

COURS DE L'INSTITUT FOURIER

ARMAND BRUMER

III- Réduction des courbes elliptiques. Applications

Cours de l'institut Fourier, tome 10 (1975), p. 114-138

http://www.numdam.org/item?id=CIF_1975__10__A4_0

© Institut Fourier – Université de Grenoble, 1975, tous droits réservés.

L'accès aux archives de la collection « Cours de l'institut Fourier » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

III - réduction des courbes elliptiques. applications

1. MAUVAISE REDUCTION D'UNE COURBE ELLIPTIQUE.

1.1. REDUCTION ADDITIVE OU MULTIPLICATIVE.

1.1.1. Soient K un corps quelconque, E une cubique plane définie sur K , d'équation affine $F(x,y) = 0$ où

$$F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \quad (a_i \in K).$$

Le discriminant Δ de la cubique E a été défini en (I.1.1.2) ; il appartient à $\mathbb{Z}[a_1, a_2, \dots, a_6]$.

Si Δ est non nul, la cubique est non singulière, autrement dit c'est une courbe elliptique. Dans le cas contraire, la cubique est dite singulière ou dégénérée.

PROPOSITION. Une cubique singulière a un seul point singulier. De plus, si K est parfait, ou de caractéristique différente de 2 et 3, ce point singulier est rationnel sur K .

■ S'il y avait 2 points singuliers, l'intersection de la droite les joignant et de la cubique serait d'ordre au moins égal à 4 : c'est impossible, donc il y a un seul point singulier ; à cause de son unicité, il est invariant par tout K -automorphisme, donc purement inséparable sur K . Si K est parfait, cela prouve la proposition. Si la caractéristique de K est différente de 2 ou 3, on peut prendre l'équation de E sous la forme de Weierstrass $y^2 = 4x^3 - g_2x - g_3$ (g_2 et $g_3 \in K$) ; le point singulier

vérifie de plus : $y = 0$, $12x^2 - g_2 = 0$, ce qui donne : $x = -3g_3/2g_2$, $y = 0$; ce point est bien rationnel sur K . ■

1.1.2. Supposons, pour simplifier les démonstrations, que la caractéristique de K est impaire. Soit E une cubique dégénérée dont le point singulier est rationnel sur K . Prenons ce point pour origine (dans le plan !) ; alors $F(0,0) = F'_x(0,0) = F'_y(0,0) = 0$, c'est-à-dire $a_6 = a_4 = a_3 = 0$, et l'équation de E devient : $y^2 + a_1xy = x^3 + a_2x^2$.

Les tangentes à l'origine ont pour équation $y = \lambda x$, où λ est racine du trinôme $X^2 + a_1X - a_2$, dont le discriminant est $b_2 = a_1^2 + 4a_2$.

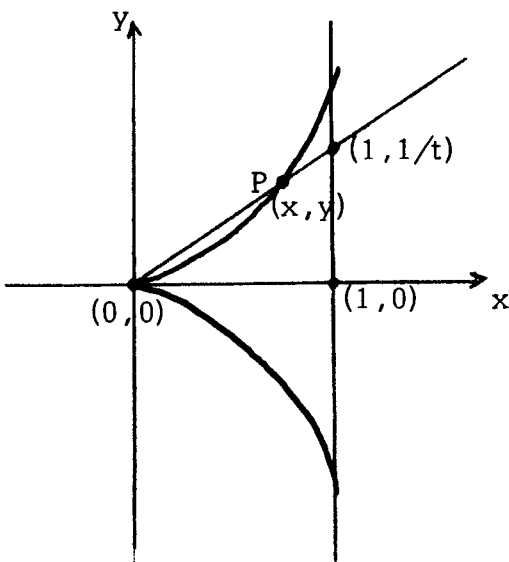
On sait que l'ensemble $E_{(0)}(K)$ des points non singuliers de $E(K)$ forme un groupe abélien dont la loi peut être définie géométriquement par : $P_1 + P_2 + P_3 = 0$ si et seulement si P_1, P_2, P_3 sont alignés sur $E_{(0)}(K)$. (cf.[11] , 5.6).

Nous allons voir que $E_{(0)}(K)$ est isomorphe au groupe additif K^+ , ou au groupe multiplicatif K^* , ou encore au groupe multiplicatif des éléments de norme 1 dans une extension quadratique de K .

1.1.3. Réduction additive.

PROPOSITION . Si $b_2 = 0$, alors $E_{(0)}(K) \simeq K^+$.

■ Lorsque $b_2 = 0$, la cubique a une tangente double à l'origine ; on peut supposer que cette tangente est la droite $y = 0$, et que la courbe a pour équation : $y^2 = x^3$.



La projection centrale de centre $(0,0)$ sur la droite $x = 1$ permet de définir une bijection entre $E_{(0)}(K)$ et K , par : $(x,y) \mapsto t = x/y$ (cela revient à paramétrer la cubique par $t : x = t^{-2}$, $y = t^{-3}$). Un calcul facile montre qu'alors, si 3 points P_i ($i=1,2,3$) non singuliers sont

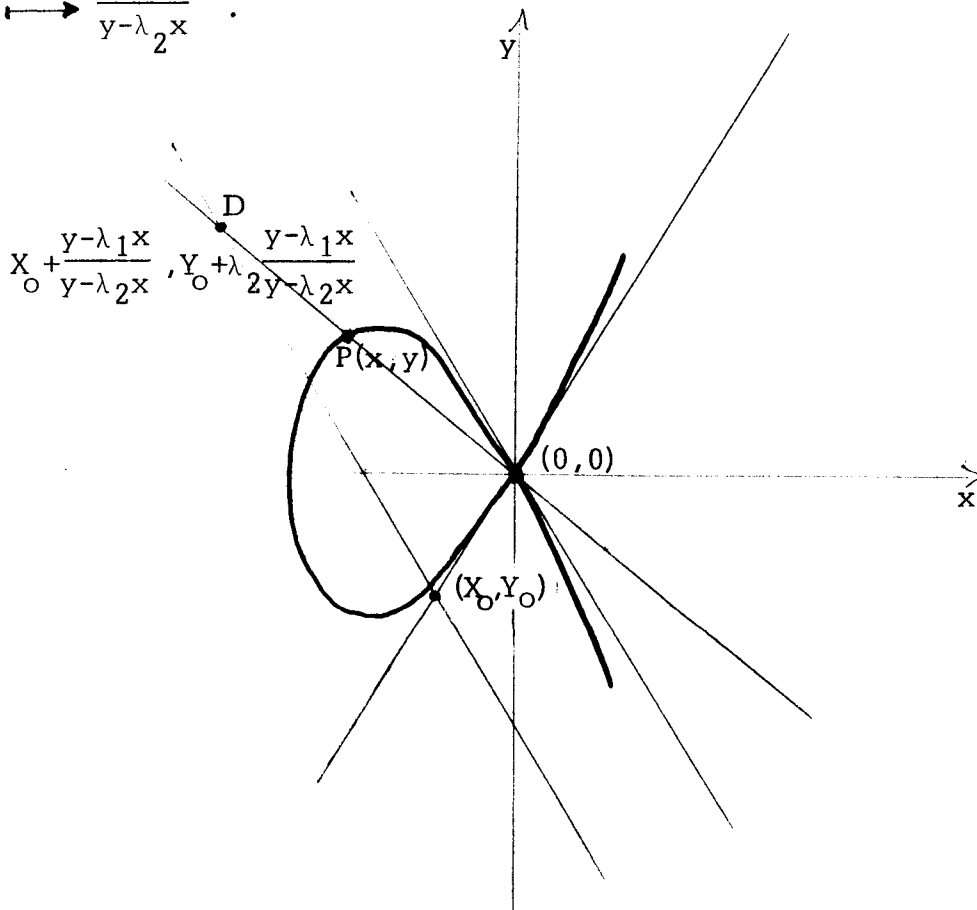
alignés sur la courbe, leurs paramètres t_i vérifient : $t_1 + t_2 + t_3 = 0$.
La bijection définie ci-dessus est donc un isomorphisme de groupes. ■

1.1.4. Réduction multiplicative.

PROPOSITION . Si $b_2 \neq 0$, et si $b_2 \in (K^*)^2$, alors $E_{(0)}(K) \simeq K^*$;
Si $b_2 \neq 0$, et si $b_2 \notin (K^*)^2$, alors $E_{(0)}(K) \simeq \{t \in K(\sqrt{b_2})/N_{K(\sqrt{b_2})/K}(t) = 1\}$

■ Lorsque $b_2 \neq 0$, la cubique a 2 tangentes distinctes à l'origine, de pente λ_1 et λ_2 . Si $b_2 \in (K^*)^2$, elles sont rationnelles sur K , et la projection de centre $(0,0)$ sur la droite $y = \lambda_2 x - \lambda_1 + \lambda_2$ permet de définir une bijection entre $E_{(0)}(K)$ et l'ensemble $K^* = K - \{0\}$, par :

$$(x, y) \longmapsto \frac{y - \lambda_1 x}{y - \lambda_2 x} .$$



Le calcul montre que cette bijection est un isomorphisme de groupes.

Enfin, si $b_2 \notin (K^*)^2$, les deux tangentes à l'origine sont irrationnelles sur K ; elles sont conjuguées sur K , et l'application $(x, y) \longmapsto \frac{y - \lambda_1 x}{y - \lambda_2 x}$

définit un isomorphisme entre $E_{(0)}(K)$ et le groupe multiplicatif des éléments de norme 1 dans $K(\sqrt{b_2})/K$: montrons la surjectivité de cette application : soient θ un élément de $K(\sqrt{b_2})$ de norme 1, et σ le générateur de $\text{Gal}(K(\sqrt{b_2})/K)$; d'après le "théorème 90" de Hilbert, il existe un élément α dans $K(\sqrt{b_2})$ tel que $\theta = \alpha^\sigma / \alpha$; comme $K(\sqrt{b_2}) = K(\lambda_2)$, et $\lambda_2^\sigma = \lambda_1$, on peut écrire $\alpha = y - \lambda_2 x$ et $\theta = \frac{y - \lambda_1 x}{y - \lambda_2 x}$ avec x, y dans K . ■

1.1.5. Application : Soit K un corps local de caractéristique résiduelle non nulle (éventuellement égale à 2), et d'idéal maximal \mathfrak{p} . Soit E une courbe elliptique sur K , définie par une équation minimale, et ayant mauvaise réduction modulo \mathfrak{p} (i.e. $\Delta \equiv 0 \pmod{\mathfrak{p}}$). Notons par un tilde la réduction modulo \mathfrak{p} .

Rappelons que le symbole quadratique $\left(\frac{d}{\mathfrak{p}}\right)$, défini pour tout élément entier d d'un corps local K de caractéristique résiduelle non nulle et d'idéal maximal \mathfrak{p} , vaut 0 (resp. +1, -1) si l'extension $K(\sqrt{d})/K$ est totalement ramifiée (resp. est triviale, est non ramifiée). De plus, si la caractéristique résiduelle de K est impaire, on montre que $\left(\frac{d}{\mathfrak{p}}\right)$ vaut 0 (resp. +1, -1) si la réduction \tilde{d} de d est nulle (resp. est un carré, n'est pas un carré) dans \tilde{K} .

Remarquons que, si l'on change l'équation de E , alors c_6 est remplacé par $c'_6 = u^6 c_6$, où u est un élément algébrique sur K . Si ces deux équations sont minimales, alors u est une unité et $\left(\frac{-c_6}{\mathfrak{p}}\right) = \left(\frac{-c'_6}{\mathfrak{p}}\right)$. Nous pouvons maintenant énoncer :

PROPOSITION . Soit K un corps local de caractéristique résiduelle non nulle et d'idéal maximal \mathfrak{p} . Soit E une courbe elliptique sur K , et soit c_6 l'"invariant" de E défini ci-dessus. Supposons que la réduction de E modulo \mathfrak{p} est mauvaise. Elle est alors de type :

- (i) additif si $\left(\frac{-c_6}{\mathfrak{p}}\right) = 0$;
- (ii) multiplicatif à tangentes rationnelles si $\left(\frac{-c_6}{\mathfrak{p}}\right) = +1$;
- (iii) multiplicatif à tangentes irrationnelles si $\left(\frac{-c_6}{\mathfrak{p}}\right) = -1$.

■ Lorsque la caractéristique résiduelle de K est impaire, on utilise ce qui précède : le changement de variable effectué en (1.1.2) donne : $\tilde{a}_6 = \tilde{a}_3 = \tilde{a}_4 = 0$, et $\tilde{c}_6 = -\tilde{b}_2^3$; ensuite, les propositions (1.1.3) et (1.1.4) donnent le type de la réduction de E en fonction de $-\tilde{c}_6$, et en fait en fonction de $(\frac{-c_6}{p})$.

Lorsque la caractéristique résiduelle de K est égale à 2, une étude analogue démontre la proposition. ■

1.1.6. Définitions. Soit E une courbe elliptique sur \mathbb{Q} . Son conduc-
teur (algébrique) est défini par : $N = \prod_{p|\Delta} p^{f_p}$, où Δ est le discriminant
d'une équation minimale pour E , où $f_p = 1$ si la réduction en p est
multiplicative, $f_p = 2$ (resp. $f_p \geq 2$) si la réduction en p est additive
et $p \geq 5$ (resp. $p = 2$ ou 3) ; lorsque $p = 2$ ou 3 , $f_p - 2$ mesure la
"ramification sauvage" (cf.[25]). On dit que E est semi-stable si N
n'a pas de facteur carré, c'est-à-dire si les mauvaises réductions de E
sont toutes de type multiplicatif.

1.2. COURBES DE TATE ET REDUCTION MULTIPLICATIVE.

Soient K un corps local, \mathcal{O} , \mathfrak{p} comme précédemment ; soient U
le groupe des unités de \mathcal{O} , et v la valuation de K normalisée par
 $v(K^*) = \mathbb{Z}$.

1.2.1. *PROPOSITION*. Toute courbe de Tate sur K est à réduction multi-
plicative à tangentes rationnelles.

■ Nous avons vu (I.3.3) que, pour tout $q \in \mathfrak{p}$, la courbe $E(q)$
d'équation $Y^2 - XY = X^3 - h_2X - h_3$, où h_2 et h_3 sont définis par des
séries entières en q à coefficients entiers rationnels sans termes cons-
tants, est une courbe elliptique sur K . Sa réduction modulo \mathfrak{p} est la
courbe $\tilde{E}(q)$ d'équation $Y^2 - XY = X^3$: c'est une cubique dégénérée, dont
les tangentes au point double sont distinctes et rationnelles sur K (I.3.3.3). ■

1.2.2. *PROPOSITION* . Si E est une courbe elliptique sur K à réduction multiplicative à tangentes irrationnelles, l'extension quadratique $K(\sqrt{b_2})/K$ est non ramifiée.

■ Puisque \tilde{b}_2 est le discriminant du trinôme dont les racines sont les pentes des tangentes au point double de \tilde{E} (cf. 1.1.2), les tangentes sont rationnelles sur $\widetilde{K(\sqrt{b_2})}$. Cela prouve, d'après la proposition (1.1.5), que $-\tilde{c}_6$ n'est pas un carré dans \tilde{K} mais en est un dans $\widetilde{K(\sqrt{b_2})}$, autrement dit que $[K(\sqrt{b_2}) : \tilde{K}] = 2$. D'autre part, $K(\sqrt{b_2})$ est le corps de décomposition (sur K) du trinôme $X^2 + a_1X - a_2$, dont les racines sont distinctes. Ainsi, $K(\sqrt{b_2})/K$ est séparable, et l'extension est non ramifiée. ■

1.2.3. *THEOREME* . Soit E une courbe elliptique sur K à réduction multiplicative. Si la réduction de E est à tangentes rationnelles (sur K), alors E est une courbe de Tate sur K ; sinon, E est une courbe de Tate sur une extension quadratique non ramifiée de K .

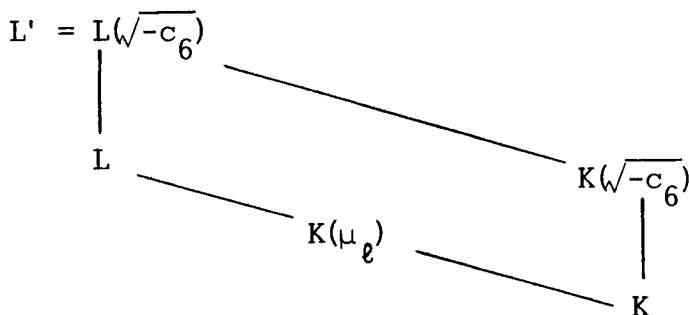
■ L'invariant j de E est tel que $v(j) < 0$: en effet, $v(\Delta) > 0$ car la réduction est mauvaise, $v(c_6) = 0$ car elle est multiplicative (proposition 1.1.5), et $j = \frac{\Delta + c_6^2}{\Delta}$. Donc il existe un unique $q \in \mathfrak{p}$ tel que $j = j(q) = \frac{1}{q} + \sum_{n \geq 0} c(n)q^n$ (cf. I.3.3.1); mais alors E et $E(q)$ sont \bar{K} -isomorphes.

Supposons d'abord que \tilde{E} est à tangentes rationnelles (sur \tilde{K}). Notons c_4 et c_6 (resp. c'_4 et c'_6) les invariants de E (resp. de $E(q)$) définis en (I.1.1.2). Montrons que E et $E(q)$ sont, en fait, isomorphes sur $K(\sqrt{-c_6})$: il existe un élément u de \bar{K}^* tel que $c'_4 = u^4 c_4$ et $c'_6 = u^6 c_6$; or \tilde{c}_6 et \tilde{c}'_6 sont non nuls puisque la réduction est multiplicative; donc u est une unité de \bar{K}^* , et $u^2 = \frac{c_6}{c'_6} \times \frac{c'_4}{c_4}$ est dans K : ainsi, $K(u) = K(u^3) = K(\sqrt{\frac{c_6}{c'_6}})$. Or $-c'_6 = 1 - 504 \sum_{n=1}^{\infty} n^5 \frac{q^n}{1-q^n}$ est un carré : c'est clair si la caractéristique résiduelle est impaire; si elle

est égale à 2 , on utilise la formule : $(U^{(2e)})^2 = U^{(3e)}$ (où e désigne l'indice de ramification de K sur Φ_2 , et où $U^{(n)} = 1 + \rho^n$ (cf. [17] .2.3)), et le fait que 8 divise 504. Donc $K(u) = K(\sqrt[6]{-c_6})$, et il existe un isomorphisme θ de E sur $E(q)$ défini sur $K(\sqrt[6]{-c_6})$.

D'autre part, d'après (1.1.5), $-\tilde{c}_6$ est un carré dans \tilde{K} , donc $\widetilde{K(\sqrt[6]{-c_6})} = \tilde{K}$. Nous allons montrer , en suivant Ogg ([25] , II), que l'extension $K(\sqrt[6]{-c_6})/K$ est non ramifiée ; cela prouvera que $K(\sqrt[6]{-c_6}) = K$, et que E et $E(q)$ sont K -isomorphes.

Soit ℓ un nombre premier impair différent de p ; notons L l'extension $K(E(q)_\ell)$, et $L' = L(\sqrt[6]{-c_6})$. Nous savons que $L = K(\mu_\ell, q^{1/\ell})$; l'extension $K(\mu_\ell)/K$ est non ramifiée, donc l'indice de ramification de L/K est celui de $K(\mu_\ell, q^{1/\ell})/K(\mu_\ell)$: il est impair (il vaut 1 ou ℓ)



Supposons L' différent de L , et notons σ l'automorphisme non trivial de L' sur L ; le composé $\theta^{-1} \circ \theta^\sigma$ est un automorphisme non trivial de E ; nous avons remarqué que j est non entier, en particulier $j \neq 0$, 1728, donc $\text{Aut}(E) = \pm 1$ et $\theta^{-1} \circ \theta^\sigma = -1$. Soit P un point de $E(q)(L')$, et $\theta(P)$ son image dans $E(L')$; alors $\theta(P) \in E(L)$ si et seulement si $\theta(P)^\sigma = \theta(P)$, c'est-à-dire $\theta^\sigma(P^\sigma) = \theta(P)$, ou encore : $P^\sigma = -P$. Appliquons ceci à un point P d'ordre ℓ de $E(q)$: alors $P \in E(q)(L)$, donc $P^\sigma = +P \neq -P$, et $\theta(P) \notin E(L)$. Ainsi, le groupe $E(L)_\ell = \theta(E(q)(L)_\ell)$ est réduit à 0 . Or, $\widetilde{E(L)}$ est isomorphe à \tilde{L}^* , qui contient μ_ℓ . Ainsi, L' est égal à L , donc $K(\sqrt[6]{-c_6})$ est contenu dans L et l'extension $K(\sqrt[6]{-c_6})/K$ est non ramifiée. Ceci termine la démonstration de la première assertion.

Pour la seconde assertion, lorsque \tilde{E} est à tangentes irrationnelles

sur \tilde{K} , remplaçons K par $K(\sqrt[3]{b_2})$ dans ce qui précède : cela prouve que E et $E(q)$ sont $K(\sqrt[3]{b_2})$ -isomorphes ; et la proposition (1.2.3) prouve que $K(\sqrt[3]{b_2})/K$ est non ramifiée. ■

1.3. GROUPE FORMEL ASSOCIE A UNE CUBIQUE PLANE.

On trouvera dans [10] tous les résultats utilisés ici sur les groupes formels.

1.3.1. Soit E une cubique plane définie sur un corps quelconque K et d'équation (1) : $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$; et posons $z = -\frac{x}{y}$, $w = -\frac{1}{y}$, c'est-à-dire $x = \frac{z}{w}$, $y = -\frac{1}{w}$. Par ce changement de variables, le point à l'infini est amené en $(0,0)$, et comme l'ordre de $\frac{x}{y}$ à l'infini est égal à $(-2) - (-3) = 1$, la variable z est une uniformisante locale pour la cubique au voisinage de l'origine $(z,w) = (0,0)$.

L'équation devient (2) : $w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3$ et permet de calculer le développement de w en série entière de z au voisinage de l'origine : $w = z^3 + a_1z^4 + (a_1^2 + a_2)z^5 + \dots = \sum_{n \geq 3} A_n z^n$ où $A_n \in \mathbb{Z}[a_i]$, A_n étant de "poids" $n-3$ (comme a_i était de "poids" i). Donc $w \in \mathbb{Z}[a_i][[z]]$, $x \in z^{-2}(\mathbb{Z}[a_i][[z]])$, $y \in z^{-3}(\mathbb{Z}[a_i][[z]])$.

Nous venons ainsi de définir, pour toute extension L de K , une application : $P \mapsto z(P) = \frac{-x(P)}{y(P)}$ de $E(L)$ dans L . Cette application admet une application réciproque définie sur l'ensemble des éléments z de L tels que la série $w(z) = \sum_{n \geq 3} A_n z^n$ converge, à savoir : $z \mapsto P(z) = (x(z), y(z))$ où $x(z) = z/w(z)$, $y(z) = -1/w(z)$.

1.3.2. Addition sur E :

PROPOSITION . Il existe une série formelle $F \in \mathbb{Z}[a_i][[Z_1, Z_2]]$ telles que $z(P_1 + P_2) = F(z(P_1) + z(P_2))$ pour tous points P_1 et P_2 de E .

■ Soient 3 points P_1, P_2, P_3 non singuliers alignés sur E , c'est-à-dire tels que $P_1 + P_2 + P_3 = 0$. Notons (z_i, w_i) les coordonnées de P_i ($i = 1, 2, 3$), et calculons formellement z_3 en fonction de z_1 et z_2 .

Le point P_3 est le 3e point d'intersection de la droite $P_1 P_2$ et de la cubique ; l'équation de la cubique est donnée par (2), celle de

$P_1 P_2$ est de la forme : $w = \lambda z + \nu$, où $\lambda = \frac{w_2 - w_1}{z_2 - z_1} = \sum_{n \geq 3} A_n \frac{z_2^n - z_1^n}{z_2 - z_1}$

et $\nu = w_1 - \lambda z_1 = \sum_{n \geq 3} A_n (z_1^n - z_1 \frac{z_2^n - z_1^n}{z_2 - z_1}) = \sum_{n \geq 3} A_n z_1 z_2 \frac{z_2^{n-1} - z_1^{n-1}}{z_2 - z_1}$. En

remplaçant w par $\lambda z + \nu$ dans (2), on obtient une équation du 3e degré en z , dont les racines sont les z_i ($i = 1, 2, 3$), et la "trace" donne :

$$z_1 + z_2 + z_3 = - \frac{a_1 \lambda + a_2 \nu + a_3 \lambda^2 + 2a_4 \lambda \nu + 3a_6 \lambda^2 \nu}{1 + a_2 \lambda + a_4 \lambda^2 + a_6 \lambda^3}$$

où λ et ν sont dans $\mathbb{Z}[a_i][[z_1, z_2]]$, de degré total en z_1 et z_2 : $\deg \lambda \geq 2$, $\deg \nu \geq 3$. Le dénominateur de cette fraction est congru à 1 modulo (z_1, z_2) , donc il est inversible dans $\mathbb{Z}[a_i][[z_1, z_2]]$, d'où la proposition. ■

Remarque : Les propriétés de l'addition sur E font de F une loi de groupe formel à un paramètre.

1.3.3. A la multiplication par n dans E (n entier ≥ 1) correspond la série formelle $\psi_n(Z) \in \mathbb{Z}[a_i][[Z]]$, définie par récurrence : $\psi_1(Z) = Z$, $\psi_{n+1}(Z) = F(Z, \psi_n(Z))$. On a : $\psi_n(z(P)) = z(nP)$.

Rappelons (cf.[10], I.3) que, si K est de caractéristique $p > 0$, il existe un entier $h \geq 1$ tel que $\psi_p(Z) \in \mathbb{F}_p[a_i][[Z^{p^h}]]$. Le plus grand entier h , s'il existe, pour lequel ceci est vérifié est appelé la hauteur du groupe formel F . Si $\psi_p(Z) = 0$, on dit que la hauteur de F est infinie. La valeur de h dépend du type de la courbe E .

PROPOSITION . Si E est une cubique plane définie sur un corps K de caractéristique $p > 0$, et si h désigne la hauteur du groupe formel F , on a le résultat suivant :

- si E est une courbe elliptique non supersingulière, $h = 1$;
- si E est une courbe elliptique supersingulière, $h = 2$;
- si E est une cubique dégénérée de type multiplicatif, $h = 1$;
- si E est une cubique dégénérée de type additif, $h = \infty$.

■ Lorsque E est à mauvaise réduction de type additif, $\tilde{E}_O(\tilde{K}) \simeq \tilde{K}^+$ et la multiplication par p dans $\tilde{E}_O(\tilde{K})$ correspond à la multiplication par p dans \tilde{K} , c'est-à-dire à l'application nulle : $h = \infty$. Lorsque E est à mauvaise réduction de type multiplicatif, la multiplication par p dans $\tilde{E}_O(\tilde{K})$ correspond à $x \mapsto x^p$ dans le groupe multiplicatif correspondant (\tilde{K}^* ou un groupe de normes), et $\psi_p(Z) = Z^p$ est de hauteur 1 . Lorsque E est à bonne réduction, p^h est l'ordre du noyau de la multiplication par p , considérée comme isogénie de E , c'est-à-dire le degré d'inséparabilité de la multiplication par p (cf. II,5.5). ■

Exemple : On calcule facilement $\psi_2(z) = 2z - a_1 z^2 - 2a_2 z^3 + \dots$. Ainsi, si $p = 2$ et si E n'est pas dégénérée, on voit que E est supersingulière si et seulement si a_1 est nul.

2. STRUCTURE DU GROUPE $E(K)$.

2.1. CAS COMPLEXE ET CAS REEL.

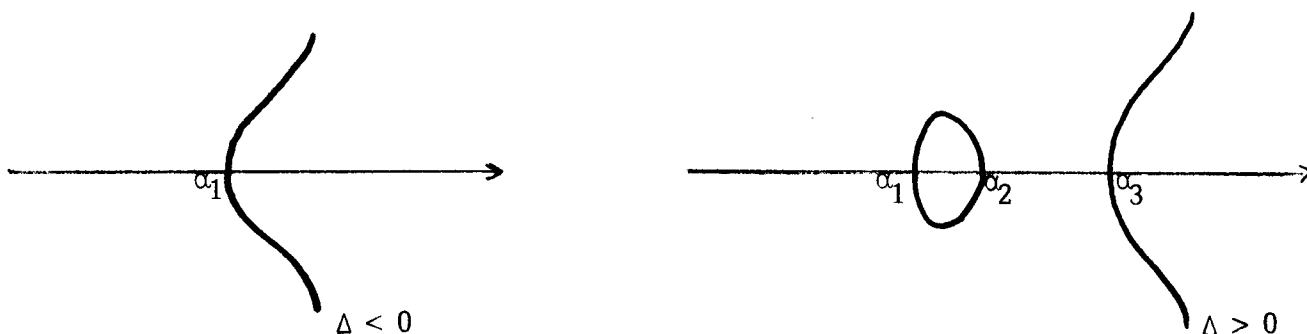
2.1.1. Nous avons vu (I.2.2.5) que $E(\mathbb{C})$ est un tore complexe \mathbb{C}/L , donc le groupe $E(\mathbb{C})$ est isomorphe à $(\mathbb{R}/\mathbb{Z})^2$.

2.1.2. Soit E une courbe elliptique définie sur \mathbb{R} par une équation

de Weierstrass : $y^2 = f(x) = 4x^3 - g_2x - g_3$. Soit Δ le discriminant de E , c'est-à-dire, à un coefficient près, le discriminant du polynôme cubique f (cf. I.1.1.3).

Si $\Delta < 0$, f a une racine réelle ; dans ce cas, $E(\mathbb{R})$ est connexe et isomorphe à \mathbb{R}/\mathbb{Z} .

Si $\Delta > 0$, f a trois racines réelles, $E(\mathbb{R})$ a deux composantes connexes et est isomorphe à $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.



2.2. CAS LOCAL ([47] ,6) .

Soient K un corps local de caractéristique résiduelle p ; $v, \mathcal{O}, \mathfrak{p}, U$, comme ci-dessus ; E une courbe elliptique sur K , définie par une équation minimale de la forme $F(x,y) = 0$, où $F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$.

2.2.1. La réduction $E(K) \longrightarrow \tilde{E}(\tilde{K})$ n'est pas surjective en général, mais si on note $\tilde{E}_{\text{ns}}(\tilde{K})$ le groupe des points non singuliers de $\tilde{E}(\tilde{K})$, et $E_{(0)}(K)$ son image réciproque par la réduction, on a le résultat suivant :

PROPOSITION . La réduction $E_{(0)}(K) \longrightarrow \tilde{E}_{\text{ns}}(\tilde{K})$ est surjective.

■ Soit $(\tilde{r}, \tilde{t}) \in \tilde{E}_{\text{ns}}(\tilde{K})$, c'est-à-dire : soient r, t des éléments de \bar{K} entiers sur \mathcal{O} tels que $F(r,t) \in \mathfrak{p}$, $F'_x(r,t) \notin \mathfrak{p}$ ou $F'_y(r,t) \in U$ (par exemple $F'_y(r,t) \in U$) . Il suffit de montrer qu'il existe $t' \in \bar{K}$ tel que $\tilde{t} = \tilde{t}'$ et $F(r,t') = 0$: c'est le lemme de Hensel (cf.[17] ,II.2). ■

2.2.2. Notons $E_{(1)}(K)$ le noyau de cette réduction, c'est-à-dire $E_{(1)}(K) = \{(x, y) \in E(K) / v(x) \leq -1 \text{ et } v(y) \leq -1\}$.

Remarquons que x et y sont liés par l'équation de E : $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, où les $a_i \in \mathcal{O}$; donc $v(x) < 0$ équivaut à $v(y) < 0$, et alors il existe un entier $n \geq 1$ tel que $v(x) = -2n$, $v(y) = -3n$. Notons, pour tout entier $n \geq 1$, $E_{(n)}(K) = \{(x, y) \in E(K) / v(x) \leq -2n\} = \{(x, y) \in E(K) / v(y) \leq -3n\}$.

Remarque : Pour tout $n \geq 0$, on a $E_{(n)}(K) \supset E_{(n+1)}(K)$. Notons $z = -x/y$ et rappelons x et y sont définis par des séries entières en z , qui convergent si $v(z) > 0$ (cf. 1.3.1); alors

$$E_{(n)}(K) = \{(x, y) \in E(K) / v(z) \geq n\}, \text{ pour tout entier } n \geq 1.$$

2.2.3. La courbe elliptique $E(K)$ est munie d'une structure de groupe. D'autre part, le groupe formel F associé à E permet de définir une structure de groupe sur \mathfrak{P} : si $z_1, z_2 \in \mathfrak{P}$, alors $F(z_1, z_2)$ est une série convergente dans \mathfrak{P} , et si l'on note $z_1 \oplus_F z_2$ sa somme, la loi \oplus_F est une loi de groupe sur \mathfrak{P} .

PROPOSITION . Pour tout $n \geq 1$, $E_{(n)}(K)$ et \mathfrak{P}^n sont des sous-groupes de E et \mathfrak{P} pour les lois définies ci-dessus, et l'application : $(x, y) \longmapsto z = -x/y$ définit un isomorphisme de groupes de $E_{(n)}(K)$ sur \mathfrak{P}^n pour ces lois.

■ Cette proposition est une conséquence du (i) du lemme (2.2.4) ci-dessous. ■

COROLLAIRE . Les groupes $E_{(n)}(K)$ définissent une filtration de $E(K)$

2.2.4. LEMME . Soient $z_1, z_2 \in \mathfrak{P}^n$ et $z_3 \in \mathfrak{P}$ tels que $z_1 \oplus_F z_2 \oplus_F z_3 = 0$. Alors :

- (i) $z_1 + z_2 + z_3 \in \wp^{2n}$ (donc $z_3 \in \wp^n$) ;
- (ii) Si $p \neq 2$, on peut se ramener à $a_1 = a_3 = 0$, et alors
 $z_1 + z_2 + z_3 \in \wp^3$;
- (iii) Si $p \neq 2, 3$, on peut se ramener à $a_1 = a_2 = a_3 = 0$, et alors
 $z_1 + z_2 + z_3 \in \wp^{5n}$;
- (iv) Si $p = 2$ et si E est supersingulière , alors $a_1 = 0$, on
peut se ramener à $a_2 = 0$, et alors $z_1 + z_2 + z_3 \in \wp^{4n}$.

■ Il suffit de regarder l'expression de $F(z_1, z_2)$ donnée en (1.3.2) et, pour (iv) , de se souvenir que, en caractéristique 2, la courbe elliptique E est supersingulière si et seulement si $a_1 = 0$ (cf. 1.4.3). ■

2.2.5. Etude de la filtration. La structure du groupe $E(K)$ est donnée par le résultat suivant :

THEOREME.

- (i) $E_{(1)}(K)$ est un pro-p-groupe ;
- (ii) $E_{(0)}(K)/E_{(1)}(K)$ est isomorphe à $\tilde{E}_{ns}(\tilde{K})$;
- (iii) Si E est à bonne réduction , $E(K) = E_{(0)}(K)$; si la réduction
est de type multiplicatif à tangentes rationnelles , $E(K)/E_{(0)}(K)$
est cyclique d'ordre $v(\Delta)$; sinon , $E(K)/E_{(0)}(K)$ est d'ordre ≤ 4 .

■ (i). D'après le lemme (3.2.4), il existe un entier $a \geq 2$ tel que $E_{(n)}(K)/E_{(an)}(K) \simeq \wp^n/\wp^{an}$ pour tout $n \geq 1$, \wp étant muni de l'addition ordinaire. Donc $E_{(1)}(K)$ est un pro-p-groupe.

(ii) provient des définitions.

(iii). La 1ère assertion est évidente. Démontrons la 2e : d'après (1.2.3), toute courbe elliptique sur K à réduction multiplicative à tangentes rationnelles est isomorphe à une courbe de Tate $E(q)$ ($q \in \wp$) . Donc il suffit de montrer que $E(q)/E_{(0)}(q) \simeq \mathbb{Z}/v(\Delta(q))\mathbb{Z}$ pour tout $q \in \wp$. Or $\tilde{E}(q)$ a pour point singulier $(0,0)$ (cf. 1.3.3) ; $E(q)$ est paramétré

par $K^*/q^{\mathbb{Z}}$ grâce aux formules $X(u)$, $Y(u)$ données en (I.2.5.1), qui convergent lorsque $|q| < |u| \leq 1$, $u \neq 1$; (cette "couronne" forme un système de représentants de $K^*/q^{\mathbb{Z}}$). Ces formules montrent que

$$X(u) \equiv \frac{u}{(1-u)^2} \quad \text{et} \quad Y(u) \equiv \frac{u}{(1-u)^3} \quad (\text{mod. } q\mathcal{O}) .$$

Ainsi, $(X, Y) \in E_{(0)}(q)$ si et seulement si $(\tilde{X}, \tilde{Y}) \neq 0$, c'est-à-dire $|q| < |u| < 1$. D'où $E_{(0)}(q) \simeq Uq^{\mathbb{Z}}/q^{\mathbb{Z}} \simeq U$, et de même

$E_{(n)}(q) \simeq U^{(n)} = 1 + \mathfrak{o}^n$. Enfin, $E(q)/E_{(0)}(q) \simeq K^*/q^{\mathbb{Z}}U \simeq \mathbb{Z}/v(q).\mathbb{Z}'$

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

La dernière assertion (cas de la réduction additive, ou multiplicative à tangentes irrationnelles) est démontrée dans ([47], 6). ■

2.3. APPLICATIONS. (K désigne encore un corps local de caractéristique résiduelle $p > 0$).

2.3.1. PROPOSITION. Si m est premier à p , la réduction :

$E_m(K) \longrightarrow \tilde{E}_m(\tilde{K})$ est injective.

■ Le groupe $E_m(K)$ est d'ordre divisant m^2 (cf. I.4.1.1) alors que $E_{(1)}(K)$ est un pro- p -groupe; donc le noyau de la réduction : $E_m(K) \longrightarrow \tilde{E}_m(\tilde{K})$, qui est égal à $E_m(K) \cap E_{(1)}(K)$, est nul. ■

Remarque : ce résultat a été démontré, par une autre méthode, en (II.6.2.2).

2.3.2. Notons $e = v(p)$ l'indice de ramification absolu de K , et a le plus grand entier tel que $z_1 + z_2 + z_3 \in \mathfrak{o}^{an}$ dès que $z_1 \oplus_F z_2 \oplus_F z_3 = 0$, $z_i \in \mathfrak{o}^n$ (cf. 2.2.4, on sait que $a \geq 2$).

PROPOSITION . S'il existe un point d'ordre p dans $E_{(n)}(K)$ ($n \geq 1$), alors : $e \geq (a-1)n$.

■ Soient : Q un point d'ordre p de $E_{(1)}(K)$, et $n = v(z(Q))$ (i.e. $Q \in E_{(n)}(K) \setminus E_{(n+1)}(K)$). Comme $pQ = 0$, on a :

$$\underbrace{z(Q) \oplus_F z(Q) \oplus_F \dots \oplus_F z(Q)}_{q \text{ fois}} = 0 ;$$

or les groupes $(\mathfrak{p}^n/\mathfrak{p}^{an}, \oplus_F)$ et $(\mathfrak{p}^n/\mathfrak{p}^{an}, +)$ sont isomorphes (cf. 2.2.4), d'où : $p.z(Q) \in \mathfrak{p}^{an}$. Ainsi, $e+n = v(p.z(Q)) \geq an$. ■

2.3.3. *COROLLAIRE 1.* Supposons K absolument non ramifié. Si p est impair, il n'y a pas de torsion dans $E_{(1)}(K)$. Si $p = 2$, les points de torsion éventuels de $E_{(1)}(K)$ sont d'ordre 2, et ne sont pas dans $E_{(2)}(K)$.

■ Puisque $E_{(1)}(K)$ est un pro- p -groupe, tous les points de torsion de $E_{(1)}(K)$ sont d'ordre une puissance de p . Soit Q un point de torsion de $E_{(1)}(K)$; comme $e = 1$, nous avons : $1 \leq v(z(Q)) \leq \frac{1}{a-1}$. Si p est impair, nous savons que $a \geq 3$ (2.2.4), donc $\frac{1}{a-1} < 1$, et un tel point Q ne peut pas exister. Si $p = 2$, nous pouvons avoir $a = 2$, et $v(z(Q)) = 1$, et c'est la seule possibilité. ■

2.3.4. *COROLLAIRE 2.* Supposons que $p = 2$, $e = 1$, et que E est à bonne réduction supersingulière. Soit Q un point d'ordre 2, de $E(\bar{K})$. Alors l'extension $K(Q)/K$ est totalement ramifiée de degré 3.

■ Notons $K' = K(Q)$, et e' l'indice de ramification absolu de K' , c'est-à-dire l'indice de ramification de K'/K . Le point \tilde{Q} est d'ordre 2 dans $\tilde{E}(\tilde{K})$, qui est supersingulière : donc $\tilde{Q} = 0$, et $Q \in E_{(1)}(K')$. Ainsi, $e' \geq a-1$ (cf. 2.3.2); or nous savons qu'ici a est au moins égal à 4 (cf. 2.2.4), donc e' est au moins égal à 3.

D'autre part, le degré de K'/K est au plus égal à 3, car il y a 3 points d'ordre 2 sur $E(\bar{K})$ (d'après I.4.1.1). ■

2.3.5. En fait, le corollaire 2 n'est qu'un cas particulier du résultat suivant :

PROPOSITION . Soit K un corps local de caractéristique résiduelle $p > 0$, d'indice de ramification absolu égal à 1 ; soit E une courbe elliptique sur K , à bonne réduction supersingulière ; soit Q un point d'ordre p de $E(\bar{K})$. Alors l'extension $K(Q)/K$ est totalement ramifiée de degré p^2-1 .

■ Nous verrons en (3.1.5) que, sous ces hypothèses, l'indice de ramification de $K(Q)/K$ est égal à p^2-1 . D'autre part, il y a (p^2-1) points d'ordre p sur $E(\bar{K})$ (cf. I,4.1.1) , donc le degré de l'extension $K(Q)/K$ est au plus égal à p^2-1 . ■

2.4. CAS RATIONNEL.

Soit E une courbe elliptique sur \mathbb{Q} , de discriminant Δ .

2.4.1. *THEOREME* (Mordell-Weil) : Le groupe $E(\mathbb{Q})$ est de type fini.

Ce théorème a été prouvé par Mordell en 1922, puis généralisé par Weil. On en trouve une démonstration dans [5] (théorème 20.1).

2.4.2. L'étude du cas local (cf. 2.2 et 2.3) donne le résultat suivant sur la torsion de $E(\mathbb{Q})$:

PROPOSITION . Si p_1, p_2, \dots, p_r désignent les facteurs premiers de Δ , tout point de torsion de $E(\mathbb{Q})$ est à coordonnées dans
 $\mathbb{Z}[\frac{1}{2}, \frac{1}{p_1}, \frac{1}{p_2}, \dots, \frac{1}{p_r}]$.

■ Soit Q un point de torsion de $E(\mathbb{Q})$; supposons que figure, au dénominateur d'une des coordonnées de Q , un nombre premier p ne divisant pas Δ .

Alors le point Q , considéré comme point de $E(\mathbb{Q}_p) = E_{(0)}(\mathbb{Q}_p)$, est dans le noyau $E_{(1)}(\mathbb{Q}_p)$ de la réduction modulo p . D'après (2.3.3), ce n'est possible que si $p = 2$. ■

Rappelons un résultat démontré en (I.4.4.3) :

PROPOSITION 1. Le groupe de torsion de $E(\mathbb{Q})$ est cyclique, ou égal au produit de $\mathbb{Z}/2\mathbb{Z}$ par un groupe cyclique.

2.4.3. La série L d'une courbe elliptique.

Nous avons associé à toute courbe projective X non singulière sur \mathbb{F}_p une série L (cf. II.7.3.2), définie par :

$$L_X(u) = \prod_{i=1}^{2g} (1 - \alpha_i u)^{-1} ;$$

dans cette formule, u est une variable complexe, g le genre de X , et $\alpha_1, \dots, \alpha_{2g}$ les valeurs propres de l'endomorphisme de Frobenius π_p sur le module de Tate $T_\ell(J(X))$ (ℓ premier différent de p), numérotées de façon que $\alpha_i \cdot \alpha_{i+g} = p$.

En particulier, si $X = \tilde{E}^{(p)}$ est la réduction modulo p de E (où p ne divise pas Δ),

$$L_{\tilde{E}^{(p)}}(p^{-s}) = \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

où $a_p = \alpha_1 + \alpha_2$ est la trace de π_p ; comme $|\alpha_1| = |\alpha_2| = \sqrt{p}$, on a $|a_p| \leq 2\sqrt{p}$.

Lorsque p divise Δ , posons $a_p = \left(\frac{-c_6}{p}\right)$; autrement dit, $a_p = +1, -1$ ou 0 , selon que la cubique dégénérée $\tilde{E}^{(p)}$ est de type multiplicatif à tangentes rationnelles, multiplicatif à tangentes irrationnelles, ou additif (cf. 1.1.5).

Définissons maintenant la série L de E par le produit eulérien suivant (qui converge pour $\text{Re } s > 3/2$) :

$$L_E(p^{-s}) = \prod_{p|\Delta} \frac{1}{(1 - a_p p^{-s})} \prod_{p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} .$$

Définissons aussi la fonction Λ_E par :

$$\Lambda_E(s) = N^{s/2} (2\pi)^{-s} \Gamma(s) L_E(p^{-s})$$

où N désigne le conducteur (algébrique) de E , défini en (1.1.6).

2.4.4. Conjectures. Nous énonçons ici quelques conjectures "classiques" sur les courbes elliptiques semi-stables définies sur \mathbb{Q} (cf.[47]). Nous supposons donc N sans facteur carré, et utilisons les notations de (2.4.3). Définissons a_n pour tout entier $n \geq 1$, à partir des a_p , par : $a_1 = 1$, $a_{nm} = a_n a_m$ si $(n, m) = 1$, et $a_p a_{p^r} = a_{p^{r+1}} + p a_{p^{r-1}}$ si $r \geq 1$. Rappelons que $\text{Dif}_O(E)$ est de dimension 1, et notons ω une forme différentielle holomorphe non nulle sur E .

Conjecture 1 : La série L de E admet un prolongement analytique holomorphe dans \mathbb{C} , et vérifie une équation fonctionnelle du type :

$$\Lambda_E(2-s) = w \Lambda_E(s), \text{ où } w = \pm 1.$$

Soit ρ l'ordre du zéro de L en $s = 1$; cette conjecture a pour conséquence : $(-1)^\rho = w$.

Conjecture 2 (Weil) : La fonction f , définie sur \mathbb{H} par

$$f(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i n \tau}, \text{ est une forme parabolique primitive de poids 2 pour}$$

$\Gamma_O(N)$; c'est une fonction propre pour tous les opérateurs de Hecke, donc

pour l'opérateur d'Atkin Lehner $W_N = \prod_{p|N} W_p^N$, et la valeur propre de

W_N associée à f est égale à $-w$. Enfin, il existe une application

rationnelle $\varphi : X_O(N) \rightarrow E$, définie sur \mathbb{Q} , telle que les formes différentielles $\omega \circ \varphi$ et $f(\tau)d\tau$ (sur $X_O(N)$) sont proportionnelles.

Rappelons que, d'après le théorème (II,2.3.1), a_n est la valeur propre de T_n associée à f . En particulier, lorsque p divise N , sur les formes nouvelles, $T_p = -W_p^N$ est une involution, ayant pour valeur propre $a_p = \left(\frac{-c_6}{p}\right) = \pm 1$. La conjecture de Weil affirme donc que

$$-w = \prod_{p|N} (-a_p) = \prod_{p|N} \left[-\left(\frac{-c_6}{p}\right) \right].$$

Notons t le nombre de facteurs premiers de N , et $\left(\frac{-c_6}{N}\right)$ le produit $\prod_{p|N} \left(\frac{-c_6}{p}\right)$; alors

$$w = (-1)^{t+1} \left(\frac{-c_6}{N}\right).$$

Conjecture 3 (Birch et Swinnerton-Dyer) (en admettant le prolongement analytique de L) : L'ordre du zéro de $L(p^{-s})$ au point $s = 1$ est égal au rang r du groupe $E(\mathbb{Q})$.

Ainsi, l'ensemble de ces trois conjectures implique :

Conjecture 4 : Le rang r du groupe $E(\mathbb{Q})$ est lié au nombre t de facteurs premiers de N par $(-1)^r = (-1)^{t+1} \left(\frac{-c_6}{N}\right)$.

2.4.5. Remarque : Lorsque E est une courbe elliptique à multiplication complexe, la série L de E se prolonge analytiquement à tout le plan complexe, comme l'a montré Deuring [7a] . Dans ce cas, Coates et Wiles [6c] viennent de démontrer une partie de la conjecture de Birch et Swinnerton-Dyer, à savoir :

THEOREME. Si E est une courbe elliptique à multiplication complexe définie sur \mathbb{Q} , et si le rang du groupe $E(\mathbb{Q})$ est au moins égal à 1 , alors $L(p^{-s})$ s'annule au point $s = 1$.

3. PROPRIETES GALOISIENNES DES POINTS D'ORDRE FINI SUR UNE COURBE ELLIPTIQUE [39] .

3.1. ETUDE LOCALE.

3.1.1. Soient K une extension finie de \mathbb{Q}_p ; v, ρ, \mathcal{O}, U comme précédemment (1.1.5) ; E une courbe elliptique sur K ; ℓ un nombre premier ; notons $L = K(E_\ell)$, v_L , ρ_L , \mathcal{O}_L ; U_L . Le groupe E_ℓ des points d'ordre ℓ de E est isomorphe à $(\mathbb{Z}/\ell\mathbb{Z})^2$, puisque K est de caractéristique nulle (I.4.1.1) et la réduction modulo ρ induit un homomorphisme surjectif de E_ℓ sur \tilde{E}_ℓ (II.6.2.1) . Notons η_ℓ le noyau. Il est contenu dans $E_{(1)}(L)$ (défini en 2.2.2) , dont la loi de groupe est définie par le groupe formel F associé à E (1.3.) ; on a même exactement :

$$\eta_{\ell} = \{z \in \mathcal{O}_L / \psi_{\ell}(z) = 0\}.$$

Lorsque la hauteur h de F est finie, l'ordre de \tilde{E}_p est égal à p^{2-h} puisque c'est le degré de séparabilité de la multiplication par p dans \tilde{E} ; donc l'ordre de η_p est p^h .

Soit G l'image de $\text{Gal}(\bar{K}/K)$ dans $\text{Aut}(E_{\ell})$, c'est-à-dire $G = \text{Gal}(K(E_{\ell})/K) = \text{Gal}(L/K)$. La suite exacte

$$0 \longrightarrow \eta_{\ell} \longrightarrow \tilde{E}_{\ell} \longrightarrow 0$$

est en fait une suite exacte de G -modules.

Suivant [39], nous allons étudier l'image I du groupe d'inertie de \bar{K}/K , dans $\text{Aut}(E_{\ell})$, c'est-à-dire le groupe d'inertie de L/K . Son action sur \tilde{E}_{ℓ} est triviale, et il laisse η_{ℓ} stable.

Nous allons donc étudier la ramification de L/K selon le type de réduction de E , à l'exception de la réduction additive.

Soit $e = v(p)$ l'indice de ramification absolu de K . Nous supposons que $e = 1$.

3.1.2. PROPOSITION. Si E a bonne réduction modulo \mathfrak{P} et si $\ell \neq p$, alors $I = \{1\}$.

■ D'après (II.6.2.2), la réduction modulo \mathfrak{P} induit un isomorphisme de E_{ℓ} sur \tilde{E}_{ℓ} . ■

3.1.3. PROPOSITION. Si E a mauvaise réduction de type multiplicatif modulo \mathfrak{P} , alors 2 cas sont possibles :

- (i) Si $\Delta \in K^{*\ell}$, I est trivial si $\ell \neq p$; d'ordre $(p-1)$ si $\ell = p$, représentable par $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$.
- (ii) Si $\Delta \notin K^{*\ell}$, I est d'ordre ℓ si $\ell \neq p$, représentable par $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$; d'ordre $p(p-1)$ si $\ell = p$, représentable par $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$.

■ Dans ce cas, \tilde{E}_{ℓ} est isomorphe à un sous-groupe de L^* , il est donc cyclique d'ordre ℓ , donc η_{ℓ} aussi. Quitte à remplacer K

par une extension non ramifiée, on peut supposer que E est une courbe de Tate sur K (cf. 1.2.3), c'est-à-dire $E(K) \simeq K^*/q^{\mathbb{Z}}$, $q \in \mathfrak{P}$. Alors $K(\eta_\ell) = K(\mu_\ell)$ est une extension de K non ramifiée si $\ell \neq p$, totalement ramifiée de degré $p-1$ si $\ell = p$. Donc $\{\zeta_\ell, q^{1/\ell}\}$ forme une base de E_ℓ sur \mathbb{F}_ℓ (si ζ_ℓ est une racine primitive ℓ ème de l'unité, et $q^{1/\ell}$ une racine ℓ ème quelconque de q). Ainsi $K(E_\ell) = K(\zeta_\ell, q^{1/\ell})$. Nous venons de rappeler la ramification de $K(\zeta_\ell)/K$; d'autre part, $K(\zeta_\ell, q^{1/\ell})/K(\zeta_\ell)$ est de degré 1 si $q \in K^{*\ell}$, de degré ℓ , totalement ramifiée, sinon. Et comme $\Delta = q \prod_{n \geq 1} (1-q^n)^{24}$, on a : $q \in K^{*\ell}$ si et seulement si $\Delta \in K^{*\ell}$. Enfin, les représentations matricielles sont données par rapport à la base $\{\zeta_\ell, q^{1/\ell}\}$ de E_ℓ . ■

3.1.4. *PROPOSITION.* Si E est à bonne réduction non supersingulière modulo \mathfrak{P} , et si $\ell = p$, alors I est représentable par un sous-groupe du groupe $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$.

■ Puisque $\dim_{\mathbb{F}_p}(\tilde{E}_p) = 2-h = 1$, dans une base de E_p associée à la suite exacte $0 \rightarrow \eta_p \rightarrow E_p \rightarrow \tilde{E}_p \rightarrow 0$, tout élément de I est représenté par une matrice de la forme $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$. ■

3.1.5. *PROPOSITION.* Si E a bonne réduction supersingulière modulo \mathfrak{P} , et si $\ell = p$, alors I est cyclique d'ordre p^2-1 .

■ Ici $h = 2$ donc $\tilde{E}_p = \{0\}$ et $E_p \simeq \eta_p \simeq \{z \in \mathbb{F}_L / \psi_p(z) = 0\}$. Or $\psi_p(z) = p(z + \alpha_2 z^2 + \dots + \alpha_{p^2-1} z^{p^2-1}) + \alpha_{p^2} z^{p^2} + \dots$ où $\alpha_i \in \mathcal{O}$, $\alpha_{p^2} \notin \mathfrak{P}$. D'après le théorème de préparation de Weierstrass (cf. [10], I.1) il existe une série formelle inversible $u(Z) \in \mathcal{O}[[Z]]$ et un polynôme $g(Z) = p(\beta_1 Z + \beta_2 Z^2 + \dots + \beta_{p^2-1} Z^{p^2-1}) + \beta_{p^2} Z^{p^2} \in \mathcal{O}[Z]$ tels que $\beta_{p^2} \notin \mathfrak{P}$ et $\psi_p(Z) = u(Z).g(Z)$. Ainsi, $\psi_p(z) = 0$ si et seulement si $g(z) = 0$; or $g(z)$ est le produit de z par un polynôme d'Eisenstein de degré p^2-1 .

Ainsi, pour tout élément P non nul de E_p , l'extension $K(P)/K$ est totalement ramifiée de degré p^2-1 . Cela prouve que l'ordre de I est multiple de p^2-1 .

Mais d'autre part, I est un sous-groupe de $\text{Aut}(E_p) \simeq \text{GL}_2(\mathbb{F}_p)$, et ce dernier groupe est d'ordre $p(p^2-1)(p-1)$. Soit I_1 le p -sous-groupe de I . On sait [36] que I_1 est un sous-groupe distingué de I , et que I/I_1 est cyclique d'ordre premier à p . Si I_1 était d'ordre p , c'est-à-dire représentable par $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ dans $\text{GL}_2(\mathbb{F}_\ell)$, I devrait être contenu dans le normalisateur $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ de I_1 ; or, ce normalisateur est d'ordre $p(p-1)^2$. Comme p^2-1 ne divise pas $p(p-1)^2$, c'est impossible, et $I_1 = \{1\}$. Mais tout sous-groupe cyclique de $\text{GL}_2(\mathbb{F}_p)$ d'ordre premier à p est contenu dans un "sous-groupe de Cartan" de $\text{GL}_2(\mathbb{F}_p)$ (cf. [39], 2.6) donc d'ordre $(p-1)^2$ ou (p^2-1) (cf. [39], 2.1). Ainsi I est cyclique d'ordre p^2-1 . ■

3.2. COURBE ELLIPTIQUE SEMI-STABLE SUR \mathbb{Q} .

Soit E une courbe définie sur \mathbb{Q} , semi-stable, définie par une équation minimale. Alors le conducteur N de E est égal à : $N = \prod_{p|\Delta} p$ (cf. 1.1.6).

Soient ℓ un nombre premier, et G l'image de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ dans $\text{Aut}(E_\ell)$, c'est-à-dire $G = \text{Gal}(\mathbb{Q}(E_\ell)/\mathbb{Q})$. Notons v_p la valuation normalisée de \mathbb{Q}_p .

3.2.1. LEMME. S'il existe p divisant Δ tel que ℓ ne divise pas $v_p(\Delta)$, alors : ou bien $G = \text{GL}_2(\mathbb{F}_\ell)$, ou bien G est contenu dans l'ensemble des matrices de la forme $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ et E contient un sous-groupe cyclique d'ordre ℓ rationnel sur \mathbb{Q} .

■ Puisque $p|\Delta$, E est à réduction multiplicative mod. p . L'hypothèse $\ell \nmid v_p(\Delta)$ équivaut à $\Delta \notin \mathbb{Q}_p^{*\ell}$. La proposition (2.1.3) prouve que le groupe d'inertie de $\mathbb{Q}_p(E_\ell)/\mathbb{Q}_p$ est d'ordre $\ell(\ell-1)$: il contient

donc un élément d'ordre ℓ , et G aussi contient un élément σ d'ordre ℓ . Dans une base $\{e_1, e_2\}$ convenable de E_ℓ sur \mathbb{F}_ℓ , σ est représenté par $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Deux cas sont alors possibles (et incompatibles !) :

Ou bien G laisse fixe la droite $\mathbb{F}_\ell e_1$, et alors G est un sous-groupe du groupe d'ordre $\ell(\ell-1)^2$ représenté dans la base $\{e_1, e_2\}$ par $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$.

Ou bien G contient un élément g tel que $ge_1 = e'_2 \notin \mathbb{F}_\ell e_1$. Dans la base $\{e_1, e'_2\}$ de E_ℓ , la matrice de σ est $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ avec $a \neq 0$, et celle de $\tau = g\sigma g^{-1}$ est $\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$ avec $b \neq 0$, puisque $\tau e'_2 = e'_2$. Ainsi G contient toutes les matrices $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$; mais $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, donc G contient le sous-groupe de $GL_2(\mathbb{F}_\ell)$ engendré par $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Ce sous-groupe est $SL_2(\mathbb{F}_\ell)$: en effet, c'est l'image, par la projection canonique de $GL_2(\mathbb{Z})$ sur $GL_2(\mathbb{F}_\ell)$, du sous-groupe de $GL_2(\mathbb{Z})$ engendré par $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, à savoir $\Gamma = SL_2(\mathbb{Z})$. Or $SL_2(\mathbb{F}_\ell)$ est le noyau du déterminant, autrement dit on a la suite exacte :

$$1 \longrightarrow SL_2(\mathbb{F}_\ell) \longrightarrow GL_2(\mathbb{F}_\ell) \xrightarrow{\det} \mathbb{F}_\ell^* \longrightarrow 1.$$

Comme l'accouplement de Weil (I.4.4) nous a montré que $\det(G) = \mathbb{F}_\ell^*$, on a alors $G = GL_2(\mathbb{F}_\ell)$. ■

3.2.2. THEOREME. Si ℓ ne divise pas $v_p(\Delta)$, pour un p divisant Δ , alors :

- (i) ou bien $G = GL_2(\mathbb{F}_\ell)$;
- (ii) ou bien E a un point rationnel d'ordre ℓ ;
- (iii) ou bien E est ℓ -isogène (sur \mathbb{Q}) à une courbe E' ayant un point rationnel d'ordre ℓ .

(ici, "point rationnel" signifie "point rationnel sur \mathbb{Q} ").

■ Vu le lemme (3.2.1), il suffit de montrer que, si $G \subset \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$, on est dans le cas (ii) ou (iii). Notons χ_i ($i = 1, 2$) les 2 homomorphis-

mes de G dans \mathbb{F}_ℓ^* définis par : $g = \begin{pmatrix} \chi_1(g) & * \\ 0 & \chi_2(g) \end{pmatrix}$. Nous allons montrer que l'un des χ_i est égal à 1, et alors le second sera égal au déterminant, donc à la restriction du caractère χ de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ défini par l'action sur μ_ℓ .

Appelons K_i le sous-corps de $\mathbb{Q}(E_\ell)$ fixe par le noyau de χ_i , et étudions la ramification de K_i/\mathbb{Q} en chaque place p . Remarquons d'abord que le degré $[K_i:\mathbb{Q}]$ divise $\ell-1$.

Si $p \nmid \ell\Delta$, d'après (2.1.2) l'extension $\mathbb{Q}_p(E_\ell)/\mathbb{Q}_p$ est non ramifiée, donc a fortiori K_i/\mathbb{Q} est non ramifiée en p .

Si $p \mid \Delta$ et $p \neq \ell$, comme $\Delta \notin \mathbb{Q}_p^{*\ell}$ par hypothèse, le groupe d'inertie de $\mathbb{Q}_p(E_\ell)/\mathbb{Q}_p$ est d'ordre ℓ d'après (3.1.3, (ii)). Ainsi l'indice de ramification de K_i/\mathbb{Q} en p doit diviser ℓ et $\ell-1$ (car $[K_i:\mathbb{Q}]$ divise $\ell-1$) : l'extension K_i/\mathbb{Q} est non ramifiée en p .

Si $p = \ell$, la réduction n'est pas supersingulière : en effet, d'après (3.1.5), si c'était le cas, le groupe d'inertie de $\mathbb{Q}(E_\ell)/\mathbb{Q}$ serait d'ordre ℓ^2-1 . Mais cet ordre doit diviser l'ordre de G , qui lui-même divise $\ell(\ell-1)^2$: c'est impossible. Ainsi la réduction est non supersingulière, ou de type multiplicatif, et d'après (3.1.3) et (3.1.4), le groupe d'inertie de $\mathbb{Q}_p(E_\ell)/\mathbb{Q}_p$ est d'ordre divisant $\ell(\ell-1)$ (car représentable par un sous-groupe de $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$) : donc l'un des caractères χ_i correspondant à 1 - est non ramifié en ℓ .

En résumé, l'un des χ_i est non ramifié partout, l'autre est non ramifié en dehors de ℓ . Comme il n'existe pas d'extension non triviale de \mathbb{Q} partout non ramifiée, l'un des χ_i est le caractère unité, et alors l'autre est le déterminant. Nous avons donc 2 cas à considérer :

Si $\chi_1 = 1$, alors $G \subset \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\}$ et le 1er vecteur de la base correspond à un point d'ordre ℓ défini sur \mathbb{Q} .

Si $\chi_2 = 1$, alors $G \subset \left\{ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \right\}$ et on a une suite exacte de G -

modules : $1 \longrightarrow \mu_\ell \longrightarrow E_\ell \longrightarrow \mathbb{Z}/\ell\mathbb{Z} \longrightarrow 1$, où l'action de G sur $\mathbb{Z}/\ell\mathbb{Z}$ est triviale. D'après (I.4.3.3), la courbe elliptique E/μ_ℓ est ℓ -isogène à E , définie sur \mathbb{Q} , et le sous-groupe E_ℓ/μ_ℓ de E/μ_ℓ est d'ordre ℓ et rationnel sur \mathbb{Q} . ■

3.2.3. COROLLAIRE. Si E est une courbe elliptique semi-stable sur \mathbb{Q} ayant bonne réduction en 2 , si $\ell > 5$ et s'il existe un facteur premier p de Δ tel que ℓ ne divise pas $v_p(\Delta)$, alors $\text{Gal}(\mathbb{Q}(E_\ell)/\mathbb{Q}) = \text{Aut}(E_\ell)$.

■ Il suffit de vérifier que les cas (ii) et (iii) du théorème (3.2.2) ne peuvent pas se produire, donc que $G = \text{GL}_2(\mathbb{F}_\ell)$. Or si E avait un point rationnel d'ordre ℓ , la courbe réduite modulo 2 aurait un sous-groupe de points rationnels sur \mathbb{F}_2 d'ordre ℓ (cf. 3.3.1) (car $\ell \neq 2$). Comme $\mathbb{P}_2(\mathbb{F}_2)$ a 5 points, cela implique $\ell \leq 5$. Ainsi, (ii) est impossible. Et le lemme ci-dessous (3.2.4) montre que toute courbe ℓ -isogène à E a bonne réduction en 2 : ainsi (iii) est impossible comme (ii) . ■

3.2.4. LEMME. Deux courbes elliptiques définies sur un même corps de nombres K , et isogènes sur K , ont exactement les mêmes places de mauvaise réduction.

Ce résultat est démontré dans [41] pour des variétés abéliennes.

3.2.5. Remarque : Dans [39] , Serre obtient le résultat plus général suivant :

THEOREME. Soient K un corps de nombres, et E une courbe elliptique sur K n'ayant pas de multiplication complexe sur \bar{K} . Alors, pour presque tout nombre premier ℓ (i.e. pour tout ℓ sauf un nombre fini), on a : $\text{Gal}(K(E_\ell)/K) = \text{Aut}(E_\ell)$.