme $P_1 * Q_1 \neq P_2 * Q_2$, par (IV.23),

$$I(P_2 * Q_2, L_3, C) = 2.$$

Nous avons finalement $\sum_{P \in L_3} I(P, L_3, C) \geq 4$; ce qui signifie, par le corollaire 45, que L_3 divise C, ce qui est impossible car C est irréductible.
3° Si $M_{33} \in \widetilde{L}_3$, alors $M_{33} \in L_3 \cap \widetilde{L}_3$ et est donc égal à T, i.e.

$$(P_1 * Q_1) * (P_2 * Q_2) = T = (P_1 * P_2) * (Q_1 * Q_2),$$

ce qui termine la démonstration.

(ii) Considérons à présent le cas où $\exists i, j$ tels que $L_i = \widetilde{L}_j$. Par symétrie, les seuls cas à envisager sont

$$\begin{aligned} P_1 &= Q_2, \\ P_1 &= Q_1 * Q_2 \quad (\text{et donc } P_1 * Q_1 = Q_2), \\ P_1 * P_2 &= P_1 * Q_1 \quad (\text{et donc } P_2 = Q_1). \end{aligned}$$

La relation (IV.16) devient alors respectivement

$$\begin{aligned} (P_1 * P_2) * (Q_1 * P_1) &= (P_1 * Q_1) * (P_2 * P_1), \\ (P_1 * P_2) * P_1 &= Q_2 * (P_2 * Q_2), \\ (P_1 * P_2) * (P_2 * Q_2) &= (P_1 * P_2) * (P_2 * Q_2). \end{aligned}$$

Comme la deuxième relation se réduit à $P_2 = P_2$ et que les deux autres relations sont immédiates, le théorème est démontré. □

Théorème 57. *Soit un corps infini K. Si $(E, \mathcal{O})$ est une courbe elliptique définie sur K, alors l'opération*

$$P + Q = \mathcal{O} * (P * Q) \tag{IV.24}$$

définit une structure de groupe commutatif ayant $\mathcal{O}$ comme élément neutre. De plus, si $\mathcal{O}'$ est un autre point de la courbe elliptique, alors l'opération

$$P +' Q = \mathcal{O}' * (P * Q)$$

définit une structure de groupe isomorphe au premier.

Preuve. (i) a) Vu la définition de la loi de composition de la sécante-tangente, la commutativité est évidente : $P + Q = \mathcal{O} * (P * Q) = \mathcal{O} * (Q * P) = Q + P$. b) $\mathcal{O}$ est l'élément neutre, car $P + \mathcal{O} = \mathcal{O} * (P * \mathcal{O}) = \mathcal{O} * (\mathcal{O} * P) = \mathcal{O} + P = P$. c) L'élément symétrique d'un élément Q est défini par :

$$-Q = (\mathcal{O} * \mathcal{O}) * Q. \tag{IV.25}$$

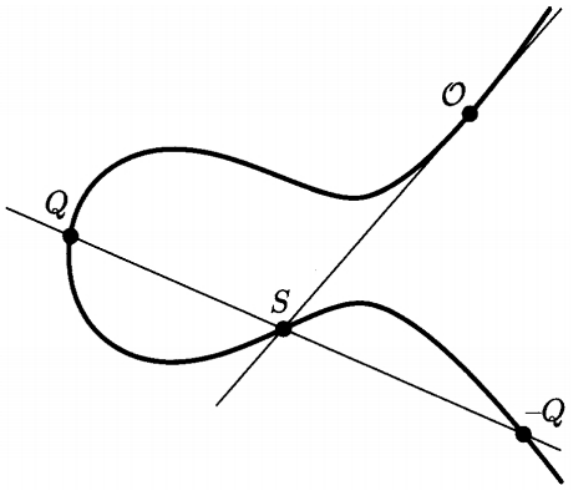

Figure 4: Symétrique d'un élément Q.

Ce qui est bien le symétrique, car

$$Q + (-Q) = \mathcal{O} * (Q * ((\mathcal{O} * \mathcal{O}) * Q)) = \mathcal{O} * (\mathcal{O} * \mathcal{O}) = \mathcal{O} + \mathcal{O} = \mathcal{O}$$

et

$$-Q + Q = \mathcal{O} * (((\mathcal{O} * \mathcal{O}) * Q) * Q) = \mathcal{O} * (\mathcal{O} * \mathcal{O}) = \mathcal{O} + \mathcal{O} = \mathcal{O}.$$

d) Il reste à montrer l'associativité. Calculons :

$$\begin{aligned} P*(Q+R) &= P*(\mathcal{O}*(Q*R)) \\ &= ((P*Q)*Q)*(\mathcal{O}*(Q*R)) \quad \text{car } P=(P*Q)*Q \\ &= ((P*Q)*\mathcal{O})*(Q*(Q*R)) \quad \text{par la relation (IV.16)} \\ &= ((P*Q)*\mathcal{O})*R \quad \text{car } Q*(Q*R)=R \\ &= (\mathcal{O}*(P*Q))*R \\ &= (P+Q)*R. \end{aligned}$$

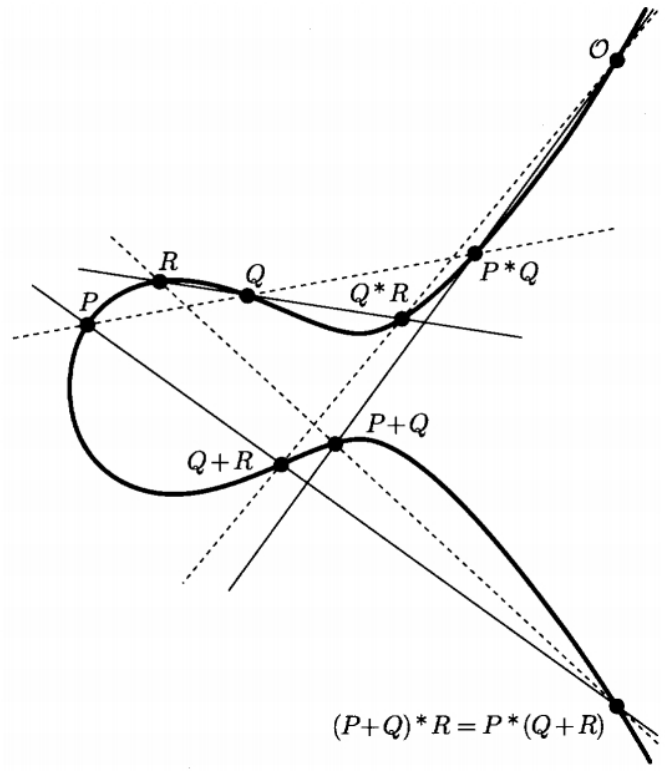

Figure 5: Vérification de l'associativité.

En appliquant $\mathcal{O}$ sur les deux membres de l'égalité, nous trouvons $P+(Q+R)=(P+Q)+R$.
(ii) Construisons l'application bijective

$$\phi : (E,+) \to (E,+'), P \mapsto P-\mathcal{O}',$$

alors

$$\phi(P+Q)=(P+Q)-\mathcal{O}'$$

$$
\begin{aligned}
&= \mathcal{O} * [(\mathcal{O} * (P * Q)) * ((\mathcal{O} * \mathcal{O}) * \mathcal{O}')] \\
&= \mathcal{O} * [(\mathcal{O} * (\mathcal{O} * \mathcal{O})) * ((P * Q) * \mathcal{O}')] \quad \text{par (IV.16)} \\
&= \mathcal{O} * [\mathcal{O} * (P +' Q)] \\
&= P +' Q = \phi(P) +' \phi(Q).
\end{aligned}
$$

L'application ϕ est donc un isomorphisme. □

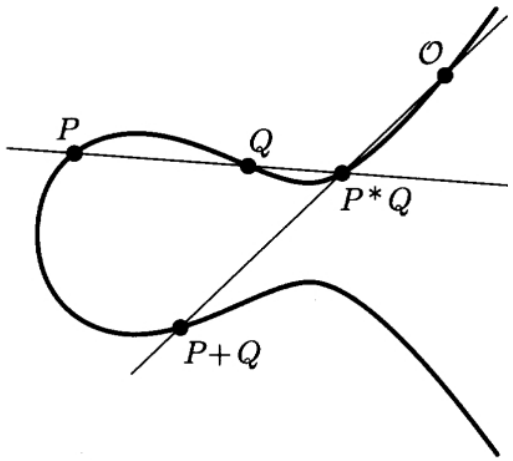

Figure 6: Loi de groupe sur une courbe elliptique.

IV.4.2 Théorème de Poincaré

Le théorème 57 peut être généralisé à un corps de caractéristique quelconque.

Théorème 58 Théorème de Poincaré. *Soit un corps K. Si $(E, \mathcal{O})$ est une courbe elliptique définie sur K, alors l'opération*

$$P + Q = \mathcal{O} * (P * Q)$$

définit une structure de groupe commutatif ayant $\mathcal{O}$ comme élément neutre. De plus, si $\mathcal{O}'$ est un autre point de la courbe elliptique, alors l'opération

$$P +' Q = \mathcal{O}' * (P * Q)$$

définit une structure de groupe isomorphe au premier.

Nous allons démontrer ce théorème dans le cas où $K = \mathbb{F}_q$. Pour cela, nous avons besoin d'introduire l'application *réduction modulo q*.

IV.4.3 L'application "réduction modulo q"

Notons $\mathbb{P}_2(\mathbb{Q})$, l'ensemble des points rationnels dans $\mathbb{P}_2$. Un point $P = (a, b, c)$ est *normalisé* si a, b et c sont des entiers sans facteur commun.

Exemple 16. Le point $(1/2, -2/3, 3/4)$ est représenté par $(6, -8, 9)$ en coordonnées normalisées.

Si $\widetilde{x}$ représente le résidu de x modulo q, i.e. $\widetilde{x} = x \bmod q$, alors à chaque point normalisé $P = (a, b, c)$ de $\mathbb{P}_2(\mathbb{Q})$ correspond, au signe près, un et un seul point $\widetilde{P} = (\widetilde{a}, \widetilde{b}, \widetilde{c})$ de $\mathbb{P}_2(\mathbb{F}_q)$, car au moins un des trois nombres a, b ou c n'est pas un multiple de q.

Définition 59. L'application *réduction modulo* q est l'application

$$\varphi : \mathbb{P}_2(\mathbb{Q}) \to \mathbb{P}_2(\mathbb{F}_q), P \mapsto \widetilde{P}. \tag{IV.26}$$

Soit $C \in \mathbb{Q}[X, Y, Z]_d$ une courbe définie sur $\mathbb{Q}$ dont les coefficients sont normalisés, nous dirons que C est *normalisée*. Alors, nous associons la courbe $\widetilde{C} \in \mathbb{F}_q[X, Y, Z]_d$ en réduisant les coefficients de C modulo q.

Proposition 60. *Avec les notations précédentes, si* $P \in C(\mathbb{Q})$, *alors* $\widetilde{P} \in \widetilde{C}(\mathbb{F}_q)$.

Preuve. Comme $\psi : \mathbb{Z} \to \mathbb{F}_q, x \mapsto \widetilde{x}$ est un homomorphisme de groupe, la thèse est immédiate. □

Corollaire 61. *Si* C_1 *et* C_2 *sont deux courbes, alors*

$$(C_1(\mathbb{Q}) \widetilde{\cap} C_2(\mathbb{Q})) \subseteq \widetilde{C_1}(\mathbb{F}_q) \cap \widetilde{C_2}(\mathbb{F}_q).$$

Preuve. Trivial. □

Lemme 62. *Soit une droite normalisée* $L \in \mathbb{P}_2(\mathbb{Q})$ *donnée par*

$$L : aX + bY + cZ = 0.$$

Alors il existe une tranformation linéaire

$$T : \mathbb{P}_2(\mathbb{Q}) \to \mathbb{P}_2(\mathbb{Q}), \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \mapsto \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & t_{22} & t_{23} \\ t_{31} & t_{32} & t_{33} \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

compatible avec la réduction modulo q *qui transforme* L *en la droite à l'infini* $L' : Z' = 0$.

Preuve. Notons $d = \text{pgcd}(b, c)$. Par le corollaire 4, $\exists r, s \in \mathbb{Z}$ tels que $rc - sb = d$. Remarquons que r et s sont nécessairement premiers entre eux. De plus, comme L est en coordonnées normalisées, $\text{pgcd}(a, d) = 1$, et donc, par le corollaire 5, $\exists t, u \in \mathbb{Z}$ tels que $td + ua = 1$. Comme $\text{pgcd}(r, s) = 1$, $\exists v, w \in \mathbb{Z} : vs - wr = u$. Définissons la matrice (t_{ij}) :

$$(t_{ij}) = \begin{pmatrix} t & v & w \\ 0 & r & s \\ a & b & c \end{pmatrix}.$$

Le déterminant de cette matrice vaut 1 par les hypothèses sur r, s, t, u, v et w. Par conséquent, la matrice $(m_{ij}) = (t_{ij})^{-1}$ aura des éléments entiers. Les matrices réduites $(\widetilde{t}_{ij})$ et $(\widetilde{m}_{ij})$ sont donc inverses l'une de l'autre, fournissant un changement de coordonnées correspondant modulo q. □

Proposition 63. *Soient une cubique irréductible non singulière C et une droite L définies sur $\mathbb{Q}$. Alors, si $C \cap L = \{P_1, P_2, P_3\}$ en coordonnées normalisées et si $\widetilde{L}$ n'est pas une composante de $\widetilde{C}$, $\widetilde{C} \cap \widetilde{L} = \{\widetilde{P_1}, \widetilde{P_2}, \widetilde{P_3}\}$.*

Preuve. (i) Supposons que L soit la droite à l'infini $Z = 0$. Notons $P_i = (a_i, b_i, 0)$ $(i = 1, 2, 3)$, les trois points d'intersection de C et de L en coordonnés normalisées et $F(X, Y, Z) = 0$, l'équation de C. Alors,

$$F(X, Y, 0) = k \prod_{i=1}^{3} (a_i Y - b_i X), \tag{IV.27}$$

avec $k \neq 0$ car C est irréductible. Comme $\widetilde{L}$ n'est pas une composante de $\widetilde{C}$, il s'ensuit que $\widetilde{F}(X, Y, 0) \neq 0 \ \forall X, Y$. Par ailleurs, étant donné que les points P_i sont en coordonnées normalisées, $(\widetilde{a}_i, \widetilde{b}_i) \neq (0, 0)$; et donc $\widetilde{k} \neq 0$. Nous pouvons par conséquent réduire (IV.27) modulo q:

$$\widetilde{F}(X, Y, 0) = \widetilde{k} \prod_{i=1}^{3} (\widetilde{a}_i Y - \widetilde{b}_i X),$$

et donc, $\widetilde{C} \cap \widetilde{L} = \{\widetilde{P_1}, \widetilde{P_2}, \widetilde{P_3}\}$.
(ii) Si L n'est pas la droite à l'infini, alors nous l'y ramenons par la transformation définie par le lemme 62. □

IV.4.4 Démonstration du théorème de Poincaré

Par le théorème 57, nous savons que si $(E, \mathcal{O})$ est une courbe elliptique définie sur $\mathbb{Q}$, alors l'opération $P + Q = \mathcal{O} * (P * Q)$ définit une structure de groupe.

Nous devons donc démontrer que, si $(\widetilde{E}, \widetilde{\mathcal{O}})$ est une courbe elliptique définie sur $\mathbb{F}_q$, l'application modulo $q : E(\mathbb{Q}) \to \widetilde{E}(\mathbb{F}_q), P \mapsto \widetilde{P}$ est un homomorphisme de groupe.

Preuve. Soient P et Q deux points de $E(\mathbb{Q})$ tels que $P + Q = R$. Notons respectivement L_1 et L_2, les droites PQ et $(P * Q)R$; et donc

$$E \cap L_1 = \{P, Q, P * Q\} \quad \text{et} \quad E \cap L_2 = \{P * Q, R, \mathcal{O}\}.$$

Par la proposition 63,

$$\widetilde{E} \cap \widetilde{L_1} = \{\widetilde{P}, \widetilde{Q}, \widetilde{P * Q}\} \quad \text{et} \quad \widetilde{E} \cap \widetilde{L_2} = \{\widetilde{P * Q}, \widetilde{R}, \widetilde{\mathcal{O}}\},$$

et donc $\widetilde{R} = \widetilde{P + Q} = \widetilde{P} + \widetilde{Q}$. □

Il reste à montrer que cette structure de groupe est indépendante du choix de $\widetilde{\mathcal{O}} \in \widetilde{E}(\mathbb{F}_q)$.

Preuve. Construisons l'application bijective

$$\phi : (\widetilde{E}, +) \to (\widetilde{E}, +'), \widetilde{P} \mapsto \widetilde{P} - \widetilde{\mathcal{O}'},$$

alors, par le théorème 57 et comme l'application modulo q est un homomorphisme de $E(\mathbb{Q})$ dans $\widetilde{E}(\mathbb{F}_q)$,

$$\begin{aligned}\phi(\widetilde{P} + \widetilde{Q}) &= \phi(\widetilde{P + Q}) = (\widetilde{P + Q}) - \widetilde{\mathcal{O}'} = (\widetilde{P} + \widetilde{Q}) - \widetilde{\mathcal{O}'} = \widetilde{P} +' \widetilde{Q} \\ &= \phi(\widetilde{P}) +' \phi(\widetilde{Q}).\end{aligned}$$

L'application ϕ est donc un isomorphisme. □

IV.4.5 Formules explicites

Nous allons à présent donner les formules explicites pour additionner deux points P et Q et pour doubler un point P sur une courbe elliptique donnée par l'équation de Weierstrass

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \qquad \text{(IV.28)}$$

où nous prenons, comme élément neutre, le point à l'infini $\mathcal{O} = (0, 1, 0)$. Étant donné que $\mathcal{O}$ est le seul point à l'infini, nous allons travailler en coordonnées non homogènes.

Soient $P = (p_1, p_2)$ et $Q = (q_1, q_2)$ deux points distincts de E.

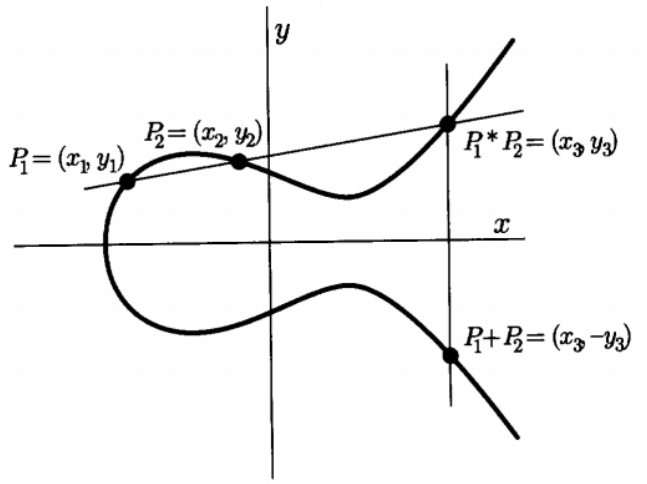

Figure 7: Addition de deux points sur une courbe de Weierstrass.

Calculons $-P = (x_{(-P)}, y_{(-P)})$, l'inverse du point P. Ce point appartient à la droite $L : x = p_1$, car $\mathcal{O} * \mathcal{O} = \mathcal{O}$. En substituant dans (IV.28), nous obtenons

$$\begin{aligned} f(p_1, y) &= y^2 + a_1 p_1 y + a_3 y - p_1^3 - a_2 p_1^2 - a_4 p_1 - a_6 \\ &= c(y - p_2)(y - y_{(-P)}) \\ &= cy^2 - c(p_2 + y_{(-P)})y + cp_2 y_{(-P)}. \end{aligned}$$

Si nous égalons les coefficients, nous avons $c = 1$ et $a_1 p_1 + a_3 = c(p_2 + y_{(-P)})$, et donc

$$-P = (p_1, -p_2 - a_1 p_1 - a_3). \tag{IV.29}$$

Addition des points P et Q (i) Si $p_1 = q_1$ et si $q_2 = -p_2 - a_1 p_1 - a_3$, alors

$$P + Q = \mathcal{O}.$$

(ii) Notons $R = (r_1, r_2)$, la somme de P et de Q. Remarquons que R n'est pas le point à l'infini (cas (i)). Supposons que $q_2 \neq -p_2 - a_1 p_1 - a_3$.
a) Si $p_1 \neq q_1$, posons

$$\lambda = \frac{q_2 - p_2}{q_1 - p_1} \quad \text{et} \quad \gamma = p_2 - \lambda p_1.$$

La sécante passant par P et Q a pour équation $y = \lambda x + \gamma$. En substituant dans (IV.28), nous avons

$$\begin{aligned} & f(x\ ,\ \lambda x+\gamma) \\ & \quad = (\lambda x+\gamma)^2 + a_1 x(\lambda x+\gamma) + a_3(\lambda x+\gamma) - x^3 - a_2 x^2 - a_4 x - a_6 \\ & \quad = -x^3 + (-a_2 + \lambda^2 + a_1\lambda)x^2 + (-a_4 + 2\lambda\gamma + a_1\gamma + a_3\lambda)x \\ & \qquad\quad -a_6 + \gamma^2 + a_3\gamma \\ & \quad = c(x-p_1)(x-q_1)(x-r_1) \\ & \quad = cx^3 - c(p_1+q_1+r_1)x^2 + c(q_1r_1+p_1q_1+p_1r_1)x - cp_1q_1r_1. \end{aligned}$$

Si nous égalons les coefficients, nous avons $c=-1$ et $-c(p_1+q_1+r_1) = -a_2+\lambda^2+a_1\lambda$, et donc

$$r_1 = -a_2 + \lambda^2 + a_1\lambda - p_1 - q_1, \tag{IV.30}$$
$$r_2 = -(\lambda r_1 + \gamma) - a_1 r_1 - a_3. \tag{IV.31}$$

b) Si $p_1 = q_1$, alors $P = Q$. L'addition de P et de Q revient alors à doubler le point P.

Doublement du point P Les formules vues ci-dessus restent valables, si ce n'est que maintenant λ représente le coefficient angulaire de la tangente à la courbe en P:

$$\lambda = \left.\frac{dy}{dx}\right|_P = -\frac{\frac{\partial f}{\partial x}(p_1,p_2)}{\frac{\partial f}{\partial y}(p_1,p_2)} = \frac{3p_1^2 + 2a_2p_1 + a_4 - a_1p_2}{2p_2 + a_1p_1 + a_3}.$$

Exemple 17. Soit la courbe elliptique

$$y^2 = x^3 + x + 1$$

définie sur $\mathbb{F}_{23}$. Les seuls points de cette courbe sont

$$\begin{array}{cccccccccc} (0,1) & (0,22) & (1,7) & (1,16) & (3,10) & (3,13) & (4,0) & (5,4) & (5,19) \\ (6,4) & (6,19) & (7,11) & (7,12) & (9,7) & (9,16) & (11,3) & (11,20) & (12,4) \\ (12,19) & (13,7) & (13,16) & (17,3) & (17,20) & (18,3) & (18,20) & (19,5) & (19,18) \end{array}$$

plus le point à l'infini $\mathcal{O}$. Prenons $P=(3,10)$ et $Q=(9,7)$. Calculons $R = P+Q$. Les formules précédentes donnent

$$\lambda = \frac{7-10}{9-3} = \frac{-3}{6} = \frac{-1}{2} = 11 \in \mathbb{F}_{23} \quad \text{et} \quad \gamma = 10 - 11\cdot 3 = -23 = 0 \in \mathbb{F}_{23},$$

$$\begin{cases} r_1 = -0 + 11^2 + 0\cdot 11 - 3 - 9 = 109 = 17 \in \mathbb{F}_{23} \\ r_2 = -(11\cdot 17 + 0) - 0\cdot 17 - 0 = -187 = -3 = 20 \in \mathbb{F}_{23} \end{cases}.$$

Par conséquent, $(3,10)+(9,7)=(17,20)$. Calculons maintenant $R=2P$. Les formules précédentes donnent

$$\lambda=\frac{3\cdot 3^2+2\cdot 0\cdot 3+1-0\cdot 10}{2\cdot 10+0\cdot 3+0}=\frac{28}{20}=\frac{5}{20}=\frac{1}{4}=6,$$

$$\gamma=10-6\cdot 3=-8=15,$$

$$\begin{cases} r_1=-0+6^2+0\cdot 6-3-3=30=7 \\ r_2=-(7\cdot 6+15)-0\cdot 6-0=-57=-11=12. \end{cases}$$

Par conséquent, $2(3,10)=(7,12)$.

Exemple 18. Soient le corps $\mathbb{F}_{2^4}$ généré par la racine α du polynôme irréductible sur $\mathbb{F}_2$ donné par $f(x)=x^4+x+1$ et la courbe elliptique

$$y^2+xy=x^3+\alpha^4x^2+1$$

définie sur $\mathbb{F}_{2^4}$. Avant toute chose, calculons les puissances successives de α

$$\begin{aligned}
\alpha^0&=[0001],\\
\alpha^1&=[0010],\\
\alpha^2&=[0100],\\
\alpha^3&=[1000],\\
\alpha^4&=\alpha+1=[0011],\\
\alpha^5&=\alpha^2+\alpha=[0110],\\
\alpha^6&=\alpha^3+\alpha^2=[1100],\\
\alpha^7&=\alpha^4+\alpha^3=\alpha^3+\alpha+1=[1011],\\
\alpha^8&=\alpha^4+\alpha^2+\alpha=\alpha^2+1=[0101],\\
\alpha^9&=\alpha^3+\alpha=[1010],\\
\alpha^{10}&=\alpha^4+\alpha^2=\alpha^2+\alpha+1=[0111],\\
\alpha^{11}&=\alpha^3+\alpha^2+\alpha=[1110],\\
\alpha^{12}&=\alpha^4+\alpha^3+\alpha^2=\alpha^3+\alpha^2+\alpha+1=[1111],\\
\alpha^{13}&=\alpha^4+\alpha^3+\alpha^2+\alpha=\alpha^3+\alpha^2+1=[1101],\\
\alpha^{14}&=\alpha^4+\alpha^3+\alpha=\alpha^3+1=[1001],\\
\alpha^{15}&=\alpha^4+\alpha=1=[0001].
\end{aligned}$$

Remarquons que pour être cohérent avec nos notations, nous aurions dû écrire l'équation de la courbe sous la forme

$$[0001]y^2+[0001]xy=[0001]x^3+[0011]x^2+[0001],$$

mais comme [0001] est l'identité multiplicative, la première écriture est correcte. Les seuls points de cette courbe sont

$$\begin{array}{cccccccc} (0,1) & (1,\alpha^6) & (1,\alpha^{13}) & (\alpha^3,\alpha^8) & (\alpha^3,\alpha^{13}) & (\alpha^5,\alpha^3) & (\alpha^5,\alpha^{11}) & (\alpha^6,\alpha^8) \\ (\alpha^6,\alpha^{14}) & (\alpha^9,\alpha^{10}) & (\alpha^9,\alpha^{13}) & (\alpha^{10},\alpha^1) & (\alpha^{10},\alpha^8) & (\alpha^{12},0) & (\alpha^{12},\alpha^{12}) & \end{array}$$

plus le point à l'infini $\mathcal{O}$. Prenons $P = (\alpha^6, \alpha^8)$ et $Q = (\alpha^3, \alpha^{13})$. Calculons $R = P + Q$. Par les formules précédentes,

$$\lambda = \frac{\alpha^{13} - \alpha^8}{\alpha^3 - \alpha^6} = \frac{(\alpha^3 + \alpha^2 + 1) + (\alpha^2 + 1)}{(\alpha^3) + (\alpha^3 + \alpha^2)} = \frac{\alpha^3}{\alpha^2} = \alpha,$$

$$\gamma = \alpha^8 - \alpha\alpha^6 = \alpha^8 + \alpha^7 = (\alpha^2) + (\alpha^3 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha = \alpha^{11},$$

$$\begin{cases} r_1 = -\alpha^4 + \alpha^2 + 1 \cdot \alpha - \alpha^6 - \alpha^3 = (\alpha + 1) + \alpha^2 + \alpha + (\alpha^3 + \alpha^2) + \alpha^3 \\ \quad = 1 \\ r_2 = -(\alpha \cdot 1 + \alpha^{11}) - 1 \cdot 1 - 0 = \alpha^3 + \alpha^2 + 1 = \alpha^{13} \end{cases}.$$

Par conséquent, $(\alpha^6, \alpha^8) + (\alpha^3, \alpha^{13}) = (1, \alpha^{13})$ ou de façon équivalente,

$$([1100], [0101]) + ([1000], [1101]) = ([0001], [1101]).$$

Calculons maintenant $R = 2P$. Par les formules précédentes,

$$\lambda = \frac{3\alpha^{12} + 2\alpha^4\alpha^6 + 0 - 1 \cdot \alpha^8}{2\alpha^8 + 1 \cdot \alpha^6 + 0} = \frac{\alpha^{12} + \alpha^8}{\alpha^6} = +\alpha^6 + \alpha^2 = \alpha^3,$$

$$\gamma = \alpha^8 - \alpha^3\alpha^6 = (\alpha^2 + 1) + (\alpha^3 + \alpha) = \alpha^{12},$$

$$\begin{cases} r_1 = -\alpha^4 + \alpha^6 + 1 \cdot \alpha^3 - \alpha^6 - \alpha^6 = \alpha^4 + \alpha^6 + \alpha^3 = \alpha^2 + \alpha + 1 = \alpha^{10} \\ r_2 = -(\alpha^3\alpha^{10} + \alpha^{12}) - 1 \cdot \alpha^{10} - 0 = \alpha^{13} + \alpha^{12} + \alpha^{10} = \alpha^2 + 1 = \alpha^8 \end{cases}.$$

Par conséquent, $2(\alpha^6, \alpha^8) = (\alpha^{10}, \alpha^8)$ ou de façon équivalente,

$$2([1100], [0101]) = ([0111], [0101]).$$

À retenir.

► Soit un corps K. Une *courbe elliptique* est une cubique irréductible non singulière de $\mathbb{P}_2(K)$ qui possède un point $\mathcal{O}$.

► Une *courbe elliptique* est une courbe birationnellement équivalente aux points de l'équation de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

plus le point à l'infini $\mathcal{O} = (0, 1, 0)$.

► Si $(E, \mathcal{O})$ est une courbe elliptique, alors l'opération $P+Q = \mathcal{O}*(P*Q)$ définit à un isomorphisme près une structure de *groupe commutatif* dont $\mathcal{O}$ est l'élément neutre où la loi de composition $P * Q$ définit le troisième point d'intersection de la droite passant passant par P et Q avec la courbe elliptique.

► Si une courbe elliptique est donnée par une équation de Weierstrass plus le point à l'infini $\mathcal{O}$, alors l'addition de deux points $P = (p_1, p_2)$ et $Q = (q_1, q_2)$ vaut

$\mathcal{O}$ si $q_1 = p_1$ et si $q_2 = -p_2 - a_1p_1 - a_3$;

$R = (r_1, r_2)$ où

$$\begin{cases} r_1 = -a_2 + \lambda^2 + a_1\lambda - p_1 - q_1, \\ r_2 = -(\lambda r_1 + \gamma) - a_1r_1 - a_3; \end{cases}$$

avec

$$\lambda = \frac{q_2 - p_2}{q_1 - p_1} \quad \text{si} \quad p_1 \neq q_1,$$
$$\lambda = \frac{3p_1^2 + 2a_2p_1 + a_4 - a_1p_2}{2p_2 + a_1p_1 + a_3} \quad \text{si} \quad p_1 = q_1$$
$$\text{et} \quad \gamma = p_2 - \lambda p_1.$$

Remarquons que $y = \lambda x + \gamma$ est soit la sécante passant par P et Q, soit la tangente à la courbe si $P = Q$.