# Résumé de cours sur les courbes elliptiques

Hugues Randriam

9 juin 2015

## 1 Définitions

**Définition 1.** — Une courbe elliptique sur un corps $K$ est la donnée de :
— une courbe algébrique (projective, lisse) $E$ de genre 1 sur $K$
— un certain point $O_E \in E(K)$.

**Définition 2.** — Une courbe elliptique sur un corps $K$ est la donnée d'une équation affine de la forme ("de Weierstrass")

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

qui définit une courbe plane $E$, les coefficients $a_1, a_2, a_3, a_4, a_6 \in K$ étant par ailleurs choisis de façon que $E$ soit *lisse*. La courbe $E$ admet alors un unique point à l'infini, noté $O_E$.

Lorsque $K$ est de caractéristique différente de 2 ou 3, un changement de variables permet de mettre l'équation sous la forme

$$y^2 = x^3 + ax + b$$

et la condition de lissité équivaut à demander que $x^3 + ax + b$ soit sans racine double, ou encore que son discriminant vérifie

$$\Delta = 4a^3 + 27b^2 \neq 0$$

dans $K$. [1]

1. Pour des raisons plus profondes, il serait préférable de normaliser le discriminant en $\Delta = -16(4a^3 + 27b^2)$ ; à notre niveau d'exposition cela ne change pas grand chose, nous conserverons la normalisation plus simple $\Delta = 4a^3 + 27b^2$.

Pour passer de la définition 1 à la définition 2, on utilise le lemme suivant qui est une conséquence directe du théorème de Riemann-Roch :

**Lemme 3.** — *Soient $E$ une courbe de genre 1 et $D$ un diviseur sur $E$ de degré $\deg(D) = d$. Alors*

$$\dim \mathcal{L}(D) = \begin{cases} 0 & si\ d < 0 \\ 0 & si\ d = 0\ et\ D \not\sim 0 \\ 1 & si\ d = 0\ et\ D \sim 0 \\ d & si\ d > 0. \end{cases}$$

Le lemme montre alors l'existence de fonctions $x$ et $y$ sur $E$ telles que les $i$ premiers éléments de la suite $(1, x, y, x^2, xy)$ forment une base de $\mathcal{L}(iO_E)$ pour $1 \leq i \leq 5$, et alors $(1, x, y, x^2, xy, x^3, y^2)$ est une famille liée dans $\mathcal{L}(6O_E)$, d'où on déduit l'équation de Weierstrass.

Dans l'autre sens, pour passer de la définition 2 à la définition 1, on peut par exemple utiliser la formule du genre, qui montre que l'équation définit bien une courbe de genre $\frac{(3-1)(3-2)}{2} = 1$.

On peut calculer le genre de $E$ d'une autre façon. Pour simplifier, supposons $K$ de caractéristique différente de 2 ou 3. Si $E$ admet l'équation affine

$$y^2 = x^3 + ax + b$$

en homogénéisant on trouve l'équation projective

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

et on peut passer de l'une à l'autre par les relations $x = X/Z$, $y = Y/Z$. Le point à l'infini est le point de coordonnées projectives

$$O_E = (0 : 1 : 0).$$

En faisant le changement de variables $u = X/Y = x/y$ et $v = Z/Y = 1/y$ on peut ramener $O_E$ en le point $u = v = 0$, et l'équation de la courbe dans ces nouvelles coordonnées affines devient

$$v = u^3 + auv^2 + bv^3.$$

En différenciant les équations affines on trouve les relations différentielles

$$2ydy = (3x^2 + a)dx, \quad (1 - 2auv - 3bv^2)dv = (3u^2 + av^2)du$$

et par ailleurs $dy = -dv/v^2$, de sorte qu'en posant

$$\omega = \frac{dx}{2y} = \frac{dy}{3x^2 + a} = \frac{-dv}{3u^2 + av^2} = \frac{-du}{1 - 2auv - 3bv^2}$$

on trouve que la différentielle $\omega$ n'admet ni zéro ni pôle sur $E$ (remarque : en $y = 0$ on a $3x^2 + a \neq 0$ car $x^3 + ax + b$ est sans racine double). Autrement dit $\mathrm{div}(\omega) = 0$, et la relation

$$\deg \mathrm{div}(\omega) = 2g - 2$$

permet de retrouver $g = 1$.

# 2 Loi de groupe

**Lemme 4.** — *Soit $D$ un diviseur de degré 0 sur $E$ sur $K$. Alors il existe un unique $P \in E(K)$ tel que*

$$D \sim (P) - (O_E).$$

L'existence s'obtient en appliquant le lemme 3 à $D + (O_E)$. On trouve $L(D + (O_E)) \neq 0$, et alors si $f \in L(D + (O_E))$ est non nulle, on a nécessairement $\mathrm{div}(f) = -D - (O_E) + (P)$ pour un certain $P$.

Pour l'unicité, on peut supposer par l'absurde qu'il existe deux points distincts $P, P'$ tels que $P \sim P'$, d'où une fonction $h$ telle que $\mathrm{div}(h) = (P') - (P)$, et alors $L(P)$ contient les deux fonctions 1 et $h$ linéairement indépendantes, ce qui contredit le lemme 3.

On peut traduire le lemme en disant qu'on obtient une *bijection*

$$\begin{array}{ccc} E(K) & \xrightarrow{\sim} & Cl^0(E)_K \\ P & \mapsto & (P) - (O_E) \end{array}$$

entre l'ensemble des points de $E$ sur $K$ et le groupe des classes d'équivalence linéaire de diviseurs de degré 0 définis sur $K$.

**Définition 5.** — On munit $E(K)$ d'une loi de groupe (notée $+$) en transportant la loi de $Cl^0(E)_K$ par cette bijection.

Par définition de cette loi de groupe on a donc :

(i) L'élément neutre de $E(K)$ est le point à l'infini $O_E$.

(ii) Pour $P, Q \in E(K)$, leur somme $P + Q$ dans $E(K)$ est l'unique point (donné par le lemme 3) tel que

$$(P) - (O_E) \ + \ (Q) - (O_E) \ \sim \ (P + Q) - (O_E)$$

dans le groupe des diviseurs de degré 0, c'est-à-dire l'unique point tel qu'il existe une fonction $f$ de diviseur

$$\mathrm{div}(f) = (P) + (Q) - (P + Q) - (O_E).$$

Plus généralement :

(iii) Considérons un diviseur $D$ sur $E$ de la forme $D = \sum_{P \in E(K)} n_P(P)$. Alors $D$ est principal (c'est-à-dire $D \sim 0$, *i.e.* il existe une fonction $f$ telle que $D = \mathrm{div}(f)$) si et seulement si

$$\deg(D) = \sum_P n_P = 0$$

et

$$\sum_P n_P P = O_E \qquad \text{dans } E(K).$$

En particulier :

(iv) On a

$$P + Q + R = O_E \qquad \text{dans } E(K)$$

si et seulement si

$$(P) - (O_E) \ + \ (Q) - (O_E) \ + \ (R) - (O_E) \ \sim \ 0$$

dans le groupe des diviseurs de degré 0, c'est-à-dire si et seulement s'il existe une fonction $f$ de diviseur

$$\mathrm{div}(f) = (P) + (Q) + (R) - 3(O_E).$$

(v) Pour tout $P \in E(K)$, son opposé $-P$ dans $E(K)$ est l'unique point tel qu'il existe une fonction $f$ de diviseur

$$\mathrm{div}(f) = (P) + (-P) - 2(O_E).$$

Les propriétés (iv) et (v) ci-dessus permettent de donner des formules explicites pour la loi de groupe. On supposera toujours $K$ de caractéristique différente de 2 ou 3, et $E$ donnée par l'équation $y^2 = x^3 + ax + b$ avec $\Delta = 4a^3 + 27b^2 \neq 0$ dans $K$.

Le principe général est le suivant : on a $P + Q + R = O_E$ si et seulement si $P, Q, R$ sont les trois points d'intersection (comptés convenablement) de $E$ et d'une droite. En effet si une droite donnée par la forme linéaire homogène $L(X, Y, Z) = 0$ intersecte $E$ en $P, Q, R$, alors la fonction $L(x, y, 1)$ admet pour diviseur $(P) + (Q) + (R) - 3(O_E)$ sur $E$. On trouve ainsi :

Tout d'abord, $O_E$ est l'élément neutre, donc

$$O_E + P = P + O_E = P$$

pour tout $P$. Ensuite, si $P$ est un point de coordonnées affines

$$P = \begin{vmatrix} x_P \\ y_P \end{vmatrix}$$

alors son opposé $-P$ a pour coordonnées

$$-P = \begin{vmatrix} x_P \\ -y_P \end{vmatrix}$$

(c'est le symétrique de $P$ par rapport à l'axe des $x$). En effet, la droite verticale passant par $P$ admet dans le plan l'équation affine $x - x_P$, et on vérifie $\mathrm{div}(x - x_P) = (P) + (-P) - 2(O_E)$ sur $E$ comme demandé dans (v).

Maintenant si

$$P = \begin{vmatrix} x_P \\ y_P \end{vmatrix} \qquad Q = \begin{vmatrix} x_Q \\ y_Q \end{vmatrix}$$

sont deux points sur $E$, avec $Q \neq \pm P$, c'est-à-dire $x_Q \neq x_P$, alors la droite passant par $P$ et $Q$ a pour équation affine $y = \lambda(x - x_P) + y_P$ où

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

et en remplaçant $y$ dans l'équation de la courbe on trouve un polynôme de degré 3 en $x$, dont les racines $x_P, x_Q, x_{P+Q}$ somment en $\lambda^2$, de sorte que

$$P + Q = \begin{vmatrix} x_{P+Q} = \lambda^2 - x_P - x_Q \\ y_{P+Q} = \lambda(x_P - x_{P+Q}) - y_P. \end{vmatrix}$$

Reste le cas particulier $x_Q = x_P$ c'est-à-dire $Q = \pm P$. Si $Q = -P$, alors

$$-P + P = O_E.$$

Enfin si $Q = P$, c'est-à-dire pour le calcul de $2P$, on doit considérer la tangente à $E$ en $P$. On peut supposer que $P$ n'est pas de 2-torsion (sinon, $P = -P$, $2P = O_E$), et cette tangente a pour équation affine $y = \lambda(x - x_P) + y_P$, où

$$\lambda = \frac{3x_P^2 + a}{2y_P}$$

s'obtient en différenciant l'équation de $E$ en $P$. On trouve alors par le même argument que précédemment

$$2P = \begin{vmatrix} x_{2P} = \lambda^2 - 2x_P \\ y_{2P} = \lambda(x_P - x_{2P}) - y_P. \end{vmatrix}$$

Notons par ailleurs que si $E$ est une courbe elliptique définie sur un corps $K$, et si $L$ est une extension de corps de $K$, alors on peut aussi considérer que $E$ est définie sur $L$. On vérifie alors aisément que :

**Proposition 6.** — *Le groupe $E(K)$ est un sous-groupe de $E(L)$.*

En fait, cela peut aussi se retrouver directement au moyen des formules explicites ci-dessus.

# 3 Points de torsion et polynômes de division

**Définition 7.** — Si $E$ est une courbe elliptique définie sur un corps $K$, on note $E[m]$ le groupe des points de $m$-torsion dans $E(\overline{K})$ (où $\overline{K}$ est une clôture algébrique de $K$), c'est-à-dire l'ensemble des points $P \in E(\overline{K})$ tels que $mP = O_E$.

Supposons maintenant $K$ de caractéristique différente de 2 ou 3.

**Exemple 8.** — Les points de 2-torsion de $E$ sont, d'une part $O_E$, ainsi que les points où $E$ admet une tangente verticale, c'est-à-dire de la forme $\begin{vmatrix} x \\ 0 \end{vmatrix}$ où $x$ est une racine de $x^3 + ax + b = 0$ dans $\overline{K}$.

On en déduit qu'en tant que groupe, $E[2]$ est toujours isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. Son sous-groupe $E[2] \cap E(K)$ sera isomorphe à $\{0\}$, à $\mathbb{Z}/2\mathbb{Z}$, ou à $(\mathbb{Z}/2\mathbb{Z})^2$, selon le nombre de racines de $x^3 + ax + b = 0$ dans $K$.

**Exemple 9.** — Les points de 3-torsion de $E$ sont ses points d'inflexion (sur $\overline{K}$), c'est-à-dire ceux où $E$ admet une tangente d'ordre 3. Par exemple $\begin{vmatrix} 0 \\ 1 \end{vmatrix}$ est de 3-torsion sur la courbe $y^2 = x^3 + 1$.

En appliquant itérativement les formules d'addition on montre par récurrence qu'il existe deux fractions rationnelles $F_m(x), G_m(x)$ telles que si $P = \begin{vmatrix} x \\ y \end{vmatrix}$ alors

$$mP = \begin{vmatrix} F_m(x) \\ yG_m(x). \end{vmatrix}$$

En particulier, $mP = O_E$ si et seulement si $x$ est un pôle de $F_m$. Or les formules de calcul de $F_m$ et $G_m$ par récurrence montrent que le dénominateur de $F_m$ est une puissance d'un polynôme $\psi_m$, appelé polynôme de $m$-division, de degré

$$\deg(\psi_m) = \begin{cases} \frac{m^2-1}{2} & \text{si } m \text{ impair} \\ 3 + \frac{m^2-4}{2} & \text{si } m \text{ pair.} \end{cases}$$

Par exemple, $\psi_2(x) = x^3 + ax + b$.

On en déduit :

**Théorème 10.** — *Pour tout entier $m \geq 1$, on a*

$$|E[m]| \leq m^2.$$

En effet, si $m$ impair, les points de $m$-torsion sont, d'une part $O_E$, et d'autre part les $\begin{vmatrix} x \\ \pm y \end{vmatrix}$ pour $x$ racine de $\psi_m$ et $y^2 = x^3 + ax + b$. Il y en a donc au plus $1 + 2 \deg \psi_m = m^2$. On raisonne de même pour $m$ pair.

(En fait on a un résultat de structure plus précis : voir le théorème 20.)

On remarquera que pour $m$ grand, il n'est pas possible en pratique d'écrire les fonctions $F_m$ et $G_m$ par récurrence pour le calcul de $mP$. On utilisera plutôt une méthode de type *exponentiation rapide*, par exemple :

$$18 \cdot P = 2 \cdot (2 \cdot 2 \cdot 2 \cdot P + P)$$

$$42 \cdot P = 2 \cdot (2 \cdot 2 \cdot (2 \cdot 2 \cdot P + P) + P)$$

$$666 \cdot P = 2 \cdot (2 \cdot 2 \cdot (2 \cdot (2 \cdot 2 \cdot 2 \cdot (2 \cdot 2 \cdot P + P) + P) + P) + P).$$

Plus généralement l'algorithme est le suivant : on écrit sous forme binaire $m = 2^k + b_{k-1}2^{k-1} + \cdots + b_1 2 + b_0$, on initialise $Q = P$, puis pour $i$ allant de $k-1$ à 0 on remplace $Q$ par $2Q + b_i P$, et enfin on renvoie $Q$. La complexité totale est de $k$ multiplications par 2 et au plus $k$ additions, où $k \approx \log_2 m$.

# 4 Structure du groupe des points

**Théorème 11.** — *Soit $E$ une courbe elliptique définie sur le corps fini $\mathbb{F}_q$. Alors $E(\mathbb{F}_q)$ est produit d'au plus deux groupes cycliques, c'est-à-dire*

— *ou bien on a un isomorphisme*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/N\mathbb{Z}$$

— *ou bien on a un isomorphisme*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$$

*pour deux entiers avec la condition de divisibilité*

$$s | r \qquad s > 1.$$

La preuve s'obtient en remarquant que $E(\mathbb{F}_q)[m] = E(\mathbb{F}_q) \cap E[m] \subset E[m]$ pour tout $m$, et on conclut par le théorème 10 joint au théorème de structure des groupes abéliens finis.

Remarquons que le premier cas $E(\mathbb{F}_q) \simeq \mathbb{Z}/N\mathbb{Z}$ signifie que $E(\mathbb{F}_q)$ contient un point $P_0$ d'ordre $N$, et que l'isomorphisme est donné par

$$\begin{array}{ccc} \mathbb{Z}/N\mathbb{Z} & \xrightarrow{\sim} & E(\mathbb{F}_q) \\ k \mod N & \mapsto & kP_0 \end{array}$$

tandis que $E(\mathbb{F}_q) \simeq \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$ signifie que $E(\mathbb{F}_q)$ contient deux points $P_1, P_2$ d'ordre $r, s$ respectivement, et que l'isomorphisme est donné par

$$\begin{array}{ccc} \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z} & \xrightarrow{\sim} & E(\mathbb{F}_q) \\ (j \mod r, k \mod s) & \mapsto & jP_1 + kP_2. \end{array}$$

En général il n'y a pas de méthode évidente pour trouver ces générateurs.

**Théorème 12** (Hasse)**.** — *Soit $E$ une courbe elliptique définie sur le corps fini $\mathbb{F}_q$. Alors l'ordre du groupe $E(\mathbb{F}_q)$ s'écrit*

$$|E(\mathbb{F}_q)| = q + 1 - t$$

*pour un certain entier $t$ de valeur absolue*

$$|t| \leq 2\sqrt{q}.$$

Ainsi on a l'encadrement $(\sqrt{q}-1)^2 \leq |E(\mathbb{F}_q)| \leq (\sqrt{q}+1)^2$. Par la proposition 6 un résultat analogue vaut encore lorsqu'on remplace $\mathbb{F}_q$ par une extension $\mathbb{F}_{q^r}$.

**Exemple 13.** — La courbe $E$ d'équation $y^2 = x^3 - x$ définie sur $\mathbb{F}_5$ a pour discriminant $\Delta = 1 \neq 0$. Les points de $E$ à coordonnées dans $\mathbb{F}_5$ sont

$$O_E \quad \begin{vmatrix}0\\0\end{vmatrix} \quad \begin{vmatrix}1\\0\end{vmatrix} \quad \begin{vmatrix}2\\1\end{vmatrix} \quad \begin{vmatrix}2\\4\end{vmatrix} \quad \begin{vmatrix}3\\2\end{vmatrix} \quad \begin{vmatrix}3\\3\end{vmatrix} \quad \begin{vmatrix}4\\0\end{vmatrix}$$

de sorte que $|E(\mathbb{F}_5)| = 8$, et par le théorème de structure, il n'y a que deux possibilités à considérer : ou bien $E(\mathbb{F}_5) \simeq \mathbb{Z}/8\mathbb{Z}$ est cyclique, ou bien sinon $E(\mathbb{F}_5) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On remarque que $E(\mathbb{F}_5)$ contient 4 points de 2-torsion, qui sont $O_E \begin{vmatrix}0\\0\end{vmatrix} \begin{vmatrix}1\\0\end{vmatrix} \begin{vmatrix}4\\0\end{vmatrix}$ et ceci exclut la possibilité $E(\mathbb{F}_5) \simeq \mathbb{Z}/8\mathbb{Z}$ (ce dernier n'ayant que 2 points de 2-torsion). Ainsi

$$E(\mathbb{F}_5) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

et comme premier générateur on peut prendre n'importe quel point d'ordre 4, par exemple

$$P_1 = \begin{vmatrix}2\\1.\end{vmatrix}$$

Les formules donnent alors

$$2P_1 = \begin{vmatrix}0\\0\end{vmatrix} \qquad 3P_1 = \begin{vmatrix}2\\4.\end{vmatrix}$$

Comme second générateur on peut alors prendre

$$P_2 = \begin{vmatrix}1\\0\end{vmatrix}$$

et on trouve de même

$$P_1 + P_2 = \begin{vmatrix}3\\3\end{vmatrix} \qquad 2P_1 + P_2 = \begin{vmatrix}4\\0\end{vmatrix} \qquad 3P_1 + P_2 = \begin{vmatrix}3\\2.\end{vmatrix}$$

# 5 Morphismes de courbes elliptiques (isogénies)

**Définition 14.** — Un morphisme (aussi appelé isogénie s'il est non constant) entre deux courbes elliptiques $E$ et $E'$ est un morphisme algébrique $f$ entre $E$ et $E'$ qui envoie $O_E$ sur $O_{E'}$.

En coordonnées affines, si $E$ est donné par l'équation $y^2 = x^3 + ax + b$ et $E'$ par $y^2 = x^3 + a'x + b'$, un morphisme $f$ entre $E$ et $E'$ pourra s'écrire sous la forme $(x, y) \mapsto (F(x, y), G(x, y))$ où $F$ et $G$ sont des fonctions rationnelles telles que $y^2 = x^3 + ax + b \implies G(x, y)^2 = F(x, y)^3 + a'F(x, y) + b'$. En particulier $f$ induit une application de $E(K)$ dans $E'(K)$. On montre :

**Proposition 15.** — *Si $f$ est un morphisme entre deux courbes elliptiques $E$ et $E'$, alors l'application*

$$E(K) \longrightarrow E'(K)$$

*qui s'en déduit est un morphisme de groupes.*

Évidemment ceci vaut encore si on remplace $K$ par une extension $L$.

**Exemple 16.** — Pour tout $u \in K^\times$, la transformation plane $(x, y) \mapsto (u^2x, u^3y)$ définit un isomorphisme de la courbe $y^2 = x^3 + ax + b$ avec la courbe $y^2 = x^3 + au^4x + bu^6$.

On remarquera que ce changement de variables laisse invariant le rapport $4a^3/(4a^3 + 27b^2)$ qu'on appellera $j$-invariant de l'équation. [2] Inversement on vérifie facilement que :

- deux courbes ont même $j$-invariant si et seulement si elles sont isomorphes sur $\overline{K}$ (mais pas forcément sur $K$)
- pour tout choix de $j \in K$, il existe une courbe définie sur $K$ dont le $j$-invariant est égal à $j$.

Ainsi le $j$-invariant paramétrise les classes d'isomorphisme de courbes elliptiques sur $\overline{K}$, et détermine en outre pour chaque classe le plus petit corps sur lequel on peut en construire un représentant.

**Exemple 17.** — Soit $K$ un corps contenant un élément $i$ tel que $i^2 = -1$, par exemple $K = \mathbb{F}_5$, $i = 2$. Alors la transformation plane $(x, y) \mapsto (-x, iy)$ définit un isomorphisme de la courbe $y^2 = x^3 - x$ dans elle-même.

2. Pour des raisons plus profondes, il serait préférable de normaliser le $j$-invariant en $j = 1728 \cdot 4a^3/(4a^3 + 27b^2)$ ; à notre niveau d'exposition cela ne change pas grand chose, nous conserverons la normalisation plus simple $j = 4a^3/(4a^3 + 27b^2)$.

Avec les notations de l'exemple 13, on voit que ce morphisme envoie $P_1$ sur $3P_1 + P_2$, et envoie $P_2$ sur $2P_1 + P_2$. Ses points fixes sont $O_E$ et $2P_1$.

**Exemple 18.** — Pour toute courbe elliptique $E$ et pour tout entier $m$, l'application de multiplication par $m$ (donnée par les formules de la loi de groupe) est un morphisme de $E$ dans elle-même.

**Exemple 19.** — Pour toute courbe elliptique $E$ sur $\mathbb{F}_q$, la transformation $(x, y) \mapsto (x^q, y^q)$ définit un morphisme $\varphi$ de $E$ dans elle-même, appelé morphisme de Frobenius. On vérifie que $\varphi$ induit l'identité sur $E(\mathbb{F}_q)$, cependant $\varphi \neq \mathrm{id}$ en tant que morphisme de $E$. D'ailleurs, passant à une extension $\mathbb{F}_{q^r}$, on vérifie que $\varphi$ n'est pas l'identité sur $E(\mathbb{F}_{q^r})$, et plus précisément on a $\varphi(P) = P$ si et seulement si $P \in E(\mathbb{F}_q)$.

On montre que si $f : E \longrightarrow E'$ et $g : E' \longrightarrow E''$ sont des morphismes de courbes elliptiques, alors $g \circ f : E \longrightarrow E''$ est un morphisme. De même si $f, g$ sont deux morphismes $E \longrightarrow E'$, alors $f + g$ (défini par la loi de groupe sur $E'$) en est un aussi.

Si l'on s'intéresse uniquement à l'ensemble $\mathrm{End}(E)$ des morphismes d'une courbe $E$ dans elle-même, on vérifie que ces opérations munissent $\mathrm{End}(E)$ d'une structure d'anneau. On l'appelle anneau des endomorphismes de $E$. Dans ce langage, avec les notations de l'exemple 19, $\mathrm{id} - \varphi$ est un endomorphisme de $E$, et on a la caractérisation de $E(\mathbb{F}_q)$ comme

$$E(\mathbb{F}_q) = \ker(\mathrm{id} - \varphi).$$

En poursuivant ce genre de considérations, on pourrait arriver à une preuve du théorème de Hasse, comme suit.

Tout d'abord, on pourrait raffiner le théorème 10 en :

**Théorème 20.** — *Sur un corps de caractéristique $p$, on a un isomorphisme*

$$E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2 \qquad \textit{pour tout } m \textit{ tel que } p \nmid m$$

*tandis que*

$$E[p^n] \simeq \{0\} \textit{ ou } \mathbb{Z}/p^n\mathbb{Z}.$$

De ce résultat, on déduit que $\mathrm{End}(E)$ "ressemble" à un sous-anneau de $M_2(\mathbb{Z})$, et que la fonction degré sur $\mathrm{End}(E)$ se comporte comme un déterminant. Plus précisément :

— $\mathrm{End}(E)$ est un $\mathbb{Z}$-module de rang au plus 4
— la fonction $f \mapsto \deg(f)$ est une forme quadratique sur $\mathrm{End}(E)$
— tout $f \in \mathrm{End}(E)$ admet un polynôme caractéristique

$$\chi_f(X) = \deg(X \cdot \mathrm{id} - f) \in \mathbb{Z}[X]$$

unitaire de degré 2 ; son coefficient constant est $\chi_f(0) = \deg(f)$, et de plus on a $\chi_f(f) = 0$ dans $\mathrm{End}(E)$.

On montre que le Frobenius $\varphi$ est de degré $\deg(\varphi) = q$, donc son polynôme caractéristique est de la forme

$$\chi_\varphi(X) = X^2 - tX + q$$

pour un certain $t$.

Pour tous $m, n$ on a alors $0 \leq \deg(m\mathrm{id} - n\varphi) = m^2 - tmn + qn^2$, d'où l'on déduit que $\chi_\varphi$ a au plus une racine réelle, donc son discriminant vérifie

$$t^2 - 4q \leq 0.$$

On conclut alors par $|E(\mathbb{F}_q)| = |\ker(\mathrm{id} - \varphi)| = \deg(\mathrm{id} - \varphi) = \chi_\varphi(1)$.

# 6 Critère de principalité constructif

On revient sur le point (iii) page 4 : un diviseur $D = \sum_{P \in E(K)} n_P(P)$ est principal si et seulement si

— $\sum_P n_P = 0$ dans $\mathbb{Z}$, et
— $\sum_P n_P P = O_E$ dans le groupe $E(K)$.

On va rendre ce critère de principalité plus constructif, sous la forme suivante : si un diviseur s'écrit

$$D = (P_1) + \cdots + (P_n) - (Q_1) - \cdots - (Q_n)$$

avec

$$P_1 + \cdots + P_n = Q_1 + \cdots + Q_n$$

alors on peut construire explicitement une fonction $f$ telle que

$$\mathrm{div}(f) = D.$$

Pour cela on procède par récurrence sur $n$. Le résultat est trivial si $n = 0$ ou même si $n = 1$ : alors $D = 0$ et on peut prendre $f$ constante.

On suppose maintenant le résultat vrai pour $n-1$. On pose

$$\widetilde{D} = (P_1) + \cdots + (P_{n-2}) + (\widetilde{P_{n-1}}) - (Q_1) - \cdots - (Q_{n-2}) - (\widetilde{Q_{n-1}})$$

où

$$\widetilde{P_{n-1}} = -Q_{n-1} - Q_n \qquad \text{et} \qquad \widetilde{Q_{n-1}} = -P_{n-1} - P_n$$

de sorte que l'hypothèse de récurrence s'applique, ce qui signifie qu'on peut construire une fonction $g$ telle que

$$\mathrm{div}(g) = \widetilde{D}.$$

On continue alors en utilisant le lemme suivant, qui est une simple reformulation de la construction de la loi de groupe sur $E(K)$ :

**Lemme 21.** — *Soient $P, Q \in E(K)$ et $\lambda X + \mu Y + \nu Z$ l'équation homogène de la droite $(PQ)$ (ou de la tangente à $E$ en $P$ si $P = Q$). Alors la fonction affine*

$$l_{P,Q} = \lambda x + \mu y + \nu$$

*admet pour diviseur*

$$\mathrm{div}(l_{P,Q}) = (P) + (Q) + (-P - Q) - 3(O_E).$$

Ce lemme nous permet de poser

$$f = g \cdot l_{P_{n-1},P_n} / l_{Q_{n-1},Q_n}$$

et on trouve effectivement

$$\mathrm{div}(f) = \widetilde{D} + \mathrm{div}(l_{P_{n-1},P_n}) - \mathrm{div}(l_{Q_{n-1},Q_n}) = D$$

comme annoncé.

# 7 Couplages

**Définition 22.** — Soient $\mathbb{A}, \mathbb{B}, \mathbb{G}$ trois groupes abéliens, avec $\mathbb{A}, \mathbb{B}$ notés additivement et $\mathbb{G}$ multiplicativement. Un couplage entre $\mathbb{A}$ et $\mathbb{B}$ à valeurs dans $\mathbb{G}$ est une application

$$e : \mathbb{A} \times \mathbb{B} \longrightarrow \mathbb{G}$$

qui est bilinéaire, c'est-à-dire telle que

$$e(a+a',b) = e(a,b)e(a',b)$$

$$e(a,b+b') = e(a,b)e(a,b')$$

pour tous $a, a' \in \mathbb{A}$, $b, b' \in \mathbb{B}$.

(Un cas important est celui où $\mathbb{A} = \mathbb{B}$, les informaticiens parlent alors parfois de couplage "de type 1".)

Les courbes elliptiques donnent lieu à la définition de plusieurs couplages intéressants. On va construire ici le couplage de Weil, qui est le premier historiquement et probablement le plus important mathématiquement. En cryptographie on utilise aussi le couplage de Tate (et encore d'autres variantes), dont la définition utilise des ingrédients assez similaires.

On travaille sur le corps fini $K = \mathbb{F}_q$, où $q = p^r$, et on fixe une clôture algébrique $\overline{K}$. On se donne un entier $m$ tel que $p \not| m$. On note

$$\boldsymbol{\mu}_m \subset \overline{K}^\times$$

le groupe des racines $m$-ièmes de l'unité, qui est un groupe cyclique d'ordre $m$. On rappelle aussi que

$$E[m] \subset E(\overline{K})$$

le groupe des points de $m$-torsion de $E$, est un produit de deux groupes cycliques d'ordre $m$ (théorème 20).

On considère le diviseur

$$\begin{aligned} D_{P,Q} = (P) + (P+Q) + (P+2Q) + \cdots + (P+(m-1)Q) \\ - (O_E) - (Q) - (2Q) - \cdots - ((m-1)Q). \end{aligned}$$

Quitte à remplacer $K$ par $\overline{K}$, ce diviseur vérifie les hypothèse du critère de principalité de la section 6, donc on peut construire une fonction $f_{P,Q}$ telle que

$$\operatorname{div}(f_{P,Q}) = D_{P,Q}.$$

Notons maintenant $\tau_Q : E \longrightarrow E$ l'application de translation par $Q$. C'est un morphisme algébrique (mais pas une isogénie, puisque ne préservant pas $O_E$). Si $f$ est une fonction sur $E$, alors $\tau_Q^* f$ est la fonction sur $E$ définie par

$$\tau_Q^* f(R) = f(R+Q)$$

en tout point $R$. Son diviseur $\mathrm{div}(\tau_Q^* f)$ est translaté de $\mathrm{div}(f)$ par $-Q$. Or $D_{P,Q}$ est invariant par translation par $\pm Q$, de sorte que

$$\mathrm{div}(\tau_Q^* f_{P,Q}) = D_{P,Q} = \mathrm{div}(f_{P,Q})$$

et le quotient $c = \tau_Q^* f_{P,Q}/f_{P,Q}$ est une constante. Ainsi, pour tout point $R$ on a

$$f_{P,Q}(R+Q) = c f_{P,Q}(R).$$

On trouve alors par récurrence $f_{P,Q}(R+kQ) = c^k f_{P,Q}(R)$, et pour $k=m$, on en déduit $c^m = 1$, c'est-à-dire $c \in \boldsymbol{\mu}_m$.

**Définition 23.** — On appelle couplage de Weil l'application

$$\begin{array}{rccc} e_m : & E[m] \times E[m] & \longrightarrow & \boldsymbol{\mu}_m \\ & (P,Q) & \mapsto & c = \tau_Q^* f_{P,Q}/f_{P,Q} \end{array}$$

ainsi construite.

**Théorème 24.** — *Cette application est bien un couplage, autrement dit, elle vérifie les propriétés de bilinéarité :*

*(i)* $e_m(P+P',Q) = e_m(P,Q)e_m(P',Q)$

*(ii)* $e_m(P,Q+Q') = e_m(P,Q)e_m(P,Q')$.

*De plus on a les propriétés supplémentaires :*

*(iii)* $e_m(P,P) = 1$

*(iv) si* $P,Q \in E(K) \cap E[m]$, *alors* $e_m(P,Q) \in K$

*(v)* $e_m : E[m] \times E[m] \twoheadrightarrow \boldsymbol{\mu}_m$ *est surjective.*

Nous prouvons seulement (i)(iii)(iv). Les propriétés (ii) et (v) sont un peu plus difficiles et seront admises.

Pour (i), on remarque qu'on peut choisir $f_{P+P',Q} = f_{P,Q} \cdot \tau_{-P}^* f_{P',Q}$. Pour (iii), on note que $D_{P,P} = 0$ donc $f_{P,P}$ est constante, et a fortiori invariante sous $\tau_P$. Enfin pour (iv), on remarque que dans la construction donnée dans la section 6, dès lors que tous les points sont à coordonnées dans $K$, alors la fonction obtenue est définie sur $K$.

**Exemple 25.** — La courbe elliptique $E$ d'équation $y^2 = x^3 + 2$ sur $\mathbb{F}_7$ a discriminant $\Delta = 3$ et $j$-invariant $j = 0$. Ses points à coordonnées dans $\mathbb{F}_7$ sont

$$O_E \quad \begin{vmatrix} 0 \\ 3 \end{vmatrix} \quad \begin{vmatrix} 0 \\ 4 \end{vmatrix} \quad \begin{vmatrix} 3 \\ 1 \end{vmatrix} \quad \begin{vmatrix} 3 \\ 6 \end{vmatrix} \quad \begin{vmatrix} 5 \\ 1 \end{vmatrix} \quad \begin{vmatrix} 5 \\ 6 \end{vmatrix} \quad \begin{vmatrix} 6 \\ 1 \end{vmatrix} \quad \begin{vmatrix} 6 \\ 6 \end{vmatrix}$$

de sorte que $|E(\mathbb{F}_7)| = 9$, et par le théorème de structure, $E(\mathbb{F}_7) \simeq \mathbb{Z}/9\mathbb{Z}$ ou $(\mathbb{Z}/3\mathbb{Z})^2$. Un calcul rapide montre qu'on est dans le second cas, et plus précisément, en posant $P = \begin{vmatrix} 0 \\ 3 \end{vmatrix}$ et $Q = \begin{vmatrix} 3 \\ 1 \end{vmatrix}$, on vérifie que $P$ et $Q$ sont d'ordre 3 et que l'addition dans $E(\mathbb{F}_7)$ est décrite par la table :

| $+$ | $O_E$ | $P$ | $2P$ |
|---|---|---|---|
| $O_E$ | $O_E$ | $\begin{vmatrix} 0 \\ 3 \end{vmatrix}$ | $\begin{vmatrix} 0 \\ 4 \end{vmatrix}$ |
| $Q$ | $\begin{vmatrix} 3 \\ 1 \end{vmatrix}$ | $\begin{vmatrix} 6 \\ 1 \end{vmatrix}$ | $\begin{vmatrix} 5 \\ 1 \end{vmatrix}$ |
| $2Q$ | $\begin{vmatrix} 3 \\ 6 \end{vmatrix}$ | $\begin{vmatrix} 5 \\ 6 \end{vmatrix}$ | $\begin{vmatrix} 6 \\ 6 \end{vmatrix}$ |

Ainsi on a

$$E[3] = E(\mathbb{F}_7)$$

et par ailleurs

$$\boldsymbol{\mu}_3 = \{1, 2, 4\} \subset \mathbb{F}_7$$

(en effet, $1^3 = 2^3 = 4^3 = 1$ sont les solutions de $x^3 = 1$ dans $\overline{\mathbb{F}_7}$).

Calculons $e_3(P, Q)$.

Pour cela, tout d'abord on cherche une fonction $f$ de diviseur

$$\mathrm{div}(f) = (P) + (P + Q) + (P + 2Q) - (O_E) - (Q) - (2Q).$$

On vérifie que

$$f = \frac{y - 2x - 3}{x - 3}$$

convient : elle s'annule bien à l'ordre 1 en $P$, $P+Q$, et $P+2Q$, et admet des pôles simples en $O_E$, $Q$, et $2Q$. Par ailleurs on calcule facilement ses valeurs en les trois points restants de $E(F_7)$ :

$$f(2P) = 2, \qquad f(2P + Q) = 1, \qquad f(2P + 2Q) = 4.$$

La valeur cherchée est donc

$$e_3(P, Q) = \tau_Q^* f / f = f(R + Q)/f(R)$$

pour tout point $R$ hors des zéros et pôles de $f$. En choisissant par exemple $R = 2P$ (mais tout autre choix donnerait le même résultat) on trouve

$$e_3(P, Q) = 1/2 = 4.$$