Les courbes elliptiques

Jérôme Levie
pour le groupe de travail : «Exemples de groupes» organisé par Frédéric Paulin

15 juin 2001

Table des matières

Introduction

Les courbes elliptiques forment un sujet très vaste en mathématiques. Leur étude fut au départ motivée par l'étude des fonctions elliptiques par les mathématiciens du dix-neuvième siècle. Ensuite le domaine connut un essor phénoménal dans diverses directions, notamment vers la démonstration du théorème de Fermat.

Dans ce travail, nous commencerons par détailler la construction géométrique de la loi de groupe sur une courbe elliptique, définie sur un corps algébriquement clos. Nous donnerons quelques exemples, puis la démontrerons en utilisant des techniques élémentaires de géométrie algébrique. Nous en profiterons pour donner quelques propriétés de base des courbes elliptiques vues comme courbes algébriques.

Ensuite, nous montrerons comment les fonctions $\mathscr{P}$ de Weierstrass permettent d'«uniformiser» une courbe elliptique, c'est-à-dire de la réaliser comme un quotient de $\mathbb{C}$ par un réseau plein (de dimension réelle deux).

1 La définition des courbes elliptiques et de leur loi de groupe

1.1 La forme normale de Weierstrass

Définition 1. *Une courbe elliptique est une cubique $\mathscr{C}$ de $\mathbb{P}^2(\mathbb{C})$, non singulière, munie d'un point O et de la structure de groupe correspondante.*

Nous détaillerons plus loin ce qui concerne la structure de groupe. En général, une telle courbe a une équation du type

$$\mathscr{C} \equiv aw^3 + bwx^2 + cwy^2 + dwxy + ewx^2 + fw^2y + gx^3 + hy^3 + px^2y + qxy^2 = 0$$

Proposition 1. *Si $\mathscr{C}$ est une courbe elliptique, on a un point d'inflexion $(1 : r : s) \in \mathbb{P}^2(\mathbb{C})$.*

Démonstration. Soit $\mathscr{C}$ définie par un polynôme f, au voisinage de $(1 : r : s) \in \mathbb{P}^2(\mathbb{C})$. Si

$$f(1, x + r, y + s) = f_1(r, s)(x, y) + f_2(r, s)(x, y) + f_3(r, s)(x, y),$$

$(1 : r : s)$ est un point singulier si et seulement si $f_1(r, s)(x, y) \neq 0$; $(1 : r : s)$ est un point d'inflexion si et seulement si $f_1 | f_2$ dans $k[x, y]$. Cette condition est équivalente à l'annulation du résultant $R(r, s) = R(f_1(r, s), f_2(r, s)) = 0$. Cette dernière équation a toujours une solution dans $\mathbb{C}^2$. □

En envoyant le point d'inflexion à l'infini, ramenant ainsi la courbe dans le plan (x, y) (à part bien sûr le point d'inflexion), et en faisant des changements d'échelle évidents, on arrive à la forme

$$\mathscr{C} \equiv y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

En complétant le carré à gauche (c'est-à-dire en faisant le changement de variables $y' = y - \frac{a_1x}{2}$), on obtient

$$\mathscr{C} \equiv y^2 + b_3y = x^3 + b_2x^2 + b_4x + b_6.$$

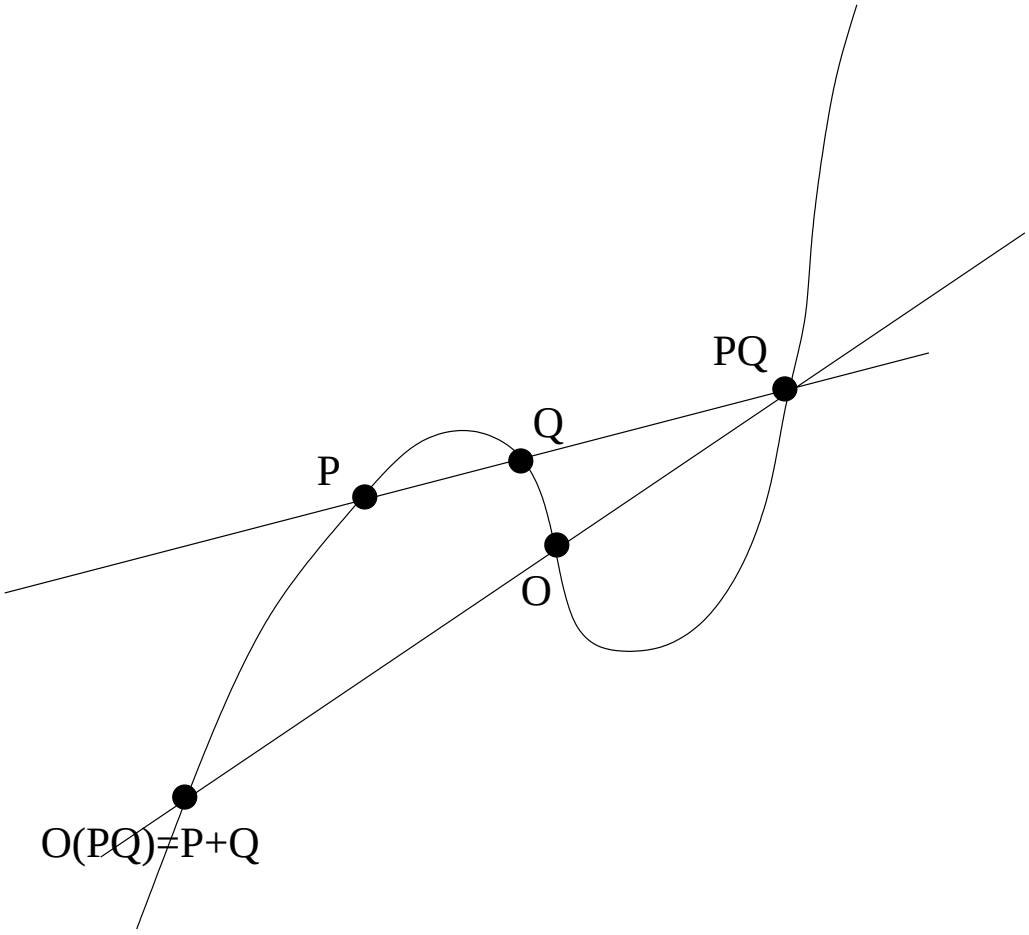
Enfin, si on pose $x' = x - \frac{a_2}{3}$, on obtient la forme normale de Weierstrass [2]

$$\mathscr{C} \equiv y^2 = 4x^3 - g_2x - g_3.$$

Sur cette forme, on vérifie facilement que la non-singularité de $\mathscr{C}$ est équivalente à la propriété $\Delta = g_2^3 - 27g_3^2 \neq 0$ (Δ est appelé le discriminant de la courbe elliptique). On définit également l'invariant $j(\mathscr{C}) = 12^3 \frac{g_2^3}{\Delta}$. Définissons maintenant la structure de groupe sur $\mathscr{C}$. Si $P, Q \in \mathscr{C}$, génériquement la droite passant par P et Q coupe une troisième fois la cubique (pour les cas non génériques, on considérera un point de tangence comme un point

d'intersection double), notons ce point PQ. Le point $P+Q$ est alors défini comme le point $O(PQ)$ (voir figure).

La commutativité de cette loi est évidente ; il est également immédiat que O est un neutre pour cette loi. Avant de démontrer l'associativité, faisons quelques remarques sur le groupe obtenu.



1.2 Remarques sur la loi de groupe

Revenons, pour un bref instant, à une courbe elliptique sur $\mathbb{Q}$ [2, 6]. Le théorème fondamental est le théorème de Mordell, sur les «points rationnels» $\mathscr{C}(\mathbb{Q})$ (c'est-à-dire les points de la courbe elliptique considérée sur $\mathbb{Q}$).

Théorème 1. *Soit $\mathscr{C}$ une courbe elliptique. Alors l'ensemble $\mathscr{C}(\mathbb{Q})$ de ses points rationnels est un groupe de type fini, isomorphe, modulo la torsion (*id est *les points $X \in \mathscr{C}$ tels qu'il existe $n \in \mathbb{N}_0$ avec $nX = 0$) à $\mathbb{Z}^r$.*

Le nombre r est appelé le rang de la courbe. Un des sports favoris des mathématiciens est de construire des courbes elliptiques de grand rang sur $\mathbb{Q}$. À ma connaissance, le record mondial est de 14. Signalons à ce propos la conjecture de Birch-Swinnerton-Dyes, affirmant que le rang d'une courbe elliptique $\mathscr{C}(Q)$ est l'ordre du zéro $s = 1$ de la fonction $L_{\mathscr{C}}(s)$ de la courbe.

Étudions maintenant les points de torsion du groupe. Par exemple, le point $(-2, 0)$ de la courbe $\mathscr{C} \equiv y^2 = x^3 + 8$ est de 2-torsion, le point $(1, 1)$

de la courbe $\mathscr{C} \equiv y^2 + y = x^3 - x^2$ est d'ordre 5... Le théorème de Nagell-Lutz, lui, affirme qu'un point de torsion rationnel d'une courbe elliptique à coefficients entiers est à coordonnées entières. Le théorème de Mazur permet enfin de caractériser la torsion rationnelle

$$\begin{array}{rcl} \mathrm{Tor}\left(\mathscr{C}\left(\mathbb{Q}\right)\right) & \simeq & \mathbb{Z}/m\mathbb{Z} \text{ avec } m \in \{1, 2, \ldots, 10, 12\} \\ & \text{ou} & \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \text{ avec } m \in \{2, 4, 6, 8\}. \end{array}$$

1.3 Démonstration de l'associativité

Commençons par quelques remarques sur les courbes algébriques. L'espace $k[X_0, \ldots, X_N]_d$ des polynômes homogènes de degré en $N+1$ variables est un espace vectoriel de dimension C^N_{N+d}, l'espace projectif $\mathbb{P}(k[X_0, \ldots, X_N]_d)$ est donc de dimension $C^N_{N+d} - 1$. Nous pouvons en déduire que, si $m \geq C^d_{N+d} - 1$, il existe toujours une courbe de degré d passant par m points donnés. Dans le cas $N = 2$ qui nous intéressera plus particulièrement, $C^2_{d+2} - 1 = \frac{d(d+3)}{2}$. Un théorème important de géométrie algébrique, appelé théorème de Bezout, affirme que deux courbes algébriques définies par deux polynômes homogènes premiers entre eux, de degrés p et q, se rencontrent en exactement mn points, comptés avec multiplicité. La proposition suivante est un corollaire de ce théorème. Nous en donnons néanmoins une démonstration directe, utilisant les propriétés du résultant.

Proposition 2. *Soient $\mathscr{C}$, $\mathscr{C}'$ deux courbes algébriques de degrés p et q sur k. Si elles ont strictement plus de pq points d'intersection, alors elles ont une composante commune.*

Preuve : Soient $P(X_0, \ldots, X_N) = \sum_{i=0}^{m} a_i X^{m-i}$, $P'(X_0, \ldots, X_N) = \sum_{i=0}^{m} a'_i X^{m-i}$, les polynômes de degré p et q définissant $\mathscr{C}$ et $\mathscr{C}'$. Supposons que P et P' possèdent $mn+1$ racines communes $\left(x_0^{(0)}, \ldots, x_N^{(0)}\right), \ldots, \left(x_0^{(mn)}, \ldots, x_N^{(mn)}\right)$. Alors le polynôme PP', de degré mn, a $mn+1$ racines, donc P et P' ont un facteur commun non trivial.

Proposition 3. *Soient $\mathscr{D}$, $\mathscr{D}'$ deux cônes avec exactement quatre points distincts en commun, sur un corps infini k. Alors toute cônique $\mathscr{D}''$ passant par ces quatre points s'écrit $\mathscr{D}'' = a\mathscr{D} + a'\mathscr{D}'$.*

Preuve : Notons P_1, P_2, P_3, P_4 ces quatre points d'intersection. Remarquons d'abord que trois d'entre eux ne peuvent être sur une même droite, sans quoi cette droite, par la proposition précédente, serait commune aux deux cônes (on utilise donc ici l'hypothèse que k est infini). Soit P un point de $\mathscr{D}''$ distinct de P_1, P_2, P_3, P_4. Alors il existe $(a : a') \in \mathbb{P}^1(k)$ tel que $P \in (a\mathscr{D} + a'\mathscr{D}')$. Mais alors $\mathscr{D}''$ et $a\mathscr{D} + a'\mathscr{D}'$ ont cinq points en commun, donc une droite en commun. Chacune des deux cônes est donc composée de deux droites, mais les droites restantes de chaque cônique ayant deux points en commun, elles sont identiques : $\mathscr{D}'' = a\mathscr{D} + a'\mathscr{D}'$.

Proposition 4. *Soient $\mathscr{B}$ et $\mathscr{B}'$ deux cubiques (sur un corps infini k) ayant exactement neuf points d'intersection $P_1, \ldots, P_9$. Si une conique $\mathscr{B}''$ passe par huit de ces points, elle passe par le neuvième, et elle s'écrit $\mathscr{B}'' = a\mathscr{B} + a'\mathscr{B}'$.*

Preuve : La première assertion découlera de la seconde. Notons d'abord que, l'intersection entre $\mathscr{B}$ et $\mathscr{B}'$ étant finie, on sait que, parmi $P_1, \ldots, P_9$, il n'y a ni quatre points sur une même droite, ni sept points sur une même cônique.

Procédons par l'absurde, c'est-à-dire supposons que $\mathscr{B}''$ ne s'écrit pas de cette manière. La famille $a\mathscr{B} + a'\mathscr{B}' + a''\mathscr{B}''$, $(a : a' : a'') \in \mathbb{P}^2(k)$, est donc bidimensionnelle.

Ensuite, on ne peut y avoir trois P_i sur une même droite. En effet, si l'on avait P_1, P_2, P_3 sur une droite L, en prenant un autre point P' sur la droite mais par sur les cubiques, et un point P'' ni sur L ni sur l'unique cônique passant par $P_4, \ldots, P_8$, on pourrait trouver $(a : a' : a'') \in \mathbb{P}^2(k)$ tel que $P', P" \in (a\mathscr{B} + a'\mathscr{B}' + a''\mathscr{B}'')$. Cette cubique est constituée de la droite L (car a en commun avec elle les points P_1, P_2, P_3, P') et d'une cônique. Mais cette cônique ne peut être que la cônique engendrée par les points $P_4, \ldots, P_8$ (puisqu'elle a cinq points en commun avec elle), or ceci est une contradiction, à cause de P''.

En outre, il n'y a pas six points sur une même cônique. En effet, si l'on avait $P_1, \ldots, P_6$ sur une même cônique $\mathscr{C}$, on pourrait prendre $(a : a' : a'') \in \mathbb{P}^2(k)$ tel que la cubique $a\mathscr{B} + a'\mathscr{B}' + a''\mathscr{B}''$ contienne un point $P' \in \mathscr{C}$ (différent de $P_1, \ldots, P_6$) et un point P'' ni sur $\mathscr{C}$ ni sur la droite $\overline{P_7.P_8}$. Cette cubique contiendrait alors la cônique $\mathscr{C}$ toute entière (puisqu'il n'y pas trois points sur une même droite), la droite restante ne pouvant être que $\overline{P_7P_8}$, contradiction.

Prenons maintenant $(a : a' : a'') \in \mathbb{P}^2(k)$ tels que la cubique $a\mathscr{B} + a'\mathscr{B}' + a''\mathscr{B}''$ passe par deux points P' et P'' sur la droite $\overline{P_1.P_2}$ mais pas sur la cônique $\mathscr{D}$ engendrée par $P_3, \ldots, P_7$. Cette cubique a $\overline{P_1.P_2}$ et $\mathscr{D}$ comme composantes, ce qui est une contradiction puisqu'elle contient P_8, qui ne peut, à cause des affirmations prouvées ci-dessus, appartenir à $\overline{P_1.P_2}$ ni à $\mathscr{D}$.

Pour prouver l'associativité (voir figure à la page 159), on utilise la dernière proposition prouvée, avec $\mathscr{B} = \overline{P.(Q+R)} \bigsqcup \overline{Q.R} \bigsqcup \overline{PQ.P+Q}$ et $\mathscr{B}' = \overline{(P+Q).R} \bigsqcup \overline{QR.Q+R} \bigsqcup \overline{P.PQ}$. Les cubiques $\mathscr{B}$ et $\mathscr{C}$ (la cônique initiale) ont neuf points en commun. Comme $\mathscr{B}'$ comprend huit de ces points $(O, P, Q, R, PQ, P+Q, QR, Q+R)$, elle passe par le neuvième, qui est $P(Q+R)$. Comme $\mathscr{B}'$ a déjà neuf points en commun avec $\mathscr{C}$ et ne peut en avoir davantage, on en déduit que

$$(P+Q)R = P(Q+R),$$

d'où

$$(P+Q)+R = P+(Q+R).$$

2 Du réseau à la courbe algébrique : l'uniformisation

Nous allons considérer des fonctions périodiques [4] par rapport à notre réseau $\Lambda_\tau = \mathbb{Z} \bigoplus \tau\mathbb{Z}$ (on prouve facilement que tout sous-groupe discret de rang deux de $\mathbb{C}$ est de cette forme, à un changement d'échelle complexe près). Notons P le parallélogramme fondamental du réseau $P = \{t + s\tau | s, t \in]0; 1[\}$, et ∂P son bord.

Définition 2. *Une fonction elliptique est une fonction méromorphe $f : \mathbb{C} \to \mathbb{C}$ qui est Λ_τ-périodique.*

Une telle fonction f définit donc une fonction $\bar{f} : \mathbb{C}/\Lambda_\tau$. On vérifie que ces fonctions forment un corps, noté $\mathscr{M}(\Lambda_\tau)$. Il est indispensable de considérer des fonctions méromorphes car il est immédiat qu'une fonction elliptique holomorphe est constante (elle est d'image compacte, donc bornée...).

Lemme 1. *Soit f une fonction elliptique sans pôles ni zéros sur ∂P. Alors, si $\mathrm{ord}_a\, f$ désigne l'ordre du zéro ou du pôle a pour f, on a :*

$$\sum_{a\in P} \mathrm{ord}_a\, f = 0 \text{ et } \sum_{a\in P} a.\,\mathrm{ord}_a\, f \in \Lambda$$

Démonstration. Pour la première assertion, il suffit d'utiliser le théroème des résidus : on a, puisque $\frac{f}{f'}$ n'a pas de pôles sur ∂P,

$$\sum_{a\in P} \mathrm{ord}_a\, f = \sum_{a\in P} \mathrm{Res}\left(\frac{f'}{f}, a\right) = \oint_{\partial P} \frac{\mathrm{d}z}{2\pi i}\frac{f'(z)}{f(z)} = 0.$$

Pour la seconde, le théorème des résidus donne

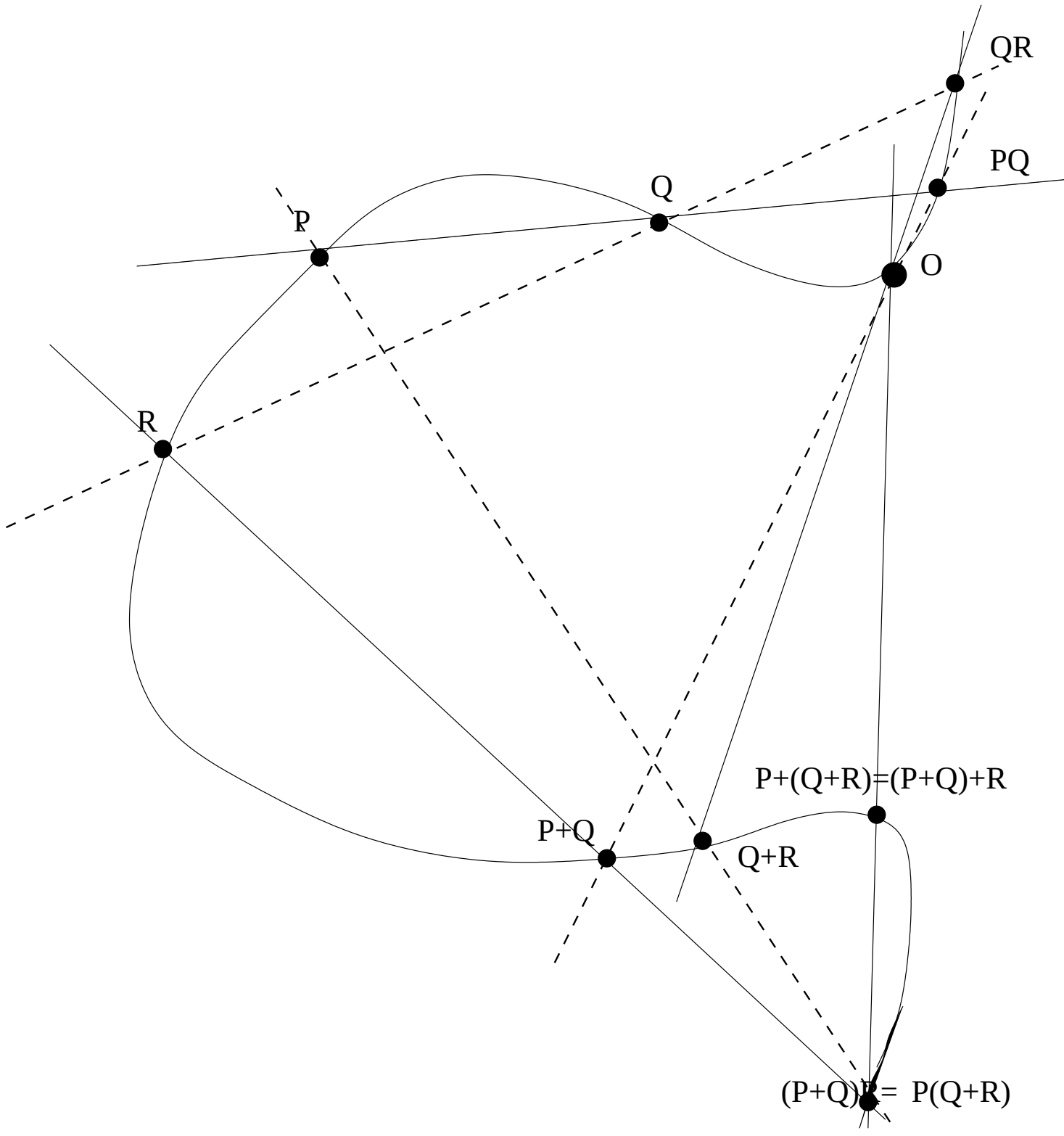
$$\sum_{a\in P} a.\,\mathrm{ord}_a\, f = \oint_{\partial P} \frac{\mathrm{d}z}{2\pi i}\frac{zf'(z)}{f(z)}.$$

En outre,

$$\begin{aligned} \oint_{\partial P} \tfrac{\mathrm{d}z}{2\pi i}\tfrac{zf'(z)}{f(z)} &= \left(\int_0^\tau + \int_\tau^{\tau+1} + \int_{\tau+1}^1 + \int_1^0\right)\tfrac{zf'(z)}{f(z)}\mathrm{d}z \\ &= \left(\left(\int_0^\tau - \int_1^{1+\tau}\right) + \left(\int_\tau^{\tau+1} - \int_0^1\right)\right)\tfrac{zf'(z)}{f(z)}\mathrm{d}z \end{aligned}$$

Le deuxième terme vaut $\tau \int_0^1 \frac{f'(z)}{f(z)}\mathrm{d}z$ et est donc dans $\mathbb{Z}\tau$. On conclut de même que le premier terme est dans $\mathbb{Z}$.

□



Le lemme suivant est très facile et sera constamment utilisé dans la suite.

Lemme 2. *Notons $\widetilde{\Lambda_\tau}$ le réseau Λ_τ privé de 0. Alors $\sum_{\omega\in\widetilde{\Lambda_\tau}} \omega^{-s} = 0$.*

Le lemme précédent montre notamment qu'il est impossible qu'une fonction elliptique possède un et un seul pôle simple. La fonction $\mathscr{P}$ de Weierstrass est une des fonctions elliptiques non constantes les plus simples, puisqu'elle a un unique pôle double, en 0.

Définition 3. *Les fonctions «de Weierstrass» sont définies comme suit*

$$\mathscr{P}(z;\tau) = z^{-2} + \sum_{\omega\in\widetilde{\Lambda_\tau}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right);$$

$$\zeta(z;\tau) = z^{-1} + \sum_{\omega\in\widetilde{\Lambda_\tau}} \left(\frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2} \right);$$

$$G_{2k}(\tau) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} (m\tau+n)^{-2k};$$

$$g_2(\tau) = 60G_2(\tau)\,,\; g_3(\tau) = 140G_3(\tau).$$

Il suit de cette définition que $\mathscr{P}'(z) = -2\sum_{\omega\in\widetilde{\Lambda_\tau}} \frac{1}{(z-w)^3}$ et que $\zeta' = -\mathscr{P}$. Le lemme suivant s'obtient par simple manipulation.

Lemme 3.

$$\zeta(z) = \frac{1}{z} - \sum_{k\geq 2} G_{2k} z^{2k-1},$$

$$\mathscr{P}(z) = \frac{1}{z^2} + \sum_{k\geq 2} G_{2k}(2k-1) z^{2k-2}$$

Remarquons que, si deux réseaux $\mathbb{C}/\Lambda$ et $\mathbb{C}/\Lambda'$ sont isomorphes, il existe $\lambda \in \mathbb{C}$ tel que $\lambda\Lambda = \Lambda'$. Si $\Lambda = \Lambda_\tau$ et $\Lambda' = \Lambda_{\tau'}$, cela revient à l'existence de $g_\lambda \in SL_2(\mathbb{Z})$ tel que $g_\lambda\tau = \tau'$. Le théorème d'uniformisation [2, 3], dont nous donnerons la preuve de façon incomplète, s'énonce alors ainsi :

Théorème 2. *La fonction $\mathscr{P}$ vérifie l'équation différentielle suivante, pour $z \in \mathbb{C}$,*

$$(\mathscr{P}'(z;\tau))^2 = 4(\mathscr{P}(z;\tau))^3 - g_2(\tau)\mathscr{P}(z;\tau) - g_3(\tau).$$

Si on note $\mathscr{C}_\tau$ la courbe d'équation $wy^2 = 4x^3 - g_2(\tau)w^2x - g^3(\tau)w^3$, on a un isomorphisme biholomorphe de groupes

$$h_\tau : \mathbb{C}/\Lambda_\tau \to \mathscr{C}_\tau : z \mapsto \begin{cases} (1 : \mathscr{P}(z) : \mathscr{P}'(z)) & si\ z = 0 \\ (0:0:1) & sinon \end{cases}.$$

En outre, toute cubique non singulière est atteinte, et les isomorphismes sont les mêmes des deux points de vue. Plus précisément, si $\lambda \in \mathbb{C}$, et si on définit $\phi_\lambda : \begin{cases} x \mapsto \lambda^2 x \\ y \mapsto \lambda^3 y \end{cases}$, on a le diagramme commutatif suivant.

$$\begin{array}{ccc} \mathbb{C}/(\lambda\Lambda_\tau) & \xrightarrow{\lambda^{-1}} & \mathbb{C}/\Lambda_\tau \\ \downarrow{\scriptstyle h_\tau} & & \downarrow{\scriptstyle h_\tau} \\ \mathscr{C}_\tau & \xrightarrow{\phi_\lambda} & \mathscr{C}_\tau \end{array}$$

Enfin, toute bijection algébrique entre deux cubiques non singulières $\mathscr{C}_{g_\lambda\tau}$ et $\mathscr{C}_\tau$ qui respecte la loi de groupe provient d'un isomorphisme

$$\mathbb{C}/(\lambda\Lambda_\tau) \cong \mathbb{C}/\Lambda_\tau.$$

Démonstration. Pour montrer la première assertion, on utilise le développement en série entière de $\mathscr{P}$. Une comparaison des premiers termes des deux séries entières montre que le quotient des deux membres est holomorphe. Or une fonction elliptique holomorphe est constante.

L'analycité de h_τ est évidente, sauf en 0, où il faut réécrire $h_\tau(z) = (z^3, \mathscr{P}(z), \mathscr{P}'(z))$ pour le voir, $\mathscr{P}$ et $\mathscr{P}'$ ayant des pôles respectivement d'ordre 2 et 3 en 0. Soit $(x, y) \in \mathscr{C}_\tau$; la fonction $\mathscr{P}(z) - x$ a deux zéros $z_1, z_2 \in \mathbb{C}$, qui vérifient $z_1 + z_2 \in \Lambda$ et $\mathscr{P}'(z_i) = \pm y$. D'où l'injectivité et la surjectivité. Pour montrer que h_τ est bien un morphisme de groupes, comme il envoie bien le neutre 0 sur le neutre $(0 : 0 : 1)$, il suffit de vérifier que, si trois points sont de somme nulle dans $\mathscr{C}_\tau$, ils sont de somme nulle dans $\mathbb{C}/\Lambda_\tau$. Or trois points sont de somme nulle dans $\mathscr{C}_\tau$ si et seulement si ils sont sur une même droite. Si cette droite a une équation $y = \mu x + c$, la fonction $\mathscr{P}'(z) - (\mu\mathscr{P}(z) - c)$ a trois zéros z_1, z_2, z_3, qui vérifient $z_1 + z_2 + z_3 \in \Lambda_\tau$ par un lemme précédent, ce qui revient à dire que leur somme est nulle dans $\mathbb{C}/\Lambda_\tau$.

La commutation du diagramme résulte essentiellement des formules d'homogénéité

$$\left\{\begin{array}{rcl} \mathscr{P}(z;\tau) & = & \lambda^2\mathscr{P}(\lambda z; g_\lambda\tau) \\ \mathscr{P}'(z;\tau) & = & \lambda^3\mathscr{P}'(\lambda z; g_\lambda\tau) \\ G_{2k}(\tau) & = & \lambda^{2k}G_{2k}(g_\lambda\tau) \end{array}\right.$$

□

Définition 4. *Un diviseur* $\Delta \in \mathrm{Div}(\mathbb{C}/\Lambda)$ *d'un tore* $\mathbb{C}/\Lambda$ *est une combinaison linéaire finie* $\Delta = \sum_{u\in\mathbb{C}/\Lambda} m_u (u)$ *. Son degré est alors* $\deg(\Delta) = \sum_{u\in\mathbb{C}/\Lambda} m_u$. *Un diviseur principal est un diviseur qui s'écrit* $(f) = \sum_{u\in\mathbb{C}/\Lambda} \mathrm{ord}_u(f)(u)$ *avec* $f \in \mathscr{M}(\Lambda_\tau)$.

Le théorème d'Abel-Jacobi permet une autre vision de la courbe elliptique $\mathbb{C}/\Lambda$.

Théorème 3. *Si on note* Div_0 *les diviseurs d'ordre* 0 *et* Div_p *les diviseurs principaux, le morphisme de* $\mathrm{Div}(\mathbb{C}/\Lambda)$ *vers* $\mathbb{C}/\Lambda$ $\xi\left(\sum_{u\in\mathbb{C}/\Lambda} m_u(u)\right) = \sum_{u\in\mathbb{C}/\Lambda} m_u.u$ *induit*

$$\xi \ : \ \frac{\mathrm{Div}_0(\mathbb{C}/\Lambda)}{\mathrm{Div}_p(\mathbb{C}/\Lambda)} \xrightarrow{\sim} \mathbb{C}/\Lambda.$$

3 De la courbe au réseau

Nous utiliserons également les fonctions $\mathscr{P}$. Soit $\mathscr{C}$ une courbe elliptique, vue comme courbe algébrique non singulière de degré 3. On cherche un réseau [2] $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ tel que $(\mathscr{P}, \mathscr{P}')$ soit un isomorphisme.

On sait que l'équation de $\mathscr{C}$ peut s'écrire

$$\mathscr{C} \equiv y^2 = P(x),$$

avec P un polynôme de degré 3 à racines simples. Ses racines e_1, e_2, e_3, «points de 2-division» de la courbe, seront telles que[1]

[1]Car $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$, $\frac{\omega_1+\omega_2}{2}$ sont exactement les points du réseau $\mathbb{C}/!\Lambda$ qui, multipliés par 2, donnent 0.

$$\begin{aligned}\mathscr{P}\left(\tfrac{\omega_1}{2}\right) &= e_1\\ \mathscr{P}\left(\tfrac{\omega_2}{2}\right) &= e_2\\ \mathscr{P}\left(\tfrac{\omega_1+\omega_2}{2}\right) &= e_3.\end{aligned}$$

Par une transformation conforme, laissant tel quel l'invariant différentiel $\frac{\mathrm{d}x}{P'(x)}$, ses racines peuvent être envoyées sur $(0,1,\lambda)$, auquel cas l'équation de la courbe s'écrit

$$y^2 = x\,(x-1)\,x-\lambda.$$

Les deux générateurs ω_1 et ω_2 du réseau qui va correspondre à la courbe sont maintenant définis comme suit

$$\omega_1(\lambda) = \int_{-\infty}^{0} \frac{\mathrm{d}x}{\sqrt{x\,(x-1)\,(x-\lambda)}},$$
$$\omega_2(\lambda) = \int_{1}^{\infty} \frac{\mathrm{d}x}{\sqrt{x\,(x-1)\,(x-\lambda)}}.$$

Ce qui donne, pour ω_2,

$$\begin{aligned}\omega_2(\lambda) &= \textstyle\int_{-\infty}^{0} \frac{\mathrm{d}x}{\sqrt{x(x-1)(x-\lambda)}}\\ &= \textstyle\int_{1}^{0} \frac{-\mathrm{d}t/t^2}{\sqrt{\left(\frac{1}{t}\right)\left(\frac{1}{t}-1\right)\left(\frac{1}{t}-\lambda\right)}}\\ &= \textstyle 2\int_{0}^{1} \frac{\mathrm{d}s}{\sqrt{(1-s^2)(1-\lambda s^2)}}\\ &= \textstyle\int_{0}^{\frac{\pi}{2}} \frac{\mathrm{d}\theta}{\sqrt{1-\lambda\sin^2\theta}}\\ &= \pi\,{}_2F_1\left(\tfrac{1}{2}\ \tfrac{1}{2}\ 1\,\middle|\,\lambda\right).\end{aligned}$$

Seule la dernière égalité[2] ne résulte pas d'un simple changement de variables : elle s'obtient en développant en série entière la racine, puis le sinus. De même on trouve

$$\omega_2(\lambda) = i\pi\,{}_2F_1\left(\frac{1}{2}\ \frac{1}{2}\ 1\,\middle|\,1-\lambda\right).$$

Il est ensuite très simple de vérifier le théorème de la section précédente à partir de ce réseau Λ.

4 L'espace des modules des courbes elliptiques

L'invariant j permet de classifier les courbes elliptiques sur $\mathbb{C}$[3] : pour $j \neq 0, 1728$, on peut écrire une courbe elliptique d'invariant j

$$\mathscr{C} \equiv y^2 = 4x^3 - 27\frac{j}{j-1728} - 27\frac{j}{j-1728}.$$

[2] Où ${}_pF_q\left(\begin{array}{ccc} a_1 & \dots & a_p \\ b_1 & \dots & b_q \end{array}\,\middle|\, z\right) = \sum_k \frac{(a_1)_k\dots(a_p)_k}{(b_1)_k\dots(b_q)_k}\frac{z^k}{k!}$ est la fonction hypergéométrique classique [5], et où $(a)_k = a(a+1)\dots(a+k-1)$ est le symbole de Pochammer.

[3] La classification est semblable pour tout corps de caractéristique différente de 2 et 3, à ceci près qu'il peut y avoir plusieurs courbes elliptiques non isomorphes de même invariant [1].

En outre, la courbe $\mathscr{C} \equiv y^2 = x^3 - 1$ est telle que $j = 0$ et la courbe $\mathscr{C} \equiv y^2 = x^3 - x$ telle que $j = 12^3$. Cependant, l'application qui associe à une courbe elliptique son invariant est ramifiée. Une discussion détaillée nous entraînerait trop loin.

On a vu que des réseaux images l'un de l'autre par un élément de $\mathcal{SL}_2(\mathbb{Z})$ étaient les mêmes. Il faut également tenir compte du changement d'échelle complexe. L'espace des classes d'isomorphisme de courbes elliptiques est donc isomorphe au demi-plan de Poincaré quotienté par le groupe modulaire projectif.

Références

[1] Centro Internazionale Matematico Estivo Cetraro 1997. *Arithmetic Theory of Elliptic Curves*. Number 1716 in Lecture Notes in mathematics. Springer, 1999.

[2] D. Husemoller. *Elliptic Curves*. Number 111 in Graduate texts in mathematics. Springer, 1987.

[3] D. Mumford. *Tata lectures on theta I*. Number 28 in Progress in Mathematics. Birkhäuser, 1983.

[4] H. McKean, V. Moll. *Elliptic Curves — Function theory, Geometry, arithmetic*. Cambridge University Press, 1997.

[5] J. Levie, G. Lafon. Quelques preuves de l'irrationalité de $\zeta(3)$. *Exposé de maîtrise sous la direction de Stéphane Fischler*, 2001.

[6] Silverman, Tate. *Rational Points on Elliptic Curves*. Springer-Verlag, 1992.