

# Courbe de Tate et uniformisation des courbes elliptiques $p$ -adiques

Olivier Wittenberg

5 novembre 2001

## Résumé

On expose ici la théorie, due à Tate, de l'uniformisation des courbes elliptiques  $p$ -adiques.

Soit  $K$  un corps  $p$ -adique. Pour  $q \in K^*$  avec  $|q| < 1$ , on construit une courbe elliptique  $E_q$  sur  $K$  telle que  $E_q(L)$  soit isomorphe à  $L^*/q^{\mathbb{Z}}$  pour toute extension algébrique  $L/K$ . On montre ensuite que toute courbe elliptique sur  $K$  d'invariant  $j$  non entier est  $\bar{K}$ -isomorphe à  $E_q$  pour un certain  $q$ , et qu'elle lui est  $K$ -isomorphe si et seulement si elle a réduction multiplicative déployée.

## 1 Rappels sur l'uniformisation complexe

Notons  $\mathfrak{H}$  le demi-plan de Poincaré. Soit  $\tau \in \mathfrak{H}$ . On note  $\Lambda_\tau$  le réseau  $\mathbb{Z} + \tau\mathbb{Z}$  et  $\wp$  la fonction de Weierstrass associée; c'est une fonction méromorphe sur  $\mathbb{C}$ , holomorphe sur  $\mathbb{C} \setminus \Lambda_\tau$ . Soit  $E_\tau$  la courbe elliptique sur  $\mathbb{C}$  définie par l'équation

$$y^2 = 4x^3 - 60G_4(\tau)x - 140G_6(\tau),$$

où  $G_k$  est la série d'Eisenstein de poids  $k$ .

**Théorème 1.0.1 (uniformisation des courbes elliptiques complexes)** — Soit  $\tau \in \mathfrak{H}$ . L'application

$$\begin{array}{ccc} \mathbb{C}/\Lambda_\tau & \longrightarrow & E_\tau(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}) \quad \text{où le plongement est donné par } (x, y) \\ z & \longmapsto & [\wp(z) : \wp'(z) : 1] \quad \text{si } z \neq 0 \\ 0 & \longmapsto & [0 : 1 : 0] \end{array}$$

est un isomorphisme de groupes de Lie complexes. De plus, toute courbe elliptique sur  $\mathbb{C}$  est isomorphe à  $E_\tau$  pour un certain  $\tau \in \mathfrak{H}$ .

On aimerait prouver un résultat similaire pour les courbes elliptiques sur  $\mathbb{Q}_p$ , ou plus généralement sur un corps  $p$ -adique (i.e. une extension finie de  $\mathbb{Q}_p$ ). Cependant, si  $E$  est une courbe elliptique sur  $\mathbb{Q}_p$ , on ne pourra certainement pas exprimer  $E(\mathbb{Q}_p)$  comme le quotient de  $\mathbb{Q}_p$  par un sous-groupe discret car  $\mathbb{Q}_p$  ne possède pas de sous-groupe discret non trivial. L'astuce est la suivante : on remarque que l'application

$$\mathbb{C}/\Lambda_\tau \longrightarrow \mathbb{C}^*/q^{\mathbb{Z}}, \quad z \longmapsto e^{2i\pi z}$$

est un isomorphisme (avec  $q = e^{2i\pi\tau}$ ). Il se trouve que ce point de vue se transpose bien aux courbes elliptiques  $p$ -adiques;  $\mathbb{Q}_p^*$  a de nombreux sous-groupes discrets, par exemple  $q^{\mathbb{Z}}$  pour  $q \in \mathbb{Z}_p^*$ .

Explicitons l'isomorphisme  $\mathbb{C}^*/q^{\mathbb{Z}} \rightarrow E_\tau(\mathbb{C})$  et réécrivons l'équation de Weierstrass de  $E_\tau$  en fonction de  $u = e^{2i\pi z}$  et de  $q = e^{2i\pi\tau}$  au lieu de  $z$  et  $\tau$ . Il s'agit d'exprimer  $\wp(z)$ ,  $\wp'(z)$ ,  $G_4(\tau)$  et  $G_6(\tau)$  en fonction de  $u$  et  $q$ . Voici ce que l'on trouve, après quelques calculs classiques d'analyse complexe (voir [2], I.6.2 et I.7.3.2) :

$$\begin{aligned} \wp(z) &= (2i\pi)^2 \left( \sum_{n \in \mathbb{Z}} \frac{q^n u}{(1 - q^n u)^2} + \frac{1}{12} - 2s_1(q) \right) \quad ; \quad \wp'(z) = (2i\pi)^3 \sum_{n \in \mathbb{Z}} \frac{q^n u(1 + q^n u)}{(1 - q^n u)^3} \\ G_4(\tau) &= \frac{(2i\pi)^4}{720} (1 + 240s_3(q)) \quad ; \quad G_6(\tau) = \frac{(2i\pi)^6}{30240} (-1 + 504s_5(q)) \end{aligned}$$

où  $s_k$  est la série formelle à coefficients entiers suivante, qui a bien un sens car la série converge pour la topologie  $Q$ -adique sur  $\mathbb{Z}[[Q]]$  :

$$s_k = \sum_{n \geq 1} \frac{n^k Q^n}{1 - Q^n}$$

Pour définir une flèche  $\mathbb{Q}_p^*/q^{\mathbb{Z}} \rightarrow E(\mathbb{Q}_p)$  lorsque  $E$  est une courbe elliptique sur  $\mathbb{Q}_p$  et  $q \in \mathbb{Z}_p^*$ , on aimerait utiliser la même formule que sur  $\mathbb{C}$ , en considérant  $\wp(z)$  et  $\wp'(z)$  comme des séries formelles en  $U$  et  $Q$ . On a alors affaire à un nouveau problème :  $\pi$  et  $i$  apparaissent dans les coefficients de ces séries. Pour les éliminer, effectuons le changement de variables suivant :

$$\begin{aligned} x &= (2i\pi)^2 \left( x' + \frac{1}{12} \right) \\ y &= (2i\pi)^3 (2y' + x') \end{aligned}$$

L'équation de Weierstrass en  $x'$  et  $y'$  s'écrit alors

$$y'^2 + x'y' = x'^3 + a_4(q)x' + a_6(q),$$

où l'on a posé :

$$a_4 = -5s_3 \quad ; \quad a_6 = -\frac{1}{12}(5s_3 + 7s_5)$$

Les séries formelles  $a_4$  et  $a_6$  sont à coefficients rationnels, et même entiers (exercice facile). Le discriminant  $\Delta_{\mathbb{C}}(q)$  de cette équation de Weierstrass se déduit facilement de celui de l'équation de Weierstrass en  $x$  et  $y$ , lui-même donné en fonction de  $q$  par la formule de Jacobi (voir [2], I.8). On obtient :

$$\Delta_{\mathbb{C}}(q) = q \prod_{n \geq 1} (1 - q^n)^{24}$$

Si  $F$  est un corps muni d'une valeur absolue pour laquelle il est complet (par exemple  $F = \mathbb{C}$  ou  $F = \mathbb{Q}_p$ ), posons, pour  $q \in F^*$  tel que  $|q| < 1$  et  $u \in L^* \setminus q^{\mathbb{Z}}$ , où  $L$  est une extension algébrique de  $F$  munie de l'unique valeur absolue prolongeant celle de  $F$  :

$$\begin{aligned} X_F(u, q) &= \sum_{n \in \mathbb{Z}} \frac{q^n u}{(1 - q^n u)^2} - 2s_1(q) \\ Y_F(u, q) &= \sum_{n \in \mathbb{Z}} \frac{(q^n u)^2}{(1 - q^n u)^3} + s_1(q) \end{aligned}$$

On vérifie tout de suite que les séries ci-dessus convergent dans  $F(u)$ , d'après les hypothèses sur  $q$  et  $u$ . D'après ce qui précède, en reprenant  $\tau \in \mathfrak{H}$  et  $q = e^{2i\pi\tau}$ , l'isomorphisme entre  $E_{\tau}(\mathbb{C})$  et  $\mathbb{C}^*/q^{\mathbb{Z}}$  s'écrit donc :

$$\begin{array}{lll} \mathbb{C}^*/q^{\mathbb{Z}} & \longrightarrow & E_{\tau}(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}) \quad \text{où le plongement est donné par } (x', y') \\ u & \longmapsto & [X_{\mathbb{C}}(u, q) : Y_{\mathbb{C}}(u, q) : 1] \quad \text{si } u \neq 1 \\ 1 & \longmapsto & [0 : 1 : 0] \end{array}$$

## 2 La courbe de Tate

### 2.1 Définitions et énoncé du théorème

Soit  $K$  un corps complet pour une valeur absolue non-archimédienne discrète. Soit  $\overline{K}$  une clôture algébrique de  $K$ , que l'on munit de l'unique valeur absolue prolongeant celle de  $K$ . Soit enfin  $q \in K^*$  tel que  $|q| < 1$ . Les séries  $a_4(q)$  et  $a_6(q)$  convergent dans  $K$  puisqu'elles sont à coefficients entiers. Soit  $E_q$  la courbe (projective) sur  $K$  définie par :

$$y^2 + xy = x^3 + a_4(q)x + a_6(q) \tag{1}$$

Soit  $\Delta$  la série formelle suivante (on vérifie tout de suite que ceci converge pour la topologie  $Q$ -adique) :

$$\Delta = Q \prod_{n \geq 1} (1 - Q^n)^{24} \in \mathbb{Z}[[Q]]$$

**Proposition 2.1.1** — *Le discriminant de l'équation de Weierstrass (1) est  $\Delta(q)$ .*

Attention à la signification de  $\Delta(q)$  : ici  $\Delta$  est un élément de  $K[[Q]]$ , et  $\Delta(q)$  désigne donc la limite de la somme des termes de degré inférieur à  $n$  lorsque  $n$  tend vers l'infini. On n'a pas *a priori*

$$\Delta(q) = q \prod_{n \geq 1} (1 - q^n)^{24}.$$

Il se trouve que cette égalité est quand même vérifiée pour  $|q| < 1$  si la valeur absolue est non-archimédienne (cela sous-entend que le produit converge, ce qui n'est pas complètement évident a priori non plus, même s'il est facile de le démontrer directement), du fait que les coefficients des produits partiels du terme de droite sont entiers (et donc bornés). En effet, si l'on note  $\Delta_N$  la série tronquée au degré  $N$ , on a, pour  $M$  assez grand (dépendant de  $N$ ),

$$\Delta_N(Q) - Q \prod_{n=1}^M (1 - Q^n)^{24} \in Q^N \mathbb{Z}[[Q]],$$

et donc

$$\left| \Delta_N(q) - q \prod_{n=1}^M (1 - q^n)^{24} \right| \leq |q|^N,$$

ce qui donne le résultat voulu lorsqu'on fait tendre  $N$  vers l'infini.

Démonstration de la proposition — Le discriminant de (1) s'exprime comme un polynôme de  $a_4(q)$  et  $a_6(q)$ , que l'on n'explicitera pas ; notons-le  $P(a_4(q), a_6(q))$ . Soit  $D = P(a_4(Q), a_6(Q)) \in \mathbb{Z}[[Q]]$ . Il reste à montrer que  $D(q) = \Delta(q)$  pour  $q \in K^*$ ,  $|q| < 1$ . Pour cela, il suffit de voir que  $D = \Delta$ . On sait, d'après la section précédente, que pour  $q \in \mathbb{C}^*$  tel que  $|q| < 1$ ,  $D(q) = q \prod_{n \geq 1} (1 - q^n)^{24}$ . La proposition sera donc prouvée si l'on établit que

$$\Delta(q) = q \prod_{n \geq 1} (1 - q^n)^{24} \quad \text{pour } q \in \mathbb{C}^*, |q| < 1.$$

Le membre de droite est une fonction holomorphe de  $q$  et il s'agit de vérifier que son développement en série entière est la série formelle  $\Delta$ , ce que l'on obtient facilement par des arguments standard d'analyse complexe.  $\square$

Comme  $\Delta \in Q + Q^2 \mathbb{Z}[[Q]]$ , la proposition implique que  $\Delta(q) \neq 0$  pour  $q \in K^*$  tel que  $|q| < 1$ . Ainsi,  $E_q$  est une courbe elliptique sur  $K$ . On l'appelle la *courbe de Tate*. Nous pouvons maintenant énoncer le théorème principal de cette section.

**Théorème 2.1.2** — Soient  $K$  un corps de caractéristique 0, complet pour une valuation discrète (par exemple un corps  $p$ -adique ou le complété de l'extension maximale non ramifiée de  $\mathbb{Q}_p$ ),  $\bar{K}$  une clôture algébrique de  $K$ ,  $\mathcal{G}_K = \text{Gal}(\bar{K}/K)$  et  $q \in K^*$  tel que  $|q| < 1$ . Alors l'application

$$\begin{aligned} \Phi: \quad \bar{K}^*/q^{\mathbb{Z}} &\longrightarrow E_q(\bar{K}) \subset \mathbb{P}^2(\bar{K}) && \text{où le plongement est donné par } (x, y) \\ u &\longmapsto [X_K(u, q) : Y_K(u, q) : 1] && \text{si } u \neq 1 \\ 1 &\longmapsto [0 : 1 : 0] \end{aligned}$$

est un isomorphisme de  $\mathcal{G}_K$ -modules.

**Corollaire 2.1.3** — Si  $L/K$  est une extension algébrique,  $\Phi$  induit un isomorphisme  $L^*/q^{\mathbb{Z}} \rightarrow E_q(L)$ .

Démonstration — La seule chose à vérifier est la surjectivité de cette application. On la prouvera directement par la suite, mais notons qu'on peut la déduire du théorème. En effet,  $H^1(\mathcal{G}_K, q^{\mathbb{Z}})$  est nul car  $\mathcal{G}_K$  agit trivialement sur  $q^{\mathbb{Z}}$  et il n'y a pas de morphisme continu non nul de  $\mathcal{G}_K$  dans  $q^{\mathbb{Z}}$ , ce dernier groupe étant discret.  $\square$

Nous allons prouver le théorème en deux étapes ; le plus difficile est la surjectivité de  $\Phi$ .

## 2.2 Preuve de « $\Phi$ morphisme de $\mathcal{G}_K$ -modules »

Un résultat préliminaire nous sera utile. Posons

$$X(U, Q) = \sum_{n \in \mathbb{Z}} \frac{Q^n U}{(1 - Q^n U)^2} - 2s_1(Q) \in \mathbb{Z}[U][[Q]]$$

$$Y(U, Q) = \sum_{n \in \mathbb{Z}} \frac{(Q^n U)^2}{(1 - Q^n U)^3} + s_1(Q) \in \mathbb{Z}[U][[Q]]$$

et notons que  $X(U, Q)$  et  $Y(U, Q)$  sont bien des éléments de  $\mathbb{Z}[U][[Q]]$ , car les séries qui les définissent convergent pour la topologie  $Q$ -adique sur  $\mathbb{Z}[U][[Q]]$ . En effet, il suffit de voir que le terme général tend vers 0, et l'on a, pour  $n \in \mathbb{Z}$ , en notant  $v_Q$  la valuation  $Q$ -adique :

$$v_Q \left( \frac{Q^n U}{(1 - Q^n U)^2} \right) = |n| \quad ; \quad v_Q \left( \frac{(Q^n U)^2}{(1 - Q^n U)^3} \right) = \frac{1}{2} (n + 3|n|)$$

**Lemme 2.2.1** — *Soit  $F$  un corps muni d'une valeur absolue pour laquelle il est complet. Pour  $q \in F^*$  tel que  $|q| < 1$  et  $u \in F^*$  tel que  $|q| < |u| < |q|^{-1}$  et  $u \neq 1$ , les séries  $X(u, q)$  et  $Y(u, q)$  (vues comme éléments de  $F[[Q]]$  que l'on applique à  $q$ ) convergent, et  $X(u, q) = X_F(u, q)$ ,  $Y(u, q) = Y_F(u, q)$ .*

Démonstration — Montrons-le pour  $X$  ; la preuve pour  $Y$  est parfaitement similaire. Tout d'abord, on a

$$X_F(u, q) = \frac{u}{(1-u)^2} + \sum_{n \geq 1} \left( \frac{q^n u}{(1-q^n u)^2} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} - \frac{2q^n}{(1-q^n)^2} \right).$$

Utilisons ensuite le fait que

$$\sum_{n \geq 1} \frac{q^n v}{(1-q^n v)^2} = \sum_{d \geq 1} \left( \sum_{m|d, m \geq 1} m v^m \right) q^d$$

si  $|q^n v| < 1$  pour  $n \geq 1$  (exercice facile). On obtient, en prenant  $v \in \{u, 1, u^{-1}\}$ , que

$$X_F(u, q) = \frac{u}{(1-u)^2} + \sum_{d \geq 1} \left( \sum_{m|d, m \geq 1} m(u^m + u^{-m} - 2) \right) q^d.$$

On a ainsi exprimé  $X_F(u, q)$  sous forme de la valeur d'une série formelle en  $q$ . Cette série formelle est précisément  $X(u, Q)$ , car on n'a fait que des manipulations formelles. D'où le résultat.  $\square$

**Lemme 2.2.2** — *Soit  $F$  un corps muni d'une valeur absolue pour laquelle il est complet. Pour  $q \in F^*$  tel que  $|q| < 1$  et  $u \in F^* \setminus q^{\mathbb{Z}}$ , on a  $X_F(u, q) = X_F(qu, q) = X_F(u^{-1}, q)$  et  $Y_F(u, q) = Y_F(qu, q) = -X_F(u, q) - Y_F(u^{-1}, q)$ .*

Démonstration — Tout est évident, excepté la dernière égalité, qui est très facile à vérifier.  $\square$

Revenons à la preuve du théorème. La première chose à faire est de montrer que  $\Phi$  est bien définie, i.e. que son image dans  $\mathbb{P}^2(\overline{K})$  est contenue dans  $E_q(\overline{K})$ . Notons  $P(X, Y, A_4, A_6) = Y^2 + XY - X^3 - A_4 X - A_6$ . Il s'agit de voir que pour  $u \in \overline{K}^* \setminus q^{\mathbb{Z}}$ , on a  $P(X_K(u, q), Y_K(u, q), a_4(q), a_6(q)) = 0$ . D'après le lemme 2.2.2, on peut supposer  $|q| < |u| \leq 1$ , ce qui permet d'appliquer le lemme 2.2.1. Ainsi, il suffit de prouver que la série formelle  $P(X(U, Q), Y(U, Q), a_4(Q), a_6(Q))$  est nulle ; notons-la  $S$ . En utilisant à nouveau le lemme 2.2.1 et d'après ce qu'on a vu dans la première section,  $S(u, q) = 0$  pour  $(u, q) \in \mathbb{C}^2$  vérifiant  $|q| < |u| < |q|^{-1}$ ,  $0 < |q| < 1$  et  $u \neq 1$ . Ceci implique que  $S = 0$ .

Montrons maintenant que  $\Phi$  est un morphisme de groupes (il sera alors évident que c'est un homomorphisme de  $\mathcal{G}_K$ -modules, par continuité de l'action de  $\mathcal{G}_K$  sur  $\overline{K}$ ). Soit  $(u_1, u_2) \in (\overline{K}^*)^2$  et posons  $u_3 = u_1 u_2$ ,  $x_i = X_K(u_i, q)$  et  $y_i = Y_K(u_i, q)$ . Les cas où l'un des  $u_i$  vaut 1 découlent du lemme 2.2.2 ; supposons donc  $u_i \notin q^{\mathbb{Z}}$ . Commençons par le cas où  $x_1 \neq x_2$ . On dispose d'une formule générale pour calculer la somme de deux points d'une courbe elliptique lorsqu'elle est donnée sous la forme d'une équation de Weierstrass et que ces deux points ne sont ni nuls ni opposés ; en la regardant, on voit que l'abscisse du point  $\Phi(u_1) + \Phi(u_2)$  est une fraction rationnelle  $F$  de  $x_1, x_2, y_1, y_2, a_4(q), a_6(q)$ , à coefficients entiers, et dont le dénominateur est une puissance de  $x_1 - x_2$  ; de même pour son ordonnée

(notons  $G$  la fraction rationnelle correspondante). Ainsi, vérifier que  $\Phi(u_1) + \Phi(u_2) = [F(x_1, x_2, y_1, y_2, a_4(q), a_6(q)) : G(x_1, x_2, y_1, y_2, a_4(q), a_6(q)) : 1]$  revient à vérifier qu'un certain système de deux polynômes en toutes ces variables et à coefficients entiers s'annule. D'après le lemme 2.2.2, on peut supposer qu'on est dans le domaine d'application du lemme 2.2.1. Il suffit donc de montrer les égalités de séries formelles suivantes :

$$X(U_1 U_2, Q) - F(X(U_1, Q), X(U_2, Q), Y(U_1, Q), Y(U_2, Q), a_4(Q), a_6(Q)) = 0$$

$$Y(U_1 U_2, Q) - G(X(U_1, Q), X(U_2, Q), Y(U_1, Q), Y(U_2, Q), a_4(Q), a_6(Q)) = 0$$

D'après le lemme 2.2.1 et les résultats de la première section, ces deux séries formelles prennent des valeurs nulles sur un ouvert non vide de  $\mathbb{C}^3$ . Elles sont donc bien nulles. En ce qui concerne le cas où  $x_1 = x_2$ , on peut refaire le même raisonnement en utilisant la formule de duplication, qui elle aussi est une fraction rationnelle à coefficients entiers en les  $x_i$ , les  $y_i$ ,  $a_4(q)$  et  $a_6(q)$ .

**Remarque** — *On peut se passer du recours aux formules explicites d'addition et de duplication. En effet,  $E_q$  étant définie sur le sous-corps de  $K$  engendré sur  $\mathbb{Q}$  par  $a_4(q)$  et  $a_6(q)$ , le morphisme d'addition  $E_q \times_K E_q \rightarrow E_q$  est lui aussi défini sur ce sous-corps. Les fractions rationnelles en les  $x_i$ , les  $y_i$ ,  $a_4(q)$  et  $a_6(q)$  qui le définissent seront donc bien à coefficients entiers.*

Maintenant que l'on sait que  $\Phi$  est un morphisme de groupes, il est évident qu'il est injectif. Il ne reste plus qu'à prouver la surjectivité.

## 2.3 Divers rappels

Le terme « anneau » désignera toujours un anneau commutatif unitaire.

### 2.3.1 Groupes formels et courbes elliptiques

**Définition 2.3.1** — *On appelle groupe formel (commutatif) défini sur un anneau  $A$  toute série formelle  $F \in A[[X, Y]]$  congrue à  $X + Y$  modulo  $(X^2, XY, Y^2)$ , vérifiant  $F(X, F(Y, Z)) = F(F(X, Y), Z)$  et  $F(X, Y) = F(Y, X)$ . On dit que  $F$  est la loi du groupe formel, et on note en général le groupe formel  $\mathcal{F}$ .*

Soit un groupe formel de loi  $F$ . On montre qu'il existe une unique série formelle  $i \in A[[T]]$  telle que  $F(T, i(T)) = 0$ , et que l'on a nécessairement  $F(X, 0) = X$  et  $F(0, Y) = Y$ . Le groupe formel défini par  $F(X, Y) = X + Y$  s'appelle le *groupe formel additif* et se note  $\hat{\mathbb{G}}_a$  (l'anneau de définition est implicite). Le groupe formel défini par  $F(X, Y) = X + Y + XY$  s'appelle le *groupe formel multiplicatif* et se note  $\hat{\mathbb{G}}_m$ .

Soit maintenant  $R$  un anneau local complet, d'idéal maximal  $\mathfrak{m}$ . Soit  $\mathcal{F}$  un groupe formel défini sur  $R$ , de loi  $F$ . On lui associe un groupe, noté  $\mathcal{F}(\mathfrak{m})$ , dont l'ensemble sous-jacent est  $\mathfrak{m}$ , et dont l'addition est définie par  $x \oplus_{\mathcal{F}} y = F(x, y)$  (la série converge dans  $R$ ). Le groupe  $\hat{\mathbb{G}}_a(\mathfrak{m})$  est égal à  $\mathfrak{m}$ , qui est un sous-groupe de  $R$ , et le groupe  $\hat{\mathbb{G}}_m(\mathfrak{m})$  est isomorphe au groupe  $1 + \mathfrak{m}$ , qui est un sous-groupe de  $R^*$ , d'où leur nom. Remarquons que l'on a les deux suites exactes suivantes :

$$0 \longrightarrow \hat{\mathbb{G}}_a(\mathfrak{m}) \longrightarrow R \longrightarrow k \longrightarrow 0$$

$$0 \longrightarrow \hat{\mathbb{G}}_m(\mathfrak{m}) \longrightarrow R^* \longrightarrow k^* \longrightarrow 0$$

Soit  $E$  une courbe elliptique sur un corps  $k$ . Choisissons une équation de Weierstrass pour  $E$ , à coefficients dans un sous-anneau  $R$  de  $k$ . On aimerait « extraire » la loi de groupe de  $E$  et lui associer un groupe formel. Pour ce faire, on va considérer le complété de l'anneau local de  $E$  en  $0$  (le neutre), et exprimer les équations qui le définissent en fonction d'une uniformisante  $z$  de  $E$  en  $0$ . Commençons par effectuer un changement de variables, de manière à ramener le neutre de  $E$  (i.e. le point à l'infini, pour le plongement choisi) aux coordonnées  $(0, 0)$ . Plus précisément, on pose  $z = -x/y$  et  $w = -1/y$ . On peut alors réécrire l'équation de Weierstrass en fonction de  $w$  et  $z$ ; on obtient ainsi une équation de la forme  $w = f(z, w)$  avec  $f \in R[Z, W]$ , que l'on aimerait résoudre.

**Proposition 2.3.2** — *Il existe une unique série formelle  $W \in R[[Z]]$  telle que  $W(Z) = f(Z, W(Z))$ . De plus,  $W \in Z^3 + Z^4 R[[Z]]$ .*

Démonstration — C'est une conséquence directe d'une bonne version du lemme de Hensel (l'anneau  $R[[Z]]$  n'est pas nécessairement local), comme énoncé dans [1], IV.1.2. Il faut tout de même calculer  $f$  explicitement.  $\square$

On peut ensuite poser  $Y(Z) = -1/W(Z)$  et  $X(Z) = Z/W(Z)$ ; comme le premier coefficient non nul de  $W$  est 1,  $X$  et  $Y$  sont à coefficients dans  $R$ . Les séries  $X(Z)$  et  $Y(Z)$  sont une solution formelle à l'équation de Weierstrass choisie. En d'autres termes,  $[X(Z) : Y(Z) : 1]$  est un élément de  $E(k((Z)))$  (vu dans  $\mathbb{P}^2(k((Z)))$ ). On peut d'ailleurs composer  $X$  et  $Y$  par n'importe quelle série formelle en  $Z$  de coefficient constant nul, et trouver ainsi un nouveau point de  $E(k((Z)))$ . Il est clair, d'après les expressions de  $X$  et  $Y$  en fonction de  $Z$  et  $W$ , que l'application

$$\begin{aligned} T: ZR[[Z]] &\longrightarrow E(k((Z))) \\ z &\longmapsto [X(z) : Y(z) : 1] \quad \text{si } z \neq 0 \\ 0 &\longmapsto [0 : 1 : 0] \end{aligned}$$

est injective. On montre de plus qu'il existe une unique série formelle  $F \in R[[Z_1, Z_2]]$  telle que pour tous  $z_1$  et  $z_2$  dans  $ZR[[Z]]$ ,  $T(z_1) + T(z_2) = T(F(z_1, z_2))$ . On montre que  $F$  définit un groupe formel, que l'on note  $\hat{E}$ . C'est le groupe formel associé à la courbe elliptique  $E$ .

Le lemme suivant nous sera utile plus tard.

**Lemme 2.3.3** — Soient  $A$  un anneau,  $a \in A^*$ ,  $f \in A[[T]]$  telle que  $f \equiv aT \pmod{T^2}$ . Il existe un unique  $g \in TA[[T]]$  tel que  $f(g(T)) = T$ . On a de plus  $g(f(T)) = T$ .

Démonstration — On construit  $g$  par approximations successives (modulo  $T^n$ ); cela ne présente pas de difficulté particulière. Pour plus de détails, voir [1], IV.2.4.  $\square$

### 2.3.2 Formulaire pour les équations de Weierstrass

On rassemble ici les formules couramment utilisées, pour la commodité du lecteur. La forme générale d'une équation de Weierstrass sur un corps  $k$  est :

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

On définit alors les éléments de  $k$  suivants (notations standard) :

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 & ; & & b_4 &= 2a_4 + a_1a_3 & ; & & b_6 &= a_3^2 + 4a_6 & ; & & b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24b_4 & ; & & c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 & ; & & \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 & ; & & j &= c_4^3/\Delta \end{aligned}$$

Une équation de Weierstrass définit une courbe elliptique si et seulement si  $\Delta \neq 0$ . Lorsque  $\Delta = 0$ , la courbe projective définie par l'équation de Weierstrass possède un unique point singulier, qui est un point double si  $c_4 \neq 0$ , une pointe sinon.

Si l'on a deux équations de Weierstrass qui définissent des courbes elliptiques isomorphes (sur  $k$ ), on peut passer de l'une à l'autre par un changement de coordonnées linéaire; plus précisément :

$$X = u^2X' + r \quad ; \quad Y = u^3Y' + su^2X' + t$$

avec  $u, r, s, t \in k$  et  $u \neq 0$ . On a alors, avec des notations évidentes :

$$u^4c'_4 = c_4 \quad ; \quad u^6c'_6 = c_6 \quad ; \quad u^{12}\Delta' = \Delta$$

### 2.3.3 Rappels sur les courbes elliptiques sur les corps locaux

Soit  $K$  un corps complet pour une valuation discrète  $v$ . On note  $R$  son anneau des entiers,  $\mathfrak{m}$  l'idéal maximal de  $R$  et  $k$  le corps résiduel. Soit  $E$  une courbe elliptique sur  $K$ , donnée par une équation de Weierstrass

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

où les  $a_i$  sont dans  $K$ . On dit que l'équation de Weierstrass est *minimale* si les  $a_i$  sont dans  $R$  et que  $v(\Delta)$  est minimal pour cette propriété. Lorsque tel est le cas, on note  $\tilde{E}$  la courbe projective sur  $k$  définie par la même équation modulo  $\mathfrak{m}$ . Comme toute courbe définie par une équation de Weierstrass,  $\tilde{E}$  a au plus un point singulier, qui peut être un point

double ou une pointe. On dit que  $E$  a *bonne réduction* si  $\tilde{E}$  est régulière (c'est donc une courbe elliptique sur  $k$ ), que  $E$  a *réduction multiplicative* si  $\tilde{E}$  possède un point double (et on parle alors de réduction multiplicative *déployée* si les pentes des deux tangentes sont rationnelles, c'est-à-dire dans  $k$ ), que  $E$  a *réduction additive* sinon. On note  $\tilde{E}_{\text{reg}}$  l'ouvert des points réguliers de  $\tilde{E}$ . Il est muni d'une structure de  $k$ -schéma en groupes, défini par la condition que la somme de trois points alignés est nulle.

Le critère suivant est utile (il se déduit trivialement du formulaire).

**Proposition 2.3.4** — *Si les  $a_i$  sont dans  $R$ , et si  $v(\Delta) < 12$  ou  $v(c_4) < 4$ , l'équation de Weierstrass est minimale.*

Définissons maintenant la réduction d'un point de  $E(K)$  en un point de  $\tilde{E}(k)$ . Soit  $[x : y : z] \in E(K)$ . Quitte à multiplier par un élément bien choisi de  $K$ , on peut supposer que  $x, y$  et  $z$  sont dans  $R$  et que l'un au moins est dans  $R^*$ . Ceci définit  $x, y$  et  $z$  de manière unique; on appelle *réduction modulo  $\mathfrak{m}$*  de  $[x : y : z]$  l'élément de  $\tilde{E}(k)$  de coordonnées homogènes  $[\tilde{x} : \tilde{y} : \tilde{z}]$  (où le tilde signifie « modulo  $\mathfrak{m}$  »). On note cette application  $P \mapsto \tilde{P}$ .

Enfin, on vérifie que  $\tilde{E}$  et la flèche de réduction  $E(K) \rightarrow \tilde{E}(k)$  ne dépendent pas de l'équation de Weierstrass minimale choisie.

Fixons quelques notations :

$$E_0(K) = \left\{ P \in E(K); \tilde{P} \in \tilde{E}_{\text{reg}}(k) \right\} \quad ; \quad E_1(K) = \left\{ P \in E(K); \tilde{P} = \tilde{0} \right\}$$

où  $\tilde{0}$  dénote le neutre de  $E(K)$ , soit le point à l'infini si l'on choisit une équation de Weierstrass. Notons que  $\tilde{0}$  est toujours un point régulier de  $\tilde{E}$  et que c'est même le neutre de  $\tilde{E}_{\text{reg}}(k)$ .

**Proposition 2.3.5** —  *$E_0(K)$  est un sous-groupe de  $E(K)$ , et la flèche de réduction  $E_0(K) \rightarrow \tilde{E}_{\text{reg}}(k)$  est un morphisme surjectif. On a donc la suite exacte :*

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \tilde{E}_{\text{reg}}(k) \longrightarrow 0$$

Démonstration — Il est évident que la flèche de réduction  $E(K) \rightarrow \tilde{E}(k)$  préserve l'alignement. Comme l'alignement détermine la structure de groupe de  $E(K)$  et de  $\tilde{E}_{\text{reg}}(k)$ , cela prouve que  $E_0(K)$  est un sous-groupe de  $E(K)$  et que  $E_0(K) \rightarrow \tilde{E}_{\text{reg}}(k)$  est un morphisme de groupes. La surjectivité est une application du lemme de Hensel; voir [1], VII.2.1 pour les détails.  $\square$

**Proposition 2.3.6** — *Soit  $E/K$  une courbe elliptique, dont on choisit une équation de Weierstrass minimale. On dispose alors du groupe formel  $\hat{E}$  et des séries  $X, Y \in R((Z))$  introduites au numéro précédent. L'application*

$$\begin{aligned} \hat{E}(\mathfrak{m}) &\longrightarrow E_1(K) \subset \mathbb{P}^2(K) \\ z \neq 0 &\longmapsto [X(z) : Y(z) : 1] \\ 0 &\longmapsto [0 : 1 : 0] \end{aligned}$$

*est un isomorphisme de groupes.*

Démonstration — Observons que les séries  $X(z)$  et  $Y(z)$  convergent car  $X$  et  $Y$  sont à coefficients dans  $R$  et  $|z| < 1$ . Pour la preuve (pas difficile), voir [1], VII.2.2.  $\square$

## 2.4 Preuve de la surjectivité de $\Phi$

Pour montrer la surjectivité de  $\Phi: \overline{K}^*/q^{\mathbb{Z}} \rightarrow E_q(\overline{K})$ , il suffit de montrer que pour toute extension finie  $L/K$ , l'application induite  $L^*/q^{\mathbb{Z}} \rightarrow E_q(L)$  est surjective. Une telle extension étant un corps complet, il suffit de prouver la surjectivité de l'application  $K^*/q^{\mathbb{Z}} \rightarrow E_q(K)$  (que l'on note encore  $\Phi$ ), quitte à remplacer  $K$  par  $L$ .

D'après les rappels du numéro précédent, on dispose d'une filtration sur  $E_q(K)$ , et d'une suite exacte où apparaissent  $\hat{E}_q$  ainsi que  $\hat{E}_q$ . On peut résumer ceci par le diagramme suivant.

$$\begin{array}{ccccccc} E_{q,1}(K) & \hookrightarrow & E_{q,0}(K) & \hookrightarrow & E_q(K) & & \\ & & \Big\| & & \Big\| & & \\ 0 & \longrightarrow & \hat{E}_q(\mathfrak{m}) & \longrightarrow & E_{q,0}(K) & \longrightarrow & \tilde{E}_{q,\text{reg}}(k) \longrightarrow 0 \end{array}$$

La situation est analogue du côté de  $K^*/q^{\mathbb{Z}}$  :

$$\begin{array}{ccccccc} 1 + \mathfrak{m} & \hookrightarrow & R^* & \hookrightarrow & K^*/q^{\mathbb{Z}} & & \\ & & \downarrow \wr & & \parallel & & \\ 0 & \longrightarrow & \hat{\mathbb{G}}_{\mathfrak{m}}(\mathfrak{m}) & \longrightarrow & R^* & \longrightarrow & k^* \longrightarrow 0 \end{array}$$

On va non seulement montrer que  $\Phi$  est un isomorphisme, mais qu'il préserve ces deux diagrammes. Notons  $v$  la valuation normalisée sur  $K$  (i.e. à valeur dans  $\mathbb{Z}$  et surjective). Avant tout, remarquons que l'équation de Weierstrass que l'on étudie (i.e. l'équation 1) est minimale. En effet, elle est à coefficients dans  $R_q$ , et un petit calcul montre que  $c_4 = 1 - 48a_4(q)$ ; comme  $a_4 \in Q\mathbb{Z}[[Q]]$ , on en déduit que  $v(c_4) = 0 < 4$ . Ainsi,  $E_q$  est définie par l'équation de Weierstrass  $y^2 + xy = x^3$ , ce qui montre que  $E_q$  est à réduction multiplicative déployée, et que le point singulier de  $\tilde{E}_q$  est  $[0 : 0 : 1]$ .

**Étape 1** — On a  $\Phi(1 + \mathfrak{m}) = E_{q,1}(K)$ .

Démonstration — Soit  $u \in 1 + \mathfrak{m}$ ,  $u \neq 1$ . En regardant la définition de  $X_K(u, q)$ , on voit tout de suite que  $v(X_K(u, q)) < 0$  (ne pas oublier que  $v(q) > 0$ ). Ainsi, pour réduire  $P = [X_K(u, q) : Y_K(u, q) : 1]$  modulo  $\mathfrak{m}$ , il faudra d'abord multiplier par une puissance strictement positive d'une uniformisante. Cela montre que la coordonnée  $z$  de  $\tilde{P}$  est nulle, i.e.  $\tilde{P}$  est un point à l'infini, mais le seul tel point est  $\tilde{0}$ ; d'où une inclusion.

D'après les diagrammes précédents, l'application  $1 + \mathfrak{m} \rightarrow E_{q,1}(K)$  induite par  $\Phi$  s'identifie à :

$$\begin{array}{ccc} \mathfrak{m} & \longrightarrow & \mathfrak{m} \\ t & \longmapsto & -\frac{X_K(1+t, q)}{Y_K(1+t, q)} \end{array}$$

(Rappelons que si  $\mathcal{F}$  est un groupe formel, l'ensemble sous-jacent à  $\mathcal{F}(\mathfrak{m})$  est  $\mathfrak{m}$ .) Pour  $t \in \mathfrak{m}$ , on peut développer  $X_K(1+t, q)$  et  $Y_K(1+t, q)$  en série entière (utiliser l'expression qui apparaît au début de la preuve du lemme 2.2.1 et faire de même pour  $Y_K$ ), de sorte qu'il existe des  $a_n$  et des  $b_n$  dans  $R$  tels que, pour  $t \in \mathfrak{m}$  :

$$\begin{aligned} X_K(1+t, q) &= \frac{1}{t^2} \left( 1 + \sum_{n \geq 1} a_n t^n \right) \\ Y_K(1+t, q) &= \frac{1}{t^3} \left( -1 + \sum_{n \geq 1} b_n t^n \right) \end{aligned}$$

Ainsi, il s'agit de voir que l'application  $\mathfrak{m} \rightarrow \mathfrak{m}$ ,  $t \mapsto t \left( 1 + \sum_{n \geq 1} c_n t^n \right)$  est surjective, où les  $c_n$  sont dans  $R$ . Ceci découle directement du lemme 2.3.3.  $\square$

**Étape 2** — On a  $\Phi(R^*) \subset E_{q,0}(K)$ .

Démonstration — Soit  $u \in R^*$ . Si  $u \in 1 + \mathfrak{m}$ , on peut utiliser l'étape 1; supposons donc  $u$  non congru à 1 modulo  $\mathfrak{m}$ . On voit alors tout de suite sur les expressions de  $X_K(u, q)$  et de  $Y_K(u, q)$  que  $v(X_K(u, q)) = v(Y_K(u, q)) = 0$ . Ainsi,  $\Phi(u)$  ne peut pas être le point  $[0 : 0 : 1]$ .  $\square$

On déduit des étapes précédentes une flèche  $\tilde{\Phi} : k^* \rightarrow \tilde{E}_{q, \text{reg}}(k)$ , par restriction à  $R$  et passage au quotient.

**Étape 3** — L'application  $\tilde{\Phi}$  est bijective.

Démonstration — Explicitions  $\tilde{\Phi}$  : en réduisant  $X_K(u, q)$  et  $Y_K(u, q)$  modulo  $\mathfrak{m}$ , on voit que

$$\tilde{\Phi}(u) = [u(1-u) : u^2 : (1-u)^3]$$

pour  $u \in k^*$ . L'application  $[x : y : z] \mapsto y^2 z / x^3$  est donc réciproque de  $\tilde{\Phi}$ , d'où le résultat.  $\square$

Les étapes 1 et 3, l'injectivité de  $\Phi$  et le lemme des cinq montrent que  $\Phi$  induit une bijection entre  $R^*$  et  $E_{q,0}(K)$ . Pour prouver la surjectivité de  $\Phi$ , il suffit de voir que l'application  $K^*/(R^*q^{\mathbb{Z}}) \rightarrow E_q(K)/E_{q,0}(K)$  est bijective, encore d'après le lemme des cinq. Cette application est injective et le groupe  $K^*/(R^*q^{\mathbb{Z}})$  est d'ordre  $v(q)$ . Le théorème sera donc prouvé si l'on montre que

$$\text{Card}(E_q(K)/E_{q,0}(K)) \leq v(q).$$

À vrai dire, cette inégalité découle de considérations géométriques sur la fibre spéciale du modèle de Néron de  $E_q$ . Précisons les choses. Si  $E$  est une courbe elliptique sur  $K$ , on prouve qu'il existe un modèle propre et régulier de  $E$  sur  $R$  (c'est-à-dire un  $R$ -schéma propre, régulier, plat et de type fini, dont la fibre générique est  $E$ ), et qu'il en existe un minimal (notons-le  $\mathcal{C}$ ), au sens où tout  $R$ -morphisme de  $\mathcal{C}$  vers un autre modèle propre et régulier de  $E$  sur  $R$  qui induit un isomorphisme sur la fibre générique est en fait un isomorphisme. Il existe une classification pour la fibre spéciale de  $\mathcal{C}$  (due à Kodaira et Néron), et un algorithme (dû à Tate) pour déterminer, à partir d'une équation de Weierstrass de  $E$ , dans quel cas de la classification on se trouve. Lorsqu'on applique l'algorithme de Tate à l'équation de  $E_q$ , on trouve tout de suite que la fibre spéciale de  $\mathcal{C}$  comporte  $n$  composantes irréductibles  $C_i$  de multiplicité 1 (avec  $n = v(\Delta(q))$ ), indexées par  $\mathbb{Z}/n\mathbb{Z}$ , où  $C_i$  rencontre  $C_{i+1}$  en un seul point, transversalement. D'autre part, la structure de  $K$ -schéma en groupes de  $E$  s'étend en une structure de  $R$ -schéma en groupes sur l'ouvert de lissité de  $\mathcal{C}$  sur  $R$  (notons  $\mathcal{E}$  cet ouvert – c'est le modèle de Néron de  $E$  sur  $R$ ). On montre que la section nulle de  $\mathcal{E}$  (i.e. le neutre de  $\mathcal{E}(R)$ ) rencontre exactement l'un des  $C_i$ , et que l'ouvert de lissité de ce  $C_i$ -là est un sous-schéma en groupes de  $\mathcal{E}$ , que l'on note  $\mathcal{E}^0$ . On montre enfin que  $E(K)/E_0(K)$  s'identifie à  $\mathcal{E}(R)/\mathcal{E}^0(R)$ , puis à  $\mathcal{E}(k)/\mathcal{E}^0(k)$ , mais il est évident que dans le cas de  $E_q$ , ce groupe est de cardinal  $n$ , d'après la description de la fibre spéciale de  $\mathcal{E}$ . Remarquons enfin qu'on a bien  $n = v(q)$ .

On peut aussi le prouver de manière très élémentaire. Il s'agit en fait de la même preuve, mais de laquelle on a retiré tout ce qui n'était pas calculatoire. Bornons-nous à donner les étapes principales de la démonstration, car le reste présente peu d'intérêt. Fixons une uniformisante  $\pi$  de  $R$ , et posons :

$$\begin{aligned} U_n &= \{(x, y) \in E_q(K) ; |\pi|^n = |y| > |x + y|\} \\ V_n &= \{(x, y) \in E_q(K) ; |\pi|^n = |x + y| > |y|\} \\ W &= \{(x, y) \in E_q(K) ; |y| = |x + y| = |q|^{1/2}\} \end{aligned}$$

On prouve que l'on a alors

$$E_q(K) = E_{q,0}(K) \cup W \cup \bigcup_{1 \leq n < \frac{1}{2}v(q)} (U_n \cup V_n)$$

et que ces réunions sont disjointes : il s'agit d'une partition de  $E_q(K)$  en au plus  $v(q)$  parties. On prouve ensuite que cette partition est plus fine que celle obtenue en considérant tous les translatés de  $E_{q,0}(K)$ , ce qui donne le résultat voulu.

### 3 Uniformisation $p$ -adique

Le théorème de la section précédente est l'analogue  $p$ -adique de l'assertion « pour  $\tau \in \mathfrak{H}$ ,  $E_\tau(\mathbb{C})$  s'écrit sous la forme  $\mathbb{C}/\Lambda$  ». Il reste à montrer un analogue de « toute courbe elliptique sur  $\mathbb{C}$  est isomorphe à  $E_\tau$  pour un certain  $\tau$  » ; c'est l'uniformisation  $p$ -adique. On ne peut espérer que toute courbe elliptique sur un corps  $p$ -adique  $K$  soit isomorphe à  $E_q$  pour un certain  $q$ , puisque l'on a toujours  $|j(E_q)| > 1$  (en effet, un petit calcul montre que  $j(E_q) = 1/q + \sum_{n \geq 0} c(n)q^n$  où  $c(n) \in \mathbb{Z}$ ). Cependant, nous verrons que toute courbe elliptique  $E$  sur  $K$  telle que  $|j(E)| > 1$  est isomorphe à une courbe  $E_q$ , quitte à passer à une extension quadratique de  $K$ .

#### 3.1 Invariant $j$ et invariant $\gamma$

Soit  $K$  un corps de caractéristique différente de 2 et de 3. Fixons une clôture algébrique  $\overline{K}$  de  $K$ . L'invariant  $j$  d'une courbe elliptique  $E$  sur  $K$  caractérise  $E$  à  $\overline{K}$ -isomorphisme près seulement. On aimerait un autre invariant, qui, à l'intérieur d'une classe de  $\overline{K}$ -isomorphisme de courbes elliptiques sur  $K$ , caractérise la classe de  $K$ -isomorphisme. C'est le rôle de l'invariant  $\gamma$ .

**Proposition-définition 3.1.1** — *Soit  $E$  une courbe elliptique sur  $K$  d'invariant  $j$  différent de 0 et de 1728. Choisissez une équation de Weierstrass de  $E$  ; on utilisera les notations standard pour les quantités qui lui sont associées ( $\Delta$ ,*

$c_4, c_6, \text{ etc.}$ ). Considérons  $-c_4/c_6$  comme un élément de  $K^*/K^{*2}$  (il est bien défini car la condition sur  $j(E)$  équivaut à  $c_4 \neq 0$  et  $c_6 \neq 0$ ); il ne dépend pas de l'équation de Weierstrass choisie. On l'appelle invariant  $\gamma$  de  $E$  sur  $K$  et on le note  $\gamma(E/K)$ .

Démonstration — L'indépendance de  $\gamma(E/K)$  par rapport à l'équation de Weierstrass choisie est triviale d'après le formulaire.  $\square$

**Proposition 3.1.2** — Soient  $E$  et  $E'$  deux courbes elliptiques sur  $K$  dont les invariants  $j$  sont différents de 0 et de 1728. Elles sont isomorphes sur  $K$  si et seulement si elles ont même invariant  $j$  et même invariant  $\gamma$ . Supposons maintenant que  $j(E) = j(E')$  mais  $\gamma(E/K) \neq \gamma(E'/K)$ . Soit  $L$  l'extension quadratique de  $K$  engendrée par une racine carrée de  $\gamma(E/K)/\gamma(E'/K)$ . Les courbes  $E$  et  $E'$  sont  $L$ -isomorphes, et il existe un  $L$ -isomorphisme  $\psi: E_L \rightarrow E'_L$  tel que  $\psi \circ \sigma = \chi(\sigma)\psi$ , pour  $\sigma \in \text{Gal}(L/K)$ , où  $\chi: \text{Gal}(L/K) \rightarrow \{-1; 1\}$  est l'unique isomorphisme (le caractère quadratique).

Démonstration — Il n'y a pas de difficulté particulière. On utilise l'hypothèse sur la caractéristique pour pouvoir écrire des équations de Weierstrass de  $E$  et  $E'$  sous la forme  $y^2 = x^3 + Ax + B$ . Voir [2], V.5.2.  $\square$

## 3.2 Théorème d'uniformisation $p$ -adique

Le théorème suivant est dû à Tate.

**Théorème 3.2.1** — Soient  $K$  un corps  $p$ -adique,  $\overline{K}$  une clôture algébrique de  $K$  et  $E$  une courbe elliptique sur  $K$  telle que  $|j(E)| > 1$ . Il existe alors un unique  $q \in \overline{K}^*$  vérifiant  $|q| < 1$  et tel que  $E$  soit  $\overline{K}$ -isomorphe à  $E_q$ . Soit  $q_0$  cette valeur de  $q$ . On a alors  $q_0 \in K$ . De plus, les conditions suivantes sont équivalentes :

1.  $E$  est  $K$ -isomorphe à  $E_{q_0}$ .
2.  $\gamma(E/K) = 1$ .
3.  $E$  a réduction multiplicative déployée.

Démonstration — Pour  $q \in \overline{K}^*$  tel que  $|q| < 1$ , on a  $j(E_q) = c_4(q)^3/\Delta(q) = (1 - 48a_4(q))^3/\Delta(q)$  or  $a_4 \in Q\mathbb{Z}[[Q]]$  et  $\Delta \in Q + Q^2\mathbb{Z}[[Q]]$ , donc on peut développer  $qj(E_q)$  en série entière (les coefficients sont entiers et  $|q| < 1$ ). De plus, ceci montre que le coefficient constant de  $qj(E_q)$  est 1. Ainsi,  $j(E_q) = 1/q + \sum_{n \geq 0} c(n)q^n$  où  $c(n)$  est un entier. Soit

$$J = 1/Q + \sum_{n \geq 0} c(n)Q^n \in \mathbb{Z}((Q)).$$

Comme  $1/J \in Q + Q^2\mathbb{Z}[[Q]]$ , le lemme 2.3.3 montre l'existence de  $G \in Q\mathbb{Z}[[Q]]$  tel que  $J \circ G = 1/Q$ . Soit  $q = G(1/j(E))$  (la série converge puisque  $|j(E)| > 1$ ); on a alors  $J(q) = j(E)$ , mais  $J(q) = j(E_q)$  et donc  $E$  et  $E_q$  sont  $\overline{K}$ -isomorphes. Par ailleurs, on a bien  $q \in K$ .

Montrons l'unicité d'un tel  $q$ . Soient  $q$  et  $q'$  dans  $\overline{K}^*$  tels que  $|q| < 1$ ,  $|q'| < 1$  et  $J(q) = J(q')$ . Comme  $1/J \in Q + Q^2\mathbb{Z}[[Q]]$ ,  $|1/J(q) - 1/J(q')| = |q - q'|$ , d'où  $q = q'$ .

Montrons maintenant l'équivalence de (1) et (2). D'après la proposition 3.1.2, il suffit de montrer que  $\gamma(E_q/K) = 1$  pour tout  $q \in K^*$  tel que  $|q| < 1$ . Comme  $\gamma(E_q/K) = -c_4(q)/c_6(q)$ , il suffit de montrer que  $c_4(q)$  et  $-c_6(q)$  sont des carrés dans  $K$ . On trouve que  $c_4(q) = 1 - 48a_4(q) = 1 + 240s_3(q)$  et que  $c_6(q) = -1 + 504s_5(q)$ . Comme  $s_k \in Q + Q^2\mathbb{Z}[[Q]]$ , le lemme suivant permet de conclure.

**Lemme 3.2.2** — Soit  $x \in K$  tel que  $|x| < 1$ . Alors  $1 + 4x$  est un carré dans  $K$ .

Démonstration — Soit  $S = (1 + 4X)^{-1/2} \in \mathbb{Q}[[X]]$  (la puissance  $-1/2$  signifie que l'on considère la série obtenue en développement à l'aide des coefficients binomiaux). On vérifie que  $S \in \mathbb{Z}[[X]]$ . Ainsi,  $S(x)$  converge dans  $K$ , et l'on a  $S(x)^2 = S^2(x) = (1 + 4x)^{-1}$  puisque  $|x| < 1$ , d'où le résultat.  $\square$

Il reste à montrer l'équivalence avec 3. On a déjà vu que  $E_q$  a réduction multiplicative déployée : 1 et 2 impliquent donc bien 3. Supposons donc que  $E$  a réduction multiplicative déployée et montrons 2. On choisit une équation de Weierstrass minimale pour  $E$  :

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

Comme  $E$  n'a pas bonne réduction,  $\tilde{E}$  possède un unique point singulier. Quitte à changer de coordonnées par une translation (ce qui n'altère pas le discriminant, et donc la minimalité de l'équation de Weierstrass), on peut supposer que le point singulier de  $\tilde{E}$  est le point rationnel de coordonnées homogènes  $[0 : 0 : 1]$ . Que le point  $[0 : 0 : 1]$  soit sur la courbe signifie que  $a_6 \in \mathfrak{m}$ . Qu'il soit de plus singulier signifie que  $a_3 \in \mathfrak{m}$  et  $a_4 \in \mathfrak{m}$ . On en déduit que  $b_4 \in \mathfrak{m}$  et  $c_4 \equiv b_2^2 \pmod{\mathfrak{m}}$ . Comme  $E$  a réduction multiplicative,  $\tilde{E}$  possède un point double; l'équation de Weierstrass considérée étant minimale,  $c_4 \notin \mathfrak{m}$ , et donc  $b_2 \notin \mathfrak{m}$ , et donc  $|b_2| = 1$ . Ainsi, on peut écrire :

$$\gamma(E/K) = \frac{1}{b_2} \left( \frac{1 - 24 \frac{b_4}{b_2^2}}{1 - 36 \frac{b_4}{b_2^2} + 216 \frac{b_6}{b_2^3}} \right)$$

On voudrait voir que  $\gamma(E/K)$  est un carré dans  $K$ . D'après le lemme 3.2.2, on peut déduire de l'équation précédente que  $\gamma(E/K) \equiv b_2 \pmod{K^{\star 2}}$ ; il suffit donc de voir que  $b_2$  est un carré. La courbe  $\tilde{E}$  a pour équation

$$y^2 + \tilde{a}_1 xy = x^3 + \tilde{a}_2 x^2.$$

L'hypothèse que les deux pentes des tangentes au point singulier sont rationnelles signifie que le polynôme homogène  $y^2 + \tilde{a}_1 xy - \tilde{a}_2 x^2$  est scindé à racines simples dans  $k$ . D'après le lemme de Hensel,  $y^2 + a_1 xy - a_2 x^2$  est donc scindé à racines simples dans  $K$  :

$$y^2 + a_1 xy - a_2 x^2 = (y - \alpha x)(y - \beta x)$$

avec  $\alpha, \beta \in R$ . Mais alors  $b_2 = a_1^2 + 4a_2 = (\alpha - \beta)^2$ , d'où le résultat.  $\square$

Signalons une application intéressante du théorème d'uniformisation  $p$ -adique, due à Serre.

**Théorème 3.2.3** — Soient  $K$  un corps de nombres,  $E$  une courbe elliptique à multiplication complexe sur  $K$ . Alors  $j(E)$  est entier sur  $\mathbb{Z}$ .

Démonstration (esquisse très rapide) — Soit  $v$  une place finie de  $K$ ; soit  $\psi$  un endomorphisme de  $E$  qui ne soit pas la multiplication par un certain entier. On veut montrer que  $j(E)$  est entier en  $v$ ; supposons qu'il ne le soit pas. On peut alors appliquer le théorème d'uniformisation à la courbe elliptique  $E_v = E \times_K K_v$  sur  $K_v$ ; on prouve ensuite, à l'aide de l'isomorphisme  $E_v(\overline{K}_v) \approx \overline{K}_v^{\star}/q^{\mathbb{Z}}$ , qu'il existe un élément  $\sigma \in \mathcal{G}_{K_v}$  qui agit sur la  $l$ -torsion de  $E_v(\overline{K}_v)$  par une transvection, pour tout  $l$  premier sauf un nombre fini. L'hypothèse que  $\psi \notin \mathbb{Z}$  signifie en particulier que  $\psi' = 2\psi - \deg(\psi)$  n'est pas de degré nul, et donc que le déterminant de l'action de  $\psi'$  sur la  $l$ -torsion de  $E_v(\overline{K}_v)$  est non nul dans  $\mathbb{Z}/l\mathbb{Z}$  pour presque tout  $l$ . Or cette action doit commuter avec celle de  $\sigma$ ; ceci permet d'aboutir à une contradiction.  $\square$

## Bibliographie

- [1] SILVERMAN, Joseph H., The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, No. 106, Springer-Verlag, New York, 1992.
- [2] SILVERMAN, Joseph H., Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, No. 151, Springer-Verlag, New York, 1999.