N° d'ordre : 09/2006-M/MT
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE

FACULTE DE MATHEMATIQUES

MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

En : MATHEMATIQUES

Spécialité : Algèbre et Théorie des Nombres

Par : AIT-AMRANE LYES

THEME

5 ET 7 DESCENTE SUR LES COURBES ELLIPTIQUES DEFINIES SUR Q

Soutenu publiquement le:21/ 09/ 2006, devant le jury composé de:

M. A. KESSI	***Professeur, U.S.T.H.B***	***Président***
M. K. BETINA	***Professeur, U.S.T.H.B***	***Directeur de Mémoire***
M. A. DERBAL	***Maître de Conférences, E.N.S***	***Examinateur***
M. D. BEHLOUL	***Chargé de Cours, U.S.T.H.B***	***Examinateur***

Remerciements

Je tiens à remercier mon directeur de thèse le Professeur Kamel Betina de m’avoir soutenu durant tous les moments difficiles et de m’avoir aider et diriger pour finaliser ce mémoire.

Je remercie aussi Mr Areski Kessi Professeur à l’U.S.T.H.B d’avoir accepter d’être président du jury.

Finalement je remercie Mr Djilali Behloul chargé de cours à l’U.S.T.H.B et Mr Abdelah Derbal maître de conférence à l’E.N.S de me faire l’honneur de participer au jury.

Table des matières

Chapitre 1

Introduction

Soit E une courbe elliptique définie sur un corps de nombres K. Le théorème de Mordell-Weil nous dit que le groupe $E(K)$ des points K-rationnels de E est un groupe abélien de type fini. On appelle $E(K)$ le groupe de Mordell-Weil. Un autre groupe important associé à E est le groupe de Tate-Shafarevich $\text{Ш}(E/K)$. C'est l'ensemble des torseurs de E qui ont des points partout localement. Donc un élément non nul du groupe de Tate-Shafarevich correspond à une courbe lisse de genre 1 qui ne respecte pas le principe de Hasse , *i.e.* elle a des points partout localement, mais elle n'a pas de point globalement.

Il n'y a aucun algorithme qui nous permet de calculer les groupes de Mordell-Weil et de Tate-Shafarevich. Mais, pour un entier $n \geq 2$ la preuve du théorème de Mordell-Weil nous donne une borne supérieure de l'ordre de $E(K)/nE(K)$, d'où l'on déduit une borne supérieure du rang de Mordell-Weil. On appelle ces calculs les calculs de descente. En appliquant une n-descente on obtient des informations partielles sur les groupes $E(K)$ et $\text{Ш}(E/K)$.

Beaucoup de travail a été fait dans le cas des 2 et 3 descentes. On donne quelques exemples de 5 et 7 descente, mais on travaille dans un cas spécial, et donc on ne peut pas appliquer nos résultas à n'importe quelle courbe elliptique. D'abord, nos calculs de descente supposent l'existence d'une isogénie de degré $n = 5$ ou 7. Ensuite, on suppose qu'une courbe de notre paire de courbes elliptiques isogènes admet un point rationnel d'ordre n.

On considère donc des paires de courbes elliptiques C et D définies sur K, liées par les suites exactes de modules de Galois

$$0 \to \mu_n \to C \xrightarrow{\phi} D \to 0 \qquad et \qquad 0 \to \mathbf{Z}/n\mathbf{Z} \to D \xrightarrow{\widehat{\phi}} C \to 0. \tag{1.1}$$

En d'autres termes $\phi : C \to D$ est une isogénie de degré n dont le noyau est isomorphe à μ_n (le groupe des racines n^{emes} de l'unité). L'accouplement de Weil nous

dit que le noyau de l'isogénie dual $\widehat{\phi} : D \to C$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$. On estime le rang de Mordell-Weil en bornant les groupes $D(K)/\phi C(K)$ et $C(K)/\widehat{\phi}D(K)$.

Ce procédé est connu sous le nom de descente via n-isogénie.

Chapitre 2

Généralités

2.1 Courbes elliptiques

2.1.1 Equation de Weierstrass

2.1.1.1 Définition

Une courbe elliptique est une paire (E,O), où E est une courbe lisse de genre 1 et $O \in E$. (Dans la suite, on écrira E au lieu de (E,O)). La courbe elliptique E est définie sur K, et on écrit E/K, si E est définie sur K comme courbe et $O \in E(K)$.

2.1.1.2 Proposition

Soit E une courbe elliptique définie sur K.

1. Il existe des fonctions $x,y \in K(E)$ telles que l'application

$$\phi : E \to \mathbf{P}^2 \qquad P \mapsto [x(P) : y(P) : 1]$$

induit un isomorphisme entre E/K et une courbe projective (lisse) C donnée par une équation

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

avec les coefficients $a_1,...,a_6 \in K$ et tel que $\phi(O) = [0 : 1 : 0]$. L'équation précedente est appelée équation de Weierstrass de la courbe C.

2. Deux équations de Weierstrass de E comme dans 1. sont liées par un changement de variables linéaire de la forme

$$x = u^2x' + r$$

$$y = u^3y' + su^2x' + t$$

avec u,r,s,$t \in K$ et $u \neq 0$.

3. Inversement, toute cubique lisse C donnée par une équation de Weierstrass est une courbe elliptique définie sur Kavec le point origine $O = [0 : 1 : 0]$.

Preuve. voir [14] chapitre III proposition 3.1.

Pour simpilfier les notations, on va écrire l'équation de Weierstrass de notre courbe elliptique en utilisant les coordonnées affines $x = \frac{X}{Z}$ **et** $y = \frac{Y}{Z}$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

Si la caractéristique de $K \neq 2$, alors on peut simplifier l'équation (2.1) en remplaçant y par $\frac{1}{2}(y - a_1x - a_3)$, ce qui donne l'équation

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

où

$$\begin{cases} b_2 = a_1^2 + 4a_2, \\ b_4 = 2a_4 + a_1a_3, \\ b_6 = a_3^2 + 4a_6. \end{cases}$$

On définit aussi les quantités

$$\begin{cases} b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 = \dfrac{b_2b_6 - b_4^2}{4}, \\ c_4 = b_2^2 - 24b_4, \\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = \dfrac{c_4^3 - c_6^2}{1728}, \\ j = {c_4}^3/\Delta, \end{cases}$$

où la quantité Δ s'appelle le discriminant de l'équation de Weierstrass (2.1), et j s'appelle le j-invariant de la courbe elliptique E. Si de plus la caractéristique de $K \neq 2,3$ on peut remplacer (x,y) par $((x-3b_2)/36, y/108)$ dans l'équation précédente, ce qui nous donne une nouvelle équation sans le terme x^2

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

Soit $P_0 = (x_0,y_0)$ un point appartenant à une courbe E/K donnée par l'équation

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

on dit que E est lisse au point P_0 si on a $(\frac{\partial f}{\partial x}(P_0), \frac{\partial f}{\partial y}(P_0)) \neq (0,0)$, et on dit qu'elle est lisse si elle est lisse en tout point, dans ce cas E/K est une courbe elliptique.

Si E/K admet un point singulier S, alors ce point est soit un noeud de la courbe (point à deux tangentes distinctes dites rationnelles si leurs équations sont à coefficient dans K), soit un point de rebroussement (point à deux tangentes confondues).

2.1.1.3 Proposition

Une courbe E/K donnée par une équation de Weierstrass (2.1), de discriminant Δ et de coefficient associé c_4 est classifiée comme suit

1. Elle est lisse si et seulement si $\Delta \neq 0$.

2. Elle admet un noeud si et seulement si $\Delta = 0$ et $c_4 \neq 0$.

3. Elle admet un point de rebroussement si et seulement si $\Delta = c_4 = 0$.

Preuve. voir [14] chapitre III proposition 1.4.

2.1.2 Structure de groupe abélien sur une courbe elliptique

Soit E/K une courbe elliptique donnée par une équation de Weierstrass

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad a_i \in K.$$

Alors la courbe E admet une structure de groupe abélien d'élément neutre le point origine $O = [0 : 1 : 0]$. La loi de composition du groupe abélien

$$E(\overline{K}) = \{(x,y) \in \overline{K} \times \overline{K} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

est définie par la propriété de trois points colinéaires P_i de la courbe E d'avoir une somme égale à O. En d'autres termes:

$$P_1 + P_2 + P_3 = O$$

le symétrique $-P$ d'un point $P = (x,y) \in E(\overline{K})$ est le point

$$-P = (x, -y - a_1x - a_3)$$

La somme $P_1 + P_2 = P_3$ où $P_i = (x_i,y_i) \in E(\overline{K})$ est donnée par les formules

$$\begin{cases} x_3 = \kappa^2 + a_1\kappa - a_2 - x_1 - x_2 \\ \\ y_3 = -(\kappa + a_1)x_3 - \nu - a_3 \end{cases}$$

où

$$\begin{cases} \kappa = \dfrac{y_2 - y_1}{x_2 - x_1} & \nu = \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1} & \text{si } x_1 \neq x_2 \\ \\ \kappa = \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \nu = \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} & \text{si } x_1 = x_2 \end{cases}$$

(donc $y = \kappa x + \nu$ est la droite passant par P_1 et P_2 si $P_1 \neq P_2$, ou la tangente à E en P_1 si $P_1 = P_2$).

Si $P = (x,y) \in E(\overline{K})$ est un point tel que $2P \neq O$, Alors on a la formule de duplication

$$x(2P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}.$$

L'ensemble des points

$$E(K) = \{(x,y) \in K \times K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

est un sous-groupe du groupe abélien $E(\overline{K})$ appelé le groupe des points rationnels de la courbe elliptique E définie sur K.

Si K est un corps de nombres, alors $E(K)$ est appelé le groupe de Mordell-Weil de la courbe elliptique E. La structure de ce groupe est déterminé par les résultats suivants:

2.1.2.1 Théorème

Soit K un corps de nombres, E une courbe elliptique définie sur K, $m \geq 2$ un entier rationnel, $E(K)$ le groupe des points rationnels de E et $mE(K)$ le sous groupe des points mP, $P \in E(K)$. Alors le groupe quotient $E(K)/mE(K)$ est fini.

Preuve. voir [14] chapitre VIII théorème 1.1.

2.1.2.2 Théorème

Soit K un corps de nombres et E/K une courbe elliptique. Alors le groupe abélien $E(K)$ des points rationnels de E est de type fini.

Preuve. voir [14] chapitre VIII théorème 6.7.

2.1.2.3 Corollaire

Soit K un corps de nombres, E/K une courbe elliptique, $E(K)$ le groupe des points rationnels de E et $E_{tors}(K)$ son sous groupe de torsion. Alors il existe un isomorphisme de groupes:

$$E(K) \cong E_{tors}(K) \times \mathbf{Z}^r.$$

L'entier r est appelé le rang de Mordell-Weil.

2.1.3 Isogénies

2.1.3.1 Définition

On dit que deux courbes elliptiques E_1 et E_2 sont isogènes s'il existe un morphisme

$$\phi : E_1 \to E_2$$

tel que $\phi(E_1) = E_2$ et $\phi(O_1) = O_2$, où O_1 et O_2 sont les points origines respectifs de E_1 et E_2.

Toute isogénie de la forme

$$x = u^2x' + r$$

$$y = u^3y' + su^2x' + t$$

avec $u,r,s,t \in K$ et $u \neq 0$, est un isomorphisme (sur$K$) de courbes elliptiques.

En appliquant donc le changement de variables précédant à une courbe elliptique E_1/K donnée par l'équation de Weierstrass

$$E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in K$$

on obtient une courbe elliptique E_2/K isomorphe (sur K) à E_1/K donnée par l'équation

$$E_2 : y'^2 + a'_1x'y' + a'_3y' = x'^3 + a'_2x'^2 + a'_4x' + a'_6 \qquad a'_i \in K$$

où les coefficients a_i' sont donnés en fonction des coefficients a_i,u,r,s,t par les formules

$$\begin{cases} ua'_1 = a_1 + 2s, \;\; u^2a'_2 = a_2 - sa_1 + 3r - s^2, \\ u^3a'_3 = a_3 + ra_1 + 2t, \\ u^4a'_4 = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - st, \\ u^6a'_6 = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1, \\ u^2b'_2 = b_2 + 12r, \\ u^4b'_4 = b_4 + rb_2 + 6r^2, \\ u^6b'_6 = b_6 + 2rb_4 + r^2b_2 + 4r^3, \\ u^8b'_8 = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4, \\ u^4c'_4 = c_4, \;\; u^6c'_6 = c_6, \;\; u^{12}\Delta' = \Delta, \;\; j\prime = j, \end{cases}$$

On voit d'après les formules précédentes que si deux courbes elliptiques E_1/K et E_2/K sont isomorphes, alors on a $j(E_1) = j(E_2)$, la réciproque est vraie sur un corps algébriquement clos (voir [14] chapitre III proposition 1.4 (b)).

2.1.3.2 Exemple

Pour chaque entier $m \in \mathbf{Z}$ on peut définir une isogénie en multipliant par m

$$[m] : E \to E \quad P \mapsto [m]P = P + ... + P \ (m \text{ fois}, m > 0).$$

Si $m < 0$ alors $[m]P = [-m](-P)$ et $[0]P = O$.

2.1.3.3 Définition

Soit E une courbe elliptique et $m \in \mathbf{Z}$, $m \neq 0$. Le sous groupe de m-torsion de E , noté $E[m]$, est l'ensemble:

$$E[m] = \{P \in E : [m]P = O\}.$$

2.1.3.4 Théorème

Soit $\phi : E_1 \to E_2$ une isogénie non-constante de degré m. Alors il existe une unique isogénie

$$\widehat{\phi} : E_2 \to E_1$$

satisfaisant

$$\widehat{\phi} \circ \phi = [m].$$

Preuve. voir [14] chapitre III théorème 6.1.

2.1.3.5 Remarque

Comme les courbes elliptiques sont des groupes abéliens, les morphismes entre les courbes elliptiques forment un groupe abélien. Donc soit

$$\text{Hom}(E_1,E_2) = \{\text{isogénies } \phi : E_1 \to E_2\} \cup \{0\}$$

et la loi de composition est définie par

$$(\phi + \psi)(P) = \phi(P) + \psi(P).$$

Si $E_1 = E_2$, alors on peut composer les isogénies. Donc si E est une courbe

elliptique, on pose

$$\mathrm{End}(E) = \mathrm{Hom}(E,E)$$

c'est un anneau pour l'addition et la multiplication qui est donnée par la composition:

$$(\phi\psi)(P) = \phi(\psi(P)).$$

$\mathrm{End}(E)$ est appelé l'anneau des endomorphismes de E. Les éléments inversibles de $\mathrm{End}(E)$ forment le groupe des automorphismes de E, noté $\mathrm{Aut}(E)$. On note par

$$\mathrm{Hom}_K(E_1,E_2), \quad \mathrm{End}_K(E), \quad \mathrm{Aut}_K(E)$$

les groupes d'isogénies définies sur K.

2.1.3.6 Formule de Vélu

Connaissant l'équation d'une courbe elliptique E définie sur un corps K et les coordonnées des points d'un sous-groupe fini F de E, nous donnons les équations de la courbe isogène E/F et de l'isogénie $f : E \to E/F$.

Désignons par G le polynôme

$$G(\xi,\eta) = \xi^3 + a_2\xi^2 + a_4\xi + a_6 - \eta^2 - a_1\xi\eta - a_3\eta.$$

Désignons par F_2 l'ensemble des points d'ordre 2 de $F - \{O\}$, par R une partie de $F - \{O\} - F_2$ telle que

$$F - \{O\} - F_2 = R \cup (-R) \qquad \text{et} \qquad R \cap (-R) = \emptyset.$$

Désignons enfin par S l'union de F_2 et R. L'isogénie f admet pour équations:

$$\begin{cases} X = x + \sum\limits_{Q\in S}\left[\dfrac{t_Q}{x-x_Q} + \dfrac{u_Q}{(x-x_Q)^2}\right] \\ \\ Y = y - \sum\limits_{Q\in S}\left[u_Q\dfrac{2y+a_1x+a_3}{(x-x_Q)^3} + t_Q\dfrac{a_1(x-x_Q)+y-y_Q}{(x-x_Q)^2} + \dfrac{a_1u_Q - g_Q^x g_Q^y}{(x-x_Q)^2}\right] \end{cases}$$

où l'on a:

$$\begin{cases} Q = (x_Q, y_Q) \\ g_Q^x = \dfrac{\partial G}{\partial \xi}(x_Q, y_Q) = 3x_Q^2 + 2a_2 x_Q + a_4 - a_1 y_Q \\ g_Q^y = \dfrac{\partial G}{\partial \eta}(x_Q, y_Q) = -2y_Q - a_1 x_Q - a_3 \\ t_Q = \begin{cases} g_Q^x & \text{si } Q \in F_2 \\ 2g_Q^x - a_1 g_Q^y = 6x_Q^2 + b_2 x_Q + b_4 & \text{si } Q \notin F_2 \end{cases} \\ u_Q = (g_Q^y)^2 = 4x_Q^3 + b_2 x_Q^2 + 2b_4 x_Q + b_6. \end{cases}$$

Passons maintenant à la relation liant X et Y. Posons

$$t = \sum_{Q \in S} t_Q \qquad \omega = \sum_{Q \in S} (u_Q + x_Q t_Q).$$

On obtient

$$Y^2 + A_1 XY + A_3 Y = X^3 + A_2 X^2 + A_4 X + A_6$$

avec

$$A_1 = a_1, \quad A_2 = a_2, \quad A_3 = a_3, \quad A_4 = a_4 - 5t, \quad A_6 = a_6 - b_2 t - 7\omega.$$

2.1.4 Réduction d'une courbe elliptique

2.1.4.1 Notations

K	un corps local complet pour la valuation discrète ϑ
R	l'anneau des entiers de $K = \{x \in K : \vartheta(x) \geq 0\}$
$R^\star$	le groupe multiplicatif des unités de l'anneau $R = \{x \in R : \vartheta(x) = 0\}$
$\mathcal{M}$	l'idéal maximal de l'anneau local $R = \{x \in R : \vartheta(x) > 0\}$
π	une uniformisante de l'anneau R
k	le corps résiduel de l'anneau $R = R/\mathcal{M}$.

On suppose de plus que $\vartheta(0) = \infty$ et $\vartheta(\pi) = 1$, et que les corps K et k sont parfaits.

Soit E/K une courbe elliptique définie par:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad a_i \in K.$$

L'équation de Weierstrass de E/K est dite minimale en ϑ si ses coefficients a_i sont ϑ-entiers (i.e. $\vartheta(a_i) \geq O$) et si son discriminant Δ est tel que $\vartheta(\Delta)$ soit minimal.

2.1.4.2 Remarques

1. Si on remplace (x,y) par $(u^{-2}x,u^{-3}y)$ dans l'équation ci-dessus alors chaque a_i devient u^ia_i, et donc si on choisit u divisible par une assez grande puissance de π, on trouve une équation de Weierstrass avec tous les coefficients $a_i \in R$. Dans ce cas, le discriminant satisfait $\vartheta(\Delta) \geq 0$.

2. Si l'équation n'est pas minimale, alors il existe un changement de variables qui donne une nouvelle équation avec le discriminant $\Delta' = u^{12}\Delta$, $\Delta \in R$.

   On conclut que si $a_i \in R$ et $\vartheta(\Delta) < 12$, alors l'équation est minimale.

   De même, comme $c_4' = u^4c_4$ et $c_6' = u^6c_6$, on en déduit que si $a_i \in R$ et $\vartheta(c_4) < 4$ (ou $\vartheta(c_6) < 6$), alors l'équation est minimale.

L'application de R dans k qui à t associe $\widetilde{t}$ donne l'application réduction:

$$E(K) \to \widetilde{E}(k)$$

qui à P associe $\widetilde{P}$. La courbe $\widetilde{E}/k$ est appelée réduction de la courbe elliptique E modulo π. Si E/K est une courbe elliptique d'équation de Weierstrass minimale en ϑ, alors pour obtenir l'équation de la courbe réduite $\widetilde{E}/k$ il suffit de réduire modulo π les coefficients a_i

$$\widetilde{E}/k: \qquad y^2 + \widetilde{a}_1xy + \widetilde{a}_3y = x^3 + \widetilde{a}_2x^2 + \widetilde{a}_4x + \widetilde{a}_6 \qquad \widetilde{a}_i \in k.$$

2.1.4.3 Définition

Soit E/K une courbe elliptique d'équation de Weierstrass minimale en ϑ et $\widetilde{E}/k$ la réduction de E modulo π. Alors on dit que

1. E a une bonne réduction sur K si $\widetilde{E}$ est lisse.

2. E a une mauvaise réduction sur K si $\widetilde{E}$ est singulière. Cette mauvaise réduction est:

(a) Multiplicative sur K si $\widetilde{E}$ possède un noeud, multiplicative déployée si les deux tangentes à $\widetilde{E}$ au noeud sont rationnelles.

(b) Additive sur K si $\widetilde{E}$ possède un point de rebroussement .

2.1.4.4 Proposition

Soit E une courbe donnée par une équation de Weierstrass de discriminant $\Delta = 0$, et S son point singulier. Alors $E^{sm} = E - \{S\}$ est un groupe abélien.

1. Supposons que E a un noeud (donc $c_4 \neq 0$) et soient

$$y = \alpha_1 x + \beta_1 \qquad \text{et} \qquad y = \alpha_2 x + \beta_2$$

les équations des deux tangentes à E au point S. Alors l'application

$$E^{sm}(\overline{K}) \to \overline{K}^{\star} \qquad (x,y) \mapsto \frac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2}$$

est un isomorphisme (de groupes abéliens).

2. Supposons que E a un point de rebroussement (donc $c_4 = 0$) et soit

$$y = \alpha x + \beta$$

l'équation de la tangente à E au point S. Alors l'application

$$E^{sm}(\overline{K}) \to \overline{K}^{+} \qquad (x,y) \mapsto \frac{x - x(S)}{y - \alpha x - \beta} \qquad .$$

est un isomorphisme.

Preuve. voir [14] chapitre III proposition 2.5.

La nature de la réduction est donnée par le théorème suivant:

2.1.4.5 Théorème

Soit E/K une courbe elliptique définie par une équation minimale de Weierstrass

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad a_i \in K$$

et soit Δ son discriminant et c_4 son coefficient associé. Alors

1. E a une bonne réduction sur K si et seulement si $\vartheta(\Delta) = 0$ (i.e. $\Delta \in R^\star$). Dans ce cas $\widetilde{E}/k$ est une courbe elliptique.

2. E a une réduction multiplicative sur K si et seulement si $\vartheta(\Delta) > 0$ et $\vartheta(c_4) = 0$ (i.e. $\Delta \in \mathcal{M}$ et $c_4 \in R^\star$). Dans ce cas $\widetilde{E}^{sm}(\overline{k}) \cong \overline{k}^\star$.

3. E a une réduction additive sur K si et seulement si $\vartheta(\Delta) > 0$ et $\vartheta(c_4) > 0$ (i.e. Δ,$c_4 \in \mathcal{M}$). Dans ce cas $\widetilde{E}^{sm}(\overline{k}) \cong \overline{k}^+$.

Preuve. voir [14] chapitre VII proposition 5.1.

On utilisera aussi le lemme suivant:

2.1.4.6 Lemme

Soit Q un point lisse de $\widetilde{E}(k)$. Alors il existe un point $P \in E$ tel que $\widetilde{P} = Q$.

Preuve. voir [3] chapitre 10 lemme 1.

2.2 Cohomologie des groupes

2.2.1 Cohomologie des groupes finis

Soit M un groupe abélien, et soit G un groupe fini qui agit sur M. On note l'action de $\sigma \in G$ sur $m \in M$ par $m \to m^\sigma$. Alors M est un G-module (à droite) si l'action de G sur M satisfait

$$m^1 = m \qquad (m + m')^\sigma = m^\sigma + m'^\sigma \qquad (m^\sigma)^\tau = m^{\sigma\tau}.$$

Soient M et N deux G-modules. Un G-homomorphisme est un homomorphisme $\phi : M \to N$ de groupes abéliens qui commute avec l'action de G, en d'autres termes

$$\phi(m^\sigma) = \phi(m)^\sigma \qquad \text{pour tous } m \in M \text{ et } \sigma \in G.$$

2.2.1.1 Définition

Le 0^{eme} groupe de cohomologie d'un G-module M, noté M^G ou $H^0(G,M)$, est défini par:

$$H^0(G,M) = \{m \in M : m^\sigma = m, \text{ pour tout } \sigma \in G\}$$

c'est un sous module de M formé de tous les éléments G-invariants.

2.2.1.2 Définition

Soit M un G-module. Le groupe des 1-cochaînes (de G vers M) est défini par:

$$C^1(G,M) = \{ \text{ applications } \xi : G \to M\}.$$

Le groupe des 1-cocycles (de G vers M) est donné par

$$Z^1(G,M) = \{\xi \in C^1(G,M) : \xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau, \text{ pour tous } \sigma,\tau \in G\}.$$

Le groupe des 1-cobords (de G vers M) est défini par

$$B^1(G,M) = \{\xi \in C^1(G,M) \text{: il existe un } m \in M \text{ tel que } \xi_\sigma = m^\sigma - m, \text{ pour tout } \sigma \in G\}.$$

Il est facile de voir que $B^1(G,M) \subset Z^1(G,M)$. Alors le 1^{er} groupe de cohomologie du G-module M est le groupe quotient

$$H^1(G,M) = Z^1(G,M)/B^1(G,M).$$

En d'autres termes, $H^1(G,M)$ est le groupe des 1-cocycles $\xi : G \to M$, modulo la relation d'équivalence définie par deux 1-cocycles sont identifiés si leurs différence est de la forme $\sigma \to m^\sigma - m$ pour un $m \in M$.

Soit $\phi : M \to N$ un homomorphisme de G-modules. Il est clair que la composition avec ϕ envoie $Z^1(G,M)$ vers $Z^1(G,N)$ et $B^1(G,M)$ vers $B^1(G,N)$. Donc ϕ induit une application en cohomologie

$$\phi : H^1(G,M) \to H^1(G,N).$$

2.2.1.3 Proposition

Soit

$$0 \to P \xrightarrow{\phi} M \xrightarrow{\psi} N \to 0$$

une suite exacte de G-modules. Alors il existe une suite exacte longue:

$$0 \to H^0(G,P) \to H^0(G,M) \to H^0(G,N) \xrightarrow{\delta} H^1(G,P) \to H^1(G,M) \to H^1(G,N)$$

où le morphisme de connection δ est défini de la manière suivante:

Soit $n \in H^0(G,N) = N^G$. On choisit un $m \in M$ tel que $\psi(m) = n$ et on définit une cochaîne $\xi \in C^1(G,M)$ par:

$$\xi_\sigma = m^\sigma - m$$

Alors, en fait, $\xi \in Z^1(G,P)$ et $\delta(n)$ est la classe de cohomologie du 1-cocycle ξ dans $H^1(G,P)$.

Preuve. voir [14] annexe B proposition 1.2.

2.2.2 Cohomologie galoisienne

Soit K un corps parfait, $\overline{K}$ une clôture algébrique de K, et soit $G_{\overline{K}/K}$ le groupe de Galois de $\overline{K}$ sur K. On sait que $G_{\overline{K}/K}$ est égal à la limite projective des $G_{L/K}$ lorsque L parcourt l'ensemble de toutes les extensions galoisiennes finies de K.

Donc $G_{\overline{K}/K}$ est un groupe profini (limite projective de groupes finis). On munit $G_{\overline{K}/K}$ d'une topologie en prenant comme base d'ouverts autour de l'identité la collection des sous groupes normaux ouverts de $G_{\overline{K}/K}$ (i.e. les sous groupes qui sont les noyaux des applications $G_{\overline{K}/K} \to G_{L/K}$ pour des extensions galoisiennes finies).

2.2.2.1 Définition

Un $G_{\overline{K}/K}$-module (discret) est un groupe abélien M sur lequel $G_{\overline{K}/K}$ agit, tel que l'action soit continue pour la topologie profinie sur $G_{\overline{K}/K}$ et la topologie discrète sur M. Comme tous les $G_{\overline{K}/K}$-modules que nous allons considérer sont discrets, on va les appeler simplement $G_{\overline{K}/K}$-modules.

2.2.2.2 Définition

Le 0^{eme} groupe de cohomologie du $G_{\overline{K}/K}$-module M est le groupe des éléments de M, $G_{\overline{K}/K}$-invariants:

$$M^{G_{\overline{K}/K}} = H^0(G_{\overline{K}/K},M) = \{m \in M : m^\sigma = m, \text{ pour tour } \sigma \in G_{\overline{K}/K}\}.$$

2.2.2.3 Définition

Soit M un $G_{\overline{K}/K}$-module. Une application $\xi : G_{\overline{K}/K} \to M$ est continue si elle est continue pour la topologie profinie sur $G_{\overline{K}/K}$ et la topologie discrète sur M (i.e. Pour tout $m \in M$, $\xi^{-1}(m)$ contient un sous groupe ouvert dans $G_{\overline{K}/K}$). On

définit le groupe des 1-cocycles continus de $G_{\overline{K}/K}$ vers M, noté $Z^1_{cont}(G_{\overline{K}/K},M)$, par:

$$Z^1_{cont}(G_{\overline{K}/K},M) = \{\xi : G_{\overline{K}/K} \to M : \xi \text{ continue et } \xi_{\sigma\tau} = \xi^\tau_\sigma + \xi_\tau, \text{ pour tous } \sigma,\tau \in G_{\overline{K}/K}\}$$

(c'est un sous groupe du groupe $Z^1(G_{\overline{K}/K},M)$). Notons que comme M est discret, tout cobord $\sigma \to m^\sigma - m$ est automatiquement continu. Le 1^{er} groupe de cohomologie du $G_{\overline{K}/K}$-module M est défini par:

$$H^1(G,M) = Z^1_{cont}(G_{\overline{K}/K},M)/B^1(G,M).$$

2.2.2.4 Proposition

Soit

$$0 \to P \xrightarrow{\phi} M \xrightarrow{\psi} N \to 0$$

une suite exacte de $G_{\overline{K}/K}$-modules. Alors il existe une suite exacte longue:

$$0 \to H^0(G_{\overline{K}/K},P) \to H^0(G_{\overline{K}/K},M) \to H^0(G_{\overline{K}/K},N)$$

$$\xrightarrow{\delta} H^1(G_{\overline{K}/K},P) \to H^1(G_{\overline{K}/K},M) \to H^1(G_{\overline{K}/K},N)$$

où le morphisme de connection δ est défini comme dans (2.2.1.3).

Preuve. voir [14] annexe B proposition 2.3.

2.2.2.5 Proposition

Soit K un corps, alors

1. $H^1(G_{\overline{K}/K},\overline{K}^+) = 0$
2. $H^1(G_{\overline{K}/K},\overline{K}^\star) = 0$
3. Supposons que $\mathrm{car}(K)$ ne divise pas m (ou $\mathrm{car}(K) = 0$). On a alors

$$H^1(G_{\overline{K}/K},\mu_m) \cong K^\star/(K^\star)^m.$$

Preuve. voir [14] annexe B proposition 2.5.

2.2.3 Cohomologie non-abélienne

Soit G un groupe fini et M un groupe (non abélien dont la loi du groupe est notée multiplicativement) sur lequel G agit. Le 0^{eme} groupe de cohomologie de M est défini par

$$H^0(G,M) = M^G = \{m \in M : m^\sigma = m, \text{ pour tout } \sigma \in G\}.$$

On définit l'ensemble des 1-cocycles de G dans M par l'ensemble des applications

$$\xi : G \to M \qquad \text{telles que } \xi_{\sigma\tau} = (\xi_\sigma)^\tau \xi_\tau \qquad \text{pour tout } \sigma,\tau \in G.$$

2.2.3.1 Remarque

En général, l'ensemble des 1-cocycles n'est pas un groupe. Comme le groupe M n'est pas abélien, le produit de deux 1-cocycles n'est pas forcemment un 1-cocycles.

On dit que deux 1-cocycles ξ et ζ sont dans la même classe de cohomologie s'il existe $m \in M$ tel que

$$m^\sigma \xi_\sigma = \zeta_\sigma m \qquad \text{pour tout } \sigma \in G.$$

On vérifie facilement que c'est une relation d'équivalence sur l'ensemble des 1-cocycles. Le 1^{er} ensemble de cohomologie de M, noté $H^1(G,M)$, est l'ensemble des 1-cocycles modulo cette relation.

2.3 Résidus quadratiques

2.3.1 Quelques résultats

Soient a et m deux entiers premiers entre eux. L'entier a est appelé résidu quadratique modulo m si la congruence $x^2 \equiv a \bmod(m)$ a une solution.

2.3.1.1 Définition

Le symbole (a/p) a pour valeur 1 si a est un résidu quadratique modulo p, -1 si a n'est pas un résidu quadratique modulo p, et zéro si $p|a$. (a/p) est appelé le symbole de Legendre.

2.3.1.2 Proposition

1. $a^{(p-1)/2} \equiv (a/p) \bmod(p)$.

2. $(ab/p) = (a/p)(b/p)$.

3. Si $a \equiv b \bmod(p)$, alors $(a/p) = (b/p)$.

Preuve. voir [6] chapitre 5 proposition 5.1.2.

2.3.1.3 Théorème

Soient p et q deux premiers impairs. Alors

1. $(-1/p) = (-1)^{(p-1)/2}$.

2. $(2/p) = (-1)^{(p^2-1)/8}$.

3. $(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}$.

Preuve. voir [6] chapitre 5 théorème 1.

2.3.1.4 Théorème

Soient p et q deux premiers impairs. Alors

1. Si $q \equiv 1 \bmod(4)$, alors q est un résidu quadratique modulo p si et seulement si $p \equiv r \bmod(q)$, où r est un résidu quadratique modulo q.

2. Si $q \equiv 3 \bmod(4)$, alors q est un résidu quadratique modulo p si et seulement si $p \equiv \pm b^2 \bmod(4q)$, où b est un entier impair premier à q.

Preuve. voir [6] chapitre 5 théorème 2.

Chapitre 3

Quelques exemples de 5 et 7 descente sur une courbe elliptique définie sur Q

3.1 Les calculs de descente

3.1.1 Equations de Weierstrass et types de réduction

Soit K un corps de nombres et n un entier ≥ 4. On considère des paires de courbes elliptiques n-isogènes C et D définies sur K. On suppose que le noyau de $\phi : C \to D$ est isomorphe à μ_n et le noyau de $\widehat{\phi} : D \to C$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$. Les paires de telles courbes elliptiques C et D sont paramétrées par la courbe modulaire $Y_1(n)$. Pour n premier, $X_1(n)$ a $n-1$ pointes, dont la moitié est définie sur $\mathbf{Q}$ et l'autre moitié sur $\mathbf{Q}(\mu_n) \cap \mathbf{R}$. On s'intéresse aux cas $n = 5$ et $n = 7$ lorsque $X_1(n) \cong \mathbf{P}^1$. On va spécifier une coordonnée λ sur $X_1(n)$ et écrire C_λ et D_λ pour la paire de courbes elliptiques n-isogènes au-dessus de λ.

3.1.1.1 Lemme

Soit E/K une courbe elliptique et $P = (x_0,y_0) \in E(K)$ un point d'ordre au moins 4. Alors:

1. E/K admet une équation de Weierstrass

$$y^2 + uxy + vy = x^3 + vx^2 \qquad \text{avec } P = (0,0).$$

2. La paire (E,P) détermine de manière unique le couple $(u,v) \in \mathbf{A}^2(K)$.

3. La paire (E,P) n'admet aucun automorphisme.

Preuve

1. Soit
$$E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
avec $P = (x_0,y_0) \in E(K)$ tel que $2P \neq O$ et $3P \neq O$. Après le changement de variables
$$(x,y) \longmapsto (x - x_0,y - y_0)$$
l'équation de E/K devient :
$$y^2 + \alpha_1xy + \alpha_3y = x^3 + \alpha_2x^2 + \alpha_4x$$
avec

$P = (0,0)$, $\alpha_1 = a_1$, $\alpha_2 = 3x_0 + a_2$, $\alpha_3 = 2y_0 + a_1x_0 + a_3$ et enfin $\alpha_4 = 3x_0^2 + 2a_2x_0 + a_4 - a_1y_0$.

Si $\alpha_3 = \alpha_4 = 0$ alors la courbe E/K est singulière, ce qui contredit le fait que E est une courbe elliptique, et donc on a $\alpha_3 \neq 0$ ou $\alpha_4 \neq 0$. On sait que si $2P = O$ la tangente au point P est verticale et le coefficient de dy est nul, dans notre cas le coefficient de dy est $2y + \alpha_1x + \alpha_3$. Donc P est d'ordre 2 si et seulement si $\alpha_3 = 0$, d'où $\alpha_3 \neq 0$. Faisons maintenant le changement de variables
$$(x,y) \longmapsto (x,y + \alpha_3^{-1}\alpha_4x),$$
l'équation de E/K devient :
$$y^2 + \beta_1xy + \beta_3y = x^3 + \beta_2x^2$$
avec
$$P = (0,0),\ \beta_1 = \alpha_1 - 2\alpha_3^{-1}\alpha_4\ ,\ \beta_2 = \alpha_2 + \alpha_1\alpha_3^{-1}\alpha_4 - \alpha_3^{-2}\alpha_4^2\ ,\ \beta_3 = \alpha_3.$$
Pour $P = (0,0)$ on a $-P = (0, -\beta_3)$ et $2P = (-\beta_2,\beta_1\beta_2 - \beta_3)$, donc si $3P = O$ on obtient $\beta_2 = 0$, d'où $\beta_2 \neq 0$. On en conclut que E/K admet une équation de la forme:
$$E/K : y^2 + \beta_1xy + \beta_3y = x^3 + \beta_2x^2 \qquad \text{avec } \beta_2 \neq 0\ ,\ \beta_3 \neq 0 \text{ et } P = (0,0).$$

On peut éliminer un paramètre par le changement de variables

$$(x,y) \mapsto (\mu^{-2}x,\mu^{-3}y)$$

avec $\mu = \beta_2^{-1}\beta_3$, alors l'équation de E/K devient:

$$y^2 + uxy + vy = x^3 + vx^2$$

avec $P = (0,0)$, $u = \beta_1\beta_2\beta_3^{-1}$ et $v = \beta_2^3\beta_3^{-2}$.

2. D'après 1. on a :

$$\begin{aligned} u &= \beta_1\beta_2\beta_3^{-1} \\ &= (\alpha_1 - 2\alpha_3^{-1}\alpha_4)(\alpha_2 + \alpha_1\alpha_3^{-1}\alpha_4 - \alpha_3^{-2}\alpha_4^2)\alpha_3^{-1} \\ &= [a_1 - 2(2y_0 + a_1x_0 + a_3)^{-1}(3x_0^2 + 2a_2x_0 + a_4 - a_1y_0)] \\ &\quad \times[(3x_0 + a_2) + a_1(2y_0 + a_1x_0 + a_3)^{-1}(3x_0^2 + 2a_2x_0 + a_4 - a_1y_0) \\ &\quad -(2y_0 + a_1x_0 + a_3)^{-2}(3x_0^2 + 2a_2x_0 + a_4 - a_1y_0)^2](2y_0 + a_1x_0 + a_3)^{-1} \end{aligned}$$

et

$$\begin{aligned} v &= \beta_2^3\beta_3^{-2} \\ &= (\alpha_2 + \alpha_1\alpha_3^{-1}\alpha_4 - \alpha_3 - 2\alpha_4^2)^3\alpha_3^{-2} \\ &= [(3x_0 + a_2) + a_1(2y_0 + a_1x_0 + a_3)^{-1}(3x_0^2 + 2a_2x_0 + a_4 - a_1y_0) \\ &\quad -(2y_0 + a_1x_0 + a_3)^{-2}(3x_0^2 + 2a_2x_0 + a_4 - a_1y_0)^2]^3(2y_0 + a_1x_0 + a_3)^{-2}. \end{aligned}$$

Et donc la paire (E,P) détermine de manière unique le couple $(u,v) \in \mathbf{A}^2(K)$.

3. Supposons qu'il existe un automorphisme de (E,P). Alors il est de la forme:

$$\phi : (x,y) \longmapsto (\gamma^2x,\gamma^3y) \qquad \gamma \in K^\star.$$

Pour $P = (0,0)$, on a $2P = (-v,vu - v)$ et $\phi(2P) = 2\phi(P) = 2P$. Par ailleurs, $\phi(2P) = \phi(-v,vu - v) = (-\gamma^2v,\gamma^3(vu - v))$, ce qui donne $\gamma = 1$, et donc l'unique automorphisme de (E,P) est l'identité.

□

Calculons maintenant $mP = (x_m(u,v),y_m(u,v))$ pour quelques valeurs de l'entier m. En égalisant quelques unes de ces expressions, on trouve des courbes affines dont le modèle projectif lisse est $X_1(n)$.

Soit

$$E/K : y^2 + uxy + vy = x^3 + vx^2 \qquad P = (0,0) \text{ un point d'ordre 5.}$$

Posons $u = 1 - \lambda$ et $v = -\theta$, alors on a:

$$-P = (0,\theta),\ 2P = (\theta,\lambda\theta),\ -2P = (\theta,0),\ 3P = (\lambda,\theta - \lambda),\ -3P = (\lambda,\lambda^2).$$

Donc $5P = O$ équivaut à $\lambda = \theta$ et donc l'équation de E/K peut s'écrire sous la forme:

$$y^2 + (1 - \lambda)xy - \lambda y = x^3 - \lambda x^2.$$

Supposons maintenant que l'on a:

$$E/K : y^2 + uxy + vy = x^3 + vx^2 \qquad P = (0,0) \text{ un point d'ordre 7.}$$

Posons $u = 1 - \upsilon$, et $v = -\theta$, alors on a:,

$$3P = (\upsilon,\theta - \upsilon),\ -3P = (\upsilon,\upsilon^2),\ 4P = \big(\frac{\theta(\theta - \upsilon)}{\upsilon^2},\frac{\theta^2(\upsilon^2 + \upsilon - \theta)}{\upsilon^3}\big),$$

donc $4P = -3P$ donne $\theta(\theta - \upsilon) = \upsilon^3$. On remplace $\theta = \lambda\upsilon$ dans la dernière équation $\lambda^2\upsilon^2 - \lambda\upsilon^2 = \upsilon^2$ ce qui donne $\upsilon = \lambda^2 - \lambda$ et $\theta = \lambda^3 - \lambda^2$ d'où l'équation de E/K peut s'écrire comme suit:

$$E/K : y^2 + (1 + \lambda - \lambda^2)xy + (\lambda^2 - \lambda^3)y = x^3 + (\lambda^2 - \lambda^3)x^2.$$

En résumé on a:

$$\begin{aligned} &n = 5 \quad D_\lambda : y^2 + (1 - \lambda)xy - \lambda y = x^3 - \lambda x^2 \\ &n = 7 \quad D_\lambda : y^2 + (1 + \lambda - \lambda^2)xy + (\lambda^2 - \lambda^3)y = x^3 + (\lambda^2 - \lambda^3)x^2. \end{aligned} \tag{3.1}$$

3.1.1.2 Lemme

Avec les notations (3.1), on a pour $n = 5$, $(D_\lambda,2P) \cong (D_{-1/\lambda},P)$, et pour $n = 7$,$(D_\lambda,2P) \cong (D_{(\lambda-1)/\lambda},P)$.

Preuve

Pour $n = 5$ (respectivement, $n = 7$) l'isogénie

$$\phi : (D_\lambda,2P) \to (D_{-1/\lambda},P)$$

donnée par

$$(x,y) \mapsto (\frac{1}{\lambda^2}x - \frac{1}{\lambda}, \frac{1}{\lambda^3}y - \frac{1}{\lambda^2}x)$$

(respectivement,

$$\phi : (D_\lambda, 2P) \to D_{(\lambda-1)/\lambda}, P)$$

donnée par

$$(x,y) \mapsto (\frac{1}{\lambda^4}x - \frac{\lambda-1}{\lambda^2}, \frac{1}{\lambda^6}y - \frac{\lambda^2-1}{\lambda^6}x + \frac{\lambda^2-2\lambda+1}{\lambda^4}))$$

est un isomorphisme et son inverse est donnée par

$$\widehat{\phi} : (x,y) \mapsto (\lambda^2 x + \lambda, \lambda^3 y + \lambda^3 x + \lambda^2)$$

(respectivement,

$$\widehat{\phi} : (x,y) \mapsto (\lambda^4 x + \lambda^3 - \lambda^2, \lambda^6 y + \lambda^4(\lambda^2-1)x + \lambda^5 - \lambda^4 + \lambda^3)).$$

□

En appliquant la formule de Vélu pour $E = D_\lambda$ et F le sous-groupe engendré par $P = \{O, P, ..., (n-1)P)$, on trouve que $C_\lambda = D_\lambda / F$ admet pour équation de Weierstrass:

$$C_\lambda : y^2 + a_1 xy + a_2 y = x^3 + a_2 x^2 - 5tx - b_2 t - 7\omega \tag{3.2}$$

où

$$n = 5 \begin{cases} a_1 = a_1(D_\lambda) = (1-\lambda) \\ a_2 = a_2(D_\lambda) = -\lambda \\ b_2 = b_2(D_\lambda) = \lambda^2 - 6\lambda + 1 \\ t = \lambda(\lambda^2 + 2\lambda - 1) \\ \omega = \lambda^2(2\lambda^2 + \lambda + 1) \end{cases}$$

$$n=7\begin{cases} a_1=a_1(D_\lambda)=(1+\lambda-\lambda^2) \\ a_2=a_2(D_\lambda)=(\lambda^2-\lambda^3) \\ b_2=b_2(D_\lambda)=\lambda^4-6\lambda^3+3\lambda^2+2\lambda+1 \\ t=\lambda(\lambda-1)(\lambda^2-\lambda+1)(\lambda^3+2\lambda^2-5\lambda+1 \\ \omega=\lambda^2(\lambda-1)^2(2\lambda^6-2\lambda^5+\lambda^4-8\lambda^3+15\lambda^2-9\lambda+2). \end{cases}$$

Les discriminants des équations de Weierstrass de C_λ et D_λ sont donnés par:

$$n=5\begin{cases} \Delta(C_\lambda)=\lambda(\lambda^2-11\lambda-1)^5 \\ \Delta(D_\lambda)=\lambda^5(\lambda^2-11\lambda-1) \end{cases}$$

$$n=7\begin{cases} \Delta(C_\lambda)=\lambda(\lambda-1)(\lambda^3-8\lambda^2+5\lambda+1)^7 \\ \Delta(D_\lambda)=\lambda^7(\lambda-1)^7(\lambda^3-8\lambda^2+5\lambda+1) \end{cases}$$

et les coefficients c_4 sont donnés par:

$$n=5\begin{cases} c_4(C_\lambda)=\lambda^4+228\lambda^3+494\lambda^2-228\lambda+1 \\ c_4(D_\lambda)=\lambda^4-12\lambda^3+14\lambda^2+12\lambda+1 \end{cases}$$

$$n=7\begin{cases} c_4(C_\lambda)=\lambda^8+228\lambda^7+42\lambda^6-1736\lambda^5+3395\lambda^4-3360\lambda^3+1666\lambda^2-236\lambda+1 \\ c_4(D_\lambda)=\lambda^8-12\lambda^7+42\lambda^6-56\lambda^5+35\lambda^4-14\lambda^2+4\lambda+1. \end{cases}$$

Tout au long de nos calculs de descente on aura besoin du type de réduction des courbes C_λ et D_λ, il est donc préférable de le décrire maintenant. On rappelle que deux courbes isogènes ont le même type de réduction.

3.1.1.3 Lemme

Soit p un premier de K avec $p \not| n$, $n=5,7$. Pour $\lambda \in K_p$ avec $\mathrm{ord}_p(\lambda) \geq 0$ les équations de Weierstrass (3.1) et (3.2) de C_λ et D_λ sont minimales et leur type

de réduction est:

1. Si $\lambda \equiv 0 \bmod(p)$ (resp. $\lambda(\lambda-1) \equiv 0 \bmod(p)$) alors C_λ et D_λ ont une réduction multiplicative déployée.

2. Si $\lambda^2 - 11\lambda - 1 \equiv 0 \bmod(p)$ (resp. $\lambda^3 - 8\lambda^2 + 5\lambda + 1 \equiv 0 \bmod(p)$) alors C_λ et D_λ ont une réduction multiplicative et elle est déployée si et seulement si $\mathrm{Norm}(p) \equiv 1 \bmod(n)$.

3. Dans les autres cas C_λ et D_λ ont une bonne réduction.

Preuve

Montrons d'abord le lemme pour $n = 5$. Soit p un premier de K avec $p \nmid 5$ et soit $\lambda \in K_p$ avec $\mathrm{ord}_p(\lambda) \geq 0$.

. Si $p \nmid \Delta(D_\lambda)$ (resp. $p \nmid \Delta(C_\lambda)$), alors les équations de Weierstrass des courbes D_λ et C_λ sont minimales.

. Si $p|\lambda$ alors $p \nmid c_4(D_\lambda)$ (resp. $p \nmid c_4(C_\lambda)$), d'où les équations sont minimales.

. Si $p \nmid \lambda$ et $p|(\lambda^2 - 11\lambda - 1)$, on a

$$\begin{cases} c_4(D_\lambda) = (\lambda^2 - 11\lambda - 1)(\lambda^2 - \lambda - 1) + 5\lambda^2 \\ \\ c_4(C_\lambda) = (\lambda^2 - 11\lambda - 1)(\lambda^2 + 239\lambda - 1) + 5^5\lambda \end{cases}$$

et donc $p \nmid c_4(D_\lambda)$ (resp. $p \nmid c_4(C_\lambda)$) d'où les équations sont minimales.

1. Si $\lambda \equiv 0 \bmod(p)$, alors $p|\Delta(D_\lambda)$ et $p \nmid c_4(D_\lambda)$ et donc les courbes D_λ et C_λ ont une réduction multiplicative, de plus les pentes des tangentes à la courbe

$$\widetilde{D_\lambda} : y^2 + xy = x^3$$

au noeud $\widetilde{P} = (0,0)$ sont les zéros de $\alpha^2 + \alpha$ (i.e. 0 et -1) qui appartiennent à R, et donc la réduction est déployée.

2. Si $\lambda^2 - 11\lambda - 1 \equiv 0 \bmod(p)$, alors $\Delta(D_\lambda) \equiv 0 \bmod(p)$ et $c_4(D_\lambda) \not\equiv 0 \bmod(p)$ et donc D_λ et C_λ ont une réduction multiplicative. Montrons qu'elle est déployée si et seulement si $\mathrm{Norm}(p) \equiv 1 \bmod(5)$, pour cela soit

$$f(x,y) = y^2 + (1-\lambda)xy - \lambda y - x^3 + \lambda x^2.$$

Alors

$$\frac{\partial f}{\partial y}(x,y) = 2y + (1-\lambda)x - \lambda$$

et $\dfrac{\partial f}{\partial y}(\widetilde{P}) = -\lambda \neq 0$ dans k, donc $P = (0,0)$ se réduit en un point lisse. Si la réduction est déployée, alors $E^{sm}(k) \cong k^\star$ et comme $\widetilde{P} \in E^{sm}(k) \setminus \{O\}$ est un point d'ordre 5, alors $5 \mid |k^\star| = \mathrm{Norm}(p) - 1$, d'où $\mathrm{Norm}(p) \equiv 1(5)$.

Supposons maintenant que la réduction n'est pas déployée. Soient γ_1,γ_2 les pentes des tangentes à $\widetilde{D_\lambda}$ au point singulier et soit $k' = k(\gamma_1,\gamma_2)$. Alors k'/k est une extension galoisienne de degré 2, soit donc σ l'élément non-trivial de $\mathrm{Gal}(k'/k)$. Alors on a un isomorphisme de groupes abéliens:

$$\widetilde{D_\lambda}^{sm}(k) \xrightarrow{\sim} \{\frac{\omega}{\sigma\omega}, \omega \in (k')^\star\} = \ker\{\mathrm{N}_{k'/k} : (k')^\star \to k^\star\}$$

$$= \{1, \frac{\gamma_1}{\gamma_2}, \frac{1+\gamma_1}{1+\gamma_2}, \ldots, \frac{1+(\mathrm{Norm}\ p-1)\gamma_1}{1+(\mathrm{Norm}\ p-1)\gamma_2}\}$$

donc $|\widetilde{D_\lambda}^{sm}(k)| = \mathrm{Norm}(p) + 1$ d'où $5 \mid (\mathrm{Norm}(p) + 1)$ ce qui implique que $\mathrm{Norm}(p) \not\equiv 1 \bmod(5)$.

3. Evident.

Montrons le lemme pour $n = 7$. Soit p un premier de K avec $p \not| 7$ et soit $\lambda \in K_p$ avec $\mathrm{ord}_p(\lambda) \geq 0$.

. Si $p \not| \Delta(D_\lambda)$ (resp. $p \not| \Delta(C_\lambda)$), alors les équations de Weierstrass des courbes D_λ et C_λ sont minimales.

. Si $p|\lambda(\lambda-1)$ alors la division euclidienne de $c_4(D_\lambda)$ (resp. $c_4(C_\lambda)$) par $\lambda(\lambda-1)$ donne:

$$\begin{cases} c_4(D_\lambda) = \lambda(\lambda-1)(\lambda^6 - 11\lambda^5 + 31\lambda^4 - 25\lambda^3 + 10\lambda^2 + 10\lambda - 4) + 1 \\ \\ c_4(D_\lambda) = \lambda(\lambda-1)(\lambda^6 + 229\lambda^5 + 271\lambda^4 - 1465\lambda^3 + 1930\lambda^2 - 1430\lambda + 236) + 1 \end{cases}$$

donc $p \not| c_4(D_\lambda)$ (resp. $p \not| c_4(C_\lambda)$) d'où les équations sont minimales.

.Si $p \not| \lambda(\lambda-1)$ et $p|(\lambda^3-8\lambda^2+5\lambda+1)$ alors l'idéal $(c_4(D_\lambda),\lambda^3-8\lambda^2+5\lambda+1)$ (resp. $(c_4(C_\lambda),\lambda^3-8\lambda^2+5\lambda+1)$) de $\mathbf{Z}[\lambda]$ contient $5^2\times7^4\times59^2$ (resp. $5^2\times7^8\times59^2$), donc la réduction est multiplicative si $p \not| 5\times59$.

1. Si $\lambda(\lambda-1)\equiv 0(p)$, alors $p|\Delta(D_\lambda)$ et $p \not| c_4(D_\lambda)$ et donc les courbes D_λ et C_λ ont une réduction multiplicative, et comme dans le cas $n=5$ on a $\widetilde{D_\lambda}: y^2+xy=x^3$, donc la réduction est déployée.

2. Si $\lambda^3-8\lambda^2+5\lambda+1\equiv 0(p)$, alors $p|\Delta(D_\lambda)$ et $p \not| c_4(D_\lambda)$ et donc D_λ et C_λ ont une réduction multiplicative. Soit

$$f(x,y)=y^2+(1+\lambda-\lambda^2)xy+(\lambda^2-\lambda^3)y-x^3-(\lambda^2-\lambda^3)x^2,$$

alors

$$\frac{\partial f}{\partial y}(x,y)=2y+(1+\lambda-\lambda^2)x+(\lambda^2-\lambda^3)$$

d'où $\dfrac{\partial f}{\partial y}(\widetilde{P})=(\lambda^2-\lambda^3)\neq 0$ dans k, donc $P=(0,0)$ se réduit en un point lisse. De la même fan que pour $n=5$ on démontre que la réduction est déployée si et seulement si $\mathrm{Norm}(p)\equiv 1 \bmod(7)$.

3. Evident.

□

D'après le lemme (3.1.1.2), on peut toujours supposer $\mathrm{ord}_p(\lambda)\geq 0$. Il reste à décrire le type de réduction dans le cas $p \mid n$. On trouve que les cas 1. et 3. du lemme précédent sont les mêmes. Pour le deuxième cas, il n'est plus possible de traiter tous les corps de nombres en même temps. Si $K=\mathbf{Q}$, l'équation de Weierstrass (3.1) reste minimale et la réduction est additive. Mais l'équation de Weierstrass (3.2) n'est pas forcément minimale, précisément lorsque $\lambda\equiv 18 \bmod(25)$ (respectivement $\lambda\equiv 5 \bmod(7)$), par exemple pour $n=5$ et $\lambda=43$ on a $c_4(C_{43})=5^5\times 7184$ et $\Delta(C_{43})=43\times 11^5\times 5^{15}$.

3.1.2 Groupes de Selmer et torseurs

3.1.2.1 Définition

Soit T/K une courbe lisse. Le groupe d'isomorphismes de T, noté $\mathrm{Isom}(T)$, est le groupe des isomorphismes (définis sur $\overline{K}$) de la courbe T vers elle même. On note $\mathrm{Isom}_K(T)$ le sous groupe de $\mathrm{Isom}(T)$ des isomorphismes définis sur K (pour simplifier les notations on va noter la composition des applications par $\alpha\beta$ au lieu de $\alpha\circ\beta$).

3.1.2.2 Remarque

Le groupe qu'on a noté Isom(T) est généralement appelé le groupe des automorphismes de T, et est noté Aut(T). Mais, si E est une courbe elliptique, on a défini Aut(E) par le groupe des isomorphismes de E dans E qui envoient O vers O. Donc Isom(E) $\neq$ Aut(E), car par exemple, Isom(E) contient les translations $\tau_P : E \to E$.

3.1.2.3 Définition

Un twist de T/K est une courbe lisse T'/K qui est isomorphe à T sur $\overline{K}$. On identifie deux twists s'ils sont isomorphes sur K. L'ensemble des twists de T/K, modulo K-isomorphisme, est noté Twist(T/K).

3.1.2.4 Théorème

Soit T/K une courbe lisse. Pour tout twist T'/K de T/K, on choisit un isomorphisme $\phi : T' \to T$ et on définit une application

$$\xi : G_{\overline{K}/K} \to \mathrm{Isom}(T) \qquad \sigma \mapsto \xi_\sigma = \phi^\sigma \phi^{-1}.$$

1. ξ est un 1-cocycle. (i.e. Pour tous σ, $\tau \in G_{\overline{K}/K}$: $\xi_{\sigma\tau} = (\xi_\sigma)^\tau \xi_\tau$). On note sa classe de cohomologie dans $H^1(G_{\overline{K}/K}$,Isom(T)) par $\{\xi\}$.

2. La classe de cohomologie $\{\xi\}$ est déterminée par la classe de K-isomorphisme de T', indépendamment du choix de ϕ. On obtient ainsi une application naturelle
$$\mathrm{Twist}(T/K) \to H^1(G_{\overline{K}/K},\mathrm{Isom}(T)).$$

3. L'application dans 2. est une bijection. En d'autres termes, les twists de T/K (à K-isomorphisme près) sont en correspondance bijective avec les éléments du groupe de cohomologie $H^1(G_{\overline{K}/K}$,Isom(T)).

Preuve. voir [14] chapitre X théorème 2.2.

3.1.2.5 Définition

Soit E/K une courbe elliptique. Un torseur (ou un espace homogène) de E/K est une courbe lisse T/K avec une action simplement transitive μ de E sur T définie sur K. [i.e. Un torseur de E/K est une paire (T,μ), où T/K est une courbe lisse et

$$\mu : T \times E \to T$$

est un morphisme défini sur K vérifiant les propriétés suivantes:

1. $\mu(p,O) = p$ pour tout $p \in T(\overline{K})$.

2. $\mu(\mu(p,P),Q) = \mu(p,P+Q))$ pour tous $p \in T(\overline{K})$ et $P,Q \in E(\overline{K})$.

3. Pour tous $p,q \in T(\overline{K})$ il existe un unique $P \in E(\overline{K})$ vérifiant $\mu(p,P) = q$.]

Et on définit aussi:

$$\nu : T \times T \to E$$

$$\nu(p,q) = (\text{l'unique } P \in E \text{ tel que } \mu(p,P) = q) \quad .$$

3.1.2.6 Lemme

Soit E/K une courbe elliptique, et T/K un torseur de E/K. On fixe un point $p_0 \in T(\overline{K})$, et on définit une application

$$\theta : E \to T \qquad \theta(P) = \mu(p_0,P)$$

Alors θ est un isomorphisme défini sur $K(p_0)$. En particulier, T/K est un twist de E/K.

Preuve. voir [14] chapitre X proposition 3.2.

3.1.2.7 Définition

Deux torseurs T/K et T'/K de E/K sont équivalents s'il existe un isomorphisme $\theta : T \to T'$ défini sur K et compatible avec les actions de E sur T et T'. [En d'autres termes, pour tous $p \in T(\overline{K})$ et $P \in E(\overline{K})$,

$$\theta(\mu(p,P)) = \mu(\theta(p),P).]$$

La classe d'équivalence contenant E, agissant sur elle même par translation, est appelée la classe triviale. La collection des classes d'équivalences des torseurs de E/K est appelée le groupe de Weil-Châtelet de E/K, et est noté $WC(E/K)$. (On dira plus loin pourquoi c'est un groupe abélien.)

3.1.2.8 Proposition

Soit T/K un torseur de E/K. Alors T/K est dans la classe triviale si est seulement si $T(K)$ est non vide.

Preuve. voir [14] chapitre X proposition 3.3.

3.1.2.9 Théorème

Soit E/K une courbe elliptique. Il existe une bijection naturelle

$$WC(E/K) \to H^1(G_{\overline{K}/K},E)$$

définie comme suit:

Soit T/K un torseur de E/K, on choisit un point quelconque $p_0 \in T(\overline{K})$. Alors

$$\{T/K\} \mapsto \{\sigma \mapsto \nu(p_0^\sigma,p_0)\}.$$

Preuve. voir [14] chapitre X théorème 3.6.

3.1.2.10 Remarque

Comme $H^1(G_{\overline{K}/K},E)$ est un groupe abélien, le théorème (3.1.2.9) définit une structure de groupe abélien sur l'ensemble $WC(E/K)$.

Supposons maintenant qu'on a deux courbes elliptiques E/K et E'/K et une isogénie non-nulle $\phi : E \to E'$ définie sur K. Alors on a une suite exacte de $G_{\overline{K}/K}$-modules

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0 \tag{3.3}$$

où l'on a noté par $E[\phi]$ le noyau de ϕ. En prenant la cohomologie galoisienne on trouve la suite exacte longue:

$$\begin{aligned} 0 \to E(K)[\phi] \to E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(G_{\overline{K}/K},E[\phi]) \\ \to H^1(G_{\overline{K}/K},E) \to H^1(G_{\overline{K}/K},E') \end{aligned} \tag{3.4}$$

et de cette suite exacte on forme la suite exacte courte:

$$0 \to E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(G_{\overline{K}/K},E[\phi]) \to H^1(G_{\overline{K}/K},E)[\phi] \to 0. \tag{3.5}$$

Notons que le théorème (3.1.2.9) nous dit que $H^1(G_{\overline{K}/K},E)[\phi]$ est identifié à $WC(E/K)[\phi]$.

Comme il est expliqué dans [14], on a de même pour tout $\vartheta \in M_K$ une suite exacte courte:

$$0 \to E'(K_\vartheta)/\phi(E(K_\vartheta)) \xrightarrow{\delta} H^1(G_\vartheta,E[\phi]) \to H^1(G_\vartheta,E)[\phi] \to 0 \qquad (3.6)$$

et on a aussi le diagramme commutatif suivant (où l'on a remplacé chaque $H^1(G,E)$ par le groupe de Weil-Châtelet correspondant et où les lignes sont exactes):

$$\begin{array}{ccccccc} 0 \to & \dfrac{E'(K)}{\phi(E(K))} & \to & H^1(G_{\overline{K}/K},E[\phi]) & \to & WC(E/K)[\phi] & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & \displaystyle\prod_{\vartheta\in M_K} \dfrac{E'(K_\vartheta)}{\phi(E(K_\vartheta))} & \to & \displaystyle\prod_{\vartheta\in M_K} H^1(G_\vartheta,E[\phi]) & \to & \displaystyle\prod_{\vartheta\in M_K} WC(E/K_\vartheta)[\phi] & \to 0 \end{array}$$

3.1.2.11 Définition

Soit $\phi : E/K \to E'/K$ une isogénie. Le groupe de Selmer de E/K par rapport à ϕ est le sous groupe de $H^1(G_{\overline{K}/K},E[\phi])$ défini par

$$S^\phi(E/K) = \ker\{H^1(G_{\overline{K}/K},E[\phi]) \to \prod_{\vartheta\in M_K} WC(E/K_\vartheta)\}.$$

Le groupe de Tate-Shafarevich de E/K est le sous groupe de $WC(E/K)$ défini par

$$\text{Ш}(E/K) = \ker\{WC(E/K) \to \prod_{\vartheta\in M_K} WC(E/K_\vartheta)\}.$$

3.1.2.12 Théorème

Soit ϕ une isogénie de courbes elliptiques $\phi : E/K \to E'/K$ définie sur K.

1. Il existe une suite exacte

$$0 \to E'(K)/\phi E(K) \to S^\phi(E/K) \to \text{Ш}(E/K)[\phi] \to 0.$$

2. Le groupe de Selmer $S^{\phi}(E/K)$ est fini.

Preuve. voir [14] chapitre X théorème 4.2.

D'après (1.1),(3.3),(3.4) et (3.5) on a la suite exacte suivante:

$$0 \to D_\lambda(K)/\phi(C_\lambda(K)) \xrightarrow{\delta} H^1(G_{\overline{K}/K},\mu_n) \to WC(C_\lambda/K)[\phi] \to 0. \tag{3.7}$$

Et d'après (3.7) et la proposition (2.2.2.5) on a

$$S^{\phi}(C_\lambda/K) \cong \{\theta \in K^\star/(K^\star)^n : C_{\lambda,\theta}(K_p) \neq \emptyset, \quad \text{pour tout premier } p\} \tag{3.8}$$

où $C_{\lambda,\theta}$ désigne le torseur de C_λ qui correspond à $\theta \in K^\star/(K^\star)^n$. Notons que comme n est impair, on peut ignorer les places infinies. On donne des équations pour les courbes $C_{\lambda,\theta}$ de deux méthodes différentes, la méthode "push-out" et la méthode de "l'espace projectif".

Equations via push-out.

Soient C_λ et D_λ données par (3.1) et (3.2). On note par $\mathbf{1}$ le générateur de $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda(K)$. On fait de sorte que $\mu_n \hookrightarrow C_\lambda$ vérifie $e_\phi(\zeta,\mathbf{1}) = \zeta$ pour tout $\zeta \in \mu_n$, où e_ϕ désigne l'accouplement de Weil, comme il est défini dans [14] chapitre III exercice 3.15.

3.1.2.13 Lemme

Soit $f \in K(D_\lambda)$ tel que $\mathrm{div}(f) = n.\mathbf{1} - n.0$, quitte à multiplier f par un élément de $K^\star$, on peut supposer que $f \circ \phi = g^n$ pour un $g \in K(C_\lambda)$. Alors l'application δ suivante:

$$0 \to \mu_n(K) \to C_\lambda(K) \xrightarrow{\phi} D_\lambda(K) \xrightarrow{\delta} K^\star/(K^\star)^n$$

est donnée par $\delta(P) = f(P) \bmod (K^\star)^n$, pour $P \neq 0,\mathbf{1}$.

Preuve. voir [5] lemme 1.4.

Soit D_λ d'équation de Weierstrass (3.1) et soit $\mathbf{1} = (0,0)$. Alors f est donnée

par:

$$\begin{aligned} n = 5 \quad & f(x,y) = xy + y - x^2 \\ n = 7 \quad & f(x,y) = (\lambda+1)x^3 - x^2y + \lambda^2x^2 - (2\lambda+1)xy - \lambda^2 y. \end{aligned} \tag{3.9}$$

Equation dans l'espace projectif.

Soit D un diviseur sur une courbe elliptique, on rappele que (voir [14], chapitre III):

$$D \sim 0 \Leftrightarrow \deg D = 0 \text{ et sum } D = 0. \tag{3.10}$$

Donc si on plonge $E \hookrightarrow \mathbf{P}^{n-1}$ grâce à un système linéaire complet de degré n alors la translation τ_P se prolonge en un automorphisme de $\mathbf{P}^{n-1}$ si et seulement si $P \in E[n]$.

Soit maintenant $T \hookrightarrow \mathbf{P}^{n-1}$ une courbe lisse de genre 1 et de degré n. On sous-entend toujours que T est plongée grâce à un système linéaire complet, ce qui équivaut à dire que T n'est contenue dans aucun hyperplan. L'action de $\mathrm{Jac}(T)$ sur T détermine une action de $G_{\overline{K}/K}$-modules $\mathrm{Jac}(T)[n] \hookrightarrow \mathrm{PGL}_n$.

Supposons que T est un torseur de C_λ avec $\xi_T \in WC(C_\lambda/K)[\phi]$. On sait que $\mu_n \hookrightarrow C_\lambda$ agit sur T et que le quotient $U = T/\mu_n$ est un torseur de $D_\lambda = C_\lambda/\mu_n$. Alors on a:

$$\phi : WC(C_\lambda/K) \to WC(D_\lambda/K); \qquad \xi_T \mapsto \xi_U = 0.$$

En choisissant un point dans $U(K)$ on obtient un diviseur de degré n sur T et donc un plongement $T \hookrightarrow \mathbf{P}^{n-1}$. Comme expliqué ci-dessus, $\mu_n \hookrightarrow C_\lambda$ se prolonge en une action sur $\mathbf{P}^{n-1}$. Géométriquement, il existe exactement n hyperplans fixés par cette action. Ils correspondent au choix du point dans $U(K)$ et ses translatés sous $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda$. En particulier, ces hyperplans sont définis sur K, donc pour un bon choix de coordonnées dans $\mathbf{P}^{n-1}$, l'action de $\mu_n \hookrightarrow \mathrm{PGL}_n$ est donnée par

$$\zeta \mapsto (1 : \zeta : ... : \zeta^{n-1}). \tag{3.11}$$

Donc les torseurs $C_{\lambda,\theta}$ se présentent comme des courbes lisses de genre 1 et de degré n dans $\mathbf{P}^{n-1}$. Inversons l'argument précédent pour montrer que toutes les courbes qu'on obtient sont de la forme $C_{\lambda,\theta}$.

Soit T une courbe lisse de genre 1 et de degré n dans $\mathbf{P}^{n-1}$ invariante sous l'action de μ_n donnée par (3.11). Comme n est premier à 6, on sait que $\mu_n \hookrightarrow \mathrm{Jac}(T)$ et donc $\mathrm{Jac}(T) \cong C_\lambda$ pour un $\lambda \in K$. Maintenent, T est un torseur de C_λ et $U := T/\mu_n$ est un torseur de D_λ. Mais l'intersection de T avec un des hyparplans est une orbite de μ_n définie globalement sur K. Donc U est trivial comme torseur de D_λ et $\xi_T \in WC(C_\lambda/K)[\phi]$. D'après la suite exacte (3.7) il vient que $T \cong C_{\lambda,\theta}$ pour un $\theta \in K^\star/(K^\star)^n$.

3.1.3 Le théorème de descente

Soit $n = 5$ (respectivement $n = 7$) et $\lambda \in \mathbf{Q}$ avec $\lambda \neq 0$ (respectivement $\lambda \neq 0{,}1$). On considère les courbes elliptiques C_λ et D_λ définies par (3.1) et (3.2). Dans chaque cas $\mathbf{Z}/n\mathbf{Z} \mapsto D_\lambda$ est engendré par $(x,y) = (0,0)$ et la courbe isogène C_λ est définie comme le quotient de D_λ par $\mathbf{Z}/n\mathbf{Z}$. On écrit $\phi : C_\lambda \to D_\lambda$ pour l'isogénie de degré n avec $C[\phi] \cong \mu_n$ et $D[\widehat{\phi}] \cong \mathbf{Z}/n\mathbf{Z}$. Dans cette section on annonce les résultats principaux qui servent à décrire les groupes de Selmer $S^\phi(C_\lambda/\mathbf{Q})$ et $S^{\widehat{\phi}}(D_\lambda/\mathbf{Q})$.

On note par

$$n = 5 \begin{cases} \alpha(\lambda) = \lambda \\ \\ \beta(\lambda) = \lambda^2 - 11\lambda - 1 \end{cases}$$

$$n = 7 \begin{cases} \alpha(\lambda) = \lambda^4(\lambda - 1) \\ \\ \beta(\lambda) = \lambda^3 - 8\lambda^2 + 5\lambda + 1. \end{cases}$$

Les zéros de ces polynômes sont des pointes de $X_1(n)$. On définit deux ensembles disjoints de premiers rationnels par:

$$\mathcal{A} = \{p \ \text{ premier} | \ \mathrm{ord}_p(\lambda) < 0 \text{ ou } \alpha(\lambda) \equiv 0 \bmod(p)\}$$

$$\mathcal{B} = \left\{ p \text{ premier} \left| \begin{array}{ll} \beta(\lambda) \equiv 0 \bmod(p) \text{ et } p \equiv 1 \bmod(n) \\ \\ \text{ou} \quad p = n = 5 \text{ et } \lambda \equiv 18 \bmod(25) \\ \\ \text{ou} \quad p = n = 7 \text{ et } \lambda \equiv 5 \bmod(7) \end{array} \right. \right\}.$$

Pour S un ensemble de premiers rationnels, on écrit $[S]$ pour le sous espace de $\mathbf{Q}^\star/(\mathbf{Q}^\star)^n$ engendré par S. Pour un accouplement Ξ d'espaces vectoriels sur $\mathbf{Z}/n\mathbf{Z}$ on écrit $\ker_G(\Xi)$ et $\ker_D(\Xi)$ pour les noyaux à gauche et à droite.

3.1.3.1 Théorème

Soit $n = 5{,}7$ et $\lambda \in \mathbf{Q}$ avec $\lambda \neq 0$, respectivement $\lambda \neq 0{,}1$. Soient $\mathcal{A}$ et $\mathcal{B}$ les ensembles de premiers rationnels définis précédemment. Alors le groupe de Selmer par rapport à l'isogénie $\phi : C_\lambda \to D_\lambda$ est donné par

$$S^\phi(C_\lambda/\mathbf{Q}) \cong \{\theta \in [\mathcal{A}] : \theta \in (\mathbf{Q}_p^\star)^n \quad \text{pour tout } p \in \mathcal{B}\}.$$

La contribution à $S^\phi(C_\lambda/\mathbf{Q})$ qui provient de $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda$ est engendrée par $\alpha(\lambda)$.

En outre, il existe un accouplement $\Xi : [\mathcal{A}] \times [\mathcal{B}] \to \mathbf{Z}/n\mathbf{Z}$ tel que

$$S^\phi(C_\lambda/\mathbf{Q}) = \ker_G(\Xi) \quad \text{et} \quad S^{\widehat{\phi}}(D_\lambda/\mathbf{Q}) = \ker_D(\Xi).$$

3.1.3.2 Lemme

Pour un premier rationnel p, la congruence $\beta(\lambda) \equiv 0(p)$ est soluble si et seulement si $p = n$ ou $p \equiv \pm 1(n)$.

Preuve

(i) Soit $n = 5$ et $p \neq 2{,}5$

$$\begin{aligned}
\beta(\lambda) \equiv 0 \bmod(p) &\Leftrightarrow \lambda^2 - 11\lambda - 1 \equiv 0 \bmod(p) \\
&\Leftrightarrow (2\lambda - 11)^2 \equiv 125 \bmod(p) \\
&\Leftrightarrow (125/p) = 1 \\
&\Leftrightarrow (5/p) = 1 \\
&\Leftrightarrow p \equiv \pm 1 \bmod(5).
\end{aligned}$$

Pour $p = 5$ on a

$$\begin{aligned}\beta(\lambda) \equiv 0 \bmod(5) &\Leftrightarrow \lambda^2 - 11\lambda - 1 \equiv 0 \bmod(5)\\ &\Leftrightarrow (\lambda+7)(\lambda-18)+125 \equiv 0 \bmod(5)\\ &\Leftrightarrow (\lambda+2)^2 \equiv 0 \bmod(5)\\ &\Leftrightarrow \lambda+2 \equiv 0 \bmod(5)\\ &\Leftrightarrow \lambda \equiv 3 \bmod(5).\end{aligned}$$

Pour $p = 2$ on remplace $\lambda = 0{,}1$ on trouve $1 \equiv 0 \bmod(2)$ ce qui est impossible.

(*ii*) Soit $n = 7$ et $p \neq 7$.

Les racines de $\beta(\lambda)$ sont le réel $\lambda = -(\zeta-\zeta^6)(\zeta^4-\zeta^3)^2/(\zeta^2-\zeta^5)^3$ et ses conjugués, où ζ est une racine 7^{eme} de l'unité. L'extension $\mathbf{Q}(\lambda)/\mathbf{Q}$ est galoisienne de degré 3. Donc cela revient à voir comment p se décompose dans $\mathbf{Q}(\lambda) = \mathbf{Q}(\mu_7) \cap \mathbf{R}$. On trouve que p se décompose en produit de trois idéaux premiers distincts de $\mathbf{Q}(\mu_7) \cap \mathbf{R}$ si et seulement si $p \equiv \pm 1 \bmod(7)$.

Pour $p = 7$ on a

$$\begin{aligned}\beta(\lambda) \equiv 0 \bmod(7) &\Leftrightarrow \lambda^3 - 8\lambda^2 + 5\lambda + 1 \equiv 0 \bmod(7)\\ &\Leftrightarrow (\lambda+2)(\lambda-5)^2 - 49 \equiv 0 \bmod(7)\\ &\Leftrightarrow (\lambda+2)^2 \equiv 0 \bmod(7)\\ &\Leftrightarrow \lambda+2 \equiv 0 \bmod(7)\\ &\Leftrightarrow \lambda \equiv 5 \bmod(7).\end{aligned}$$

□

Comme $\lambda^2-11\lambda-1 = (\lambda+7)(\lambda-18)+125$ et $\lambda^3-8\lambda^2+5\lambda+1 = (\lambda+2)(\lambda-5)^2-49$, la condition pour que $n \in \mathcal{B}$ est $\beta(\lambda) \equiv 0 \bmod(125)$, respectivement $\beta(\lambda) \equiv 0 \bmod(49)$, c'est aussi la condition pour que l'équation (3.2) ne soit pas minimale d'après ce qu'on a vu dans la section (3.1.1).

3.1.3.3 Lemme

Soient G,H et K des groupes abéliens et soient $f : G \to H$ et $g : H \to K$ deux homomorphismes de groupes abéliens . On a la suite exacte suivante

$$0 \to \ker(f) \xrightarrow{i} \ker(gf) \xrightarrow{\widetilde{f}} \ker(g) \xrightarrow{\delta} \mathrm{coker}(f) \xrightarrow{\bar{g}} \mathrm{coker}(gf) \xrightarrow{\bar{p}} \mathrm{coker}(g) \to 0$$

où i désigne l'injection canonique, $\bar{p}$ la projection canonique, $\widetilde{f}$ la restriction de f à $\ker(gf)$, δ et $\bar{g}$ sont définis par:

$$\delta(x) = x + \mathrm{Im}(f) \qquad \text{pour tou } x \in \ker(g)$$

$$\bar{g}(x + \mathrm{Im}(f)) = g(x) + \mathrm{Im}(gf) \qquad \text{pour tout } x \in H.$$

3.1.4 Quelques exemples

Soit $n = 5$ ou 7 et $\lambda \in \mathbf{Q}$ avec $\lambda \neq 0$, respectivement $\lambda \neq 0, 1$. Le théorème (3.1.3.1) nous donne des informations sur les groupes de Mordell-Weil $C_\lambda(\mathbf{Q})$ et $D_\lambda(\mathbf{Q})$ et sur les groupes de Tate-Shafarevich $\coprod(C_\lambda/\mathbf{Q})$ et $\coprod(D_\lambda/\mathbf{Q})$. D'après la classification de Mazur des groupes de torsion des courbes elliptiques sur $\mathbf{Q}$ on trouve:

$$D_\lambda(\mathbf{Q})_{tors} = \begin{cases} \mathbf{Z}/5\mathbf{Z} \text{ ou } \mathbf{Z}/10\mathbf{Z} & \text{si } n = 5 \\ \mathbf{Z}/7\mathbf{Z} & \text{si } n = 7. \end{cases}$$

Soit r =rang $C_\lambda(\mathbf{Q})$ =rang $D_\lambda(\mathbf{Q})$ et i =$\dim_n C_\lambda(\mathbf{Q})[n]$. D'après le lemme (3.1.3.3) on a une suite exacte:

$$0 \to \ker(\phi) \to \ker(\widehat{\phi}\phi) \to \ker(\widehat{\phi}) \to \mathrm{coker}(\phi) \to \mathrm{coker}(\widehat{\phi}\phi) \to \mathrm{coker}(\widehat{\phi}) \to 0$$

i.e.

$$\begin{aligned} 0 \to C_\lambda(\mathbf{Q})[\phi] \to C_\lambda(\mathbf{Q})[n] \to D_\lambda(\mathbf{Q})[\widehat{\phi}] \to D_\lambda(\mathbf{Q})/\phi C_\lambda(\mathbf{Q}) \\ \to C_\lambda(\mathbf{Q})/nC_\lambda(\mathbf{Q}) \to C_\lambda(\mathbf{Q})/\widehat{\phi}D_\lambda(\mathbf{Q}) \to 0. \end{aligned} \tag{3.12}$$

On a $\dim_n C_\lambda(\mathbf{Q})[\phi] = 0$ (car $C_\lambda(\mathbf{Q})[\phi] = \{O\}$) et $\dim_n C_\lambda(\mathbf{Q})/nC_\lambda(\mathbf{Q}) = r + i$, et de la suite exacte (3.12) on déduit:

$$\dim_n D_\lambda(\mathbf{Q})/\phi C_\lambda(\mathbf{Q}) + \dim_n C_\lambda(\mathbf{Q})/\widehat{\phi} D_\lambda(\mathbf{Q}) = r + 1. \tag{3.13}$$

Les suites exactes

$$\begin{aligned} 0 \to D_\lambda(\mathbf{Q})/\phi C_\lambda(\mathbf{Q}) \to S^\phi(C_\lambda/\mathbf{Q}) \to \text{Ш}(C_\lambda/\mathbf{Q})[\phi] \to 0 \\ 0 \to C_\lambda(\mathbf{Q})/\widehat{\phi} D_\lambda(Q) \to S^{\widehat{\phi}}(D_\lambda/\mathbf{Q}) \to \text{Ш}(D_\lambda/Q)[\widehat{\phi}] \to 0 \end{aligned} \tag{3.14}$$

nous donnent

$$\dim_n S^\phi(C_\lambda/\mathbf{Q}) = |\mathcal{A}| - \text{rang}(\Xi) = \dim_n D_\lambda(\mathbf{Q})/\phi C_\lambda(\mathbf{Q}) + \dim_n \text{Ш}(C_\lambda/\mathbf{Q})[\phi]$$

$$\dim_n S^{\widehat{\phi}}(D_\lambda/\mathbf{Q}) = |\mathcal{B}| - \text{rang}(\Xi) = \dim_n C_\lambda(\mathbf{Q})/\widehat{\phi} D_\lambda(\mathbf{Q}) + \dim_n \text{Ш}(D_\lambda/\mathbf{Q})[\widehat{\phi}]$$

et donc:

$$\begin{aligned} |\mathcal{A}| + |\mathcal{B}| - 2\text{rang}(\Xi) = &\dim_n D_\lambda(\mathbf{Q})/\phi C_\lambda(\mathbf{Q}) + \dim_n C_\lambda(\mathbf{Q})/\widehat{\phi} D_\lambda(\mathbf{Q}) \\ &+ \dim_n \text{Ш}(C_\lambda/\mathbf{Q})[\phi] + \dim_n \text{Ш}(D_\lambda/\mathbf{Q})[\widehat{\phi}] \end{aligned}$$

d'où l'on en déduit notre borne supérieure pour le rang de Mordell-Weil qui est

$$|\mathcal{A}| + |\mathcal{B}| - 1 - 2 \text{ rang}(\Xi). \tag{3.15}$$

Pour les exemples suivants on aura besoin des suites exactes suivantes:

$$\begin{aligned} 0 \to \text{Ш}(C_\lambda/\mathbf{Q})[\phi] \to \text{Ш}(C_\lambda/\mathbf{Q})[n] \to \text{Ш}(D_\lambda/\mathbf{Q})[\widehat{\phi}] \\ 0 \to \text{Ш}(D_\lambda/\mathbf{Q})[\widehat{\phi}] \to \text{Ш}(D_\lambda/\mathbf{Q})[n] \to \text{Ш}(C_\lambda/\mathbf{Q})[\phi] \end{aligned} \tag{3.16}$$

3.1.4.1 Exemple

Soit $n = 5$ et $\lambda = 38 = 2 \times 19$, alors $\alpha(\lambda) = 38$ et $\beta(\lambda) = 1025 = 5^2 \times 41$ d'où $\mathcal{A} = \{\text{p premier} : p \mid 38\} = \{2,19\}$ et comme $41 \equiv 1(5)$ alors $\mathcal{B} = \{41\}$. Et donc

$$[\mathcal{A}] = \{2^i.19^j, 0 \leq i,j \leq 4\} \qquad \text{et} \qquad [\mathcal{B}] = \{41^i, 0 \leq i \leq 4\}.$$

Comme $5 \mid 40$, alors $\mu_5 \subset \mu_{40} \subset \mathbf{Q}_{41}$ et pour tout $0 \leq i,j \leq 4$ on a $2^i.19^j \in \mathbf{Z}_{41}^\star$, considérons donc l'accouplement suivant défini par le symbole de Legendre (pour plus de détails sur ce symbole voir [12] chapitre III section 5)

$$\Xi : [\mathcal{A}] \times [\mathcal{B}] \to \mu_5 \qquad (a,b) \mapsto (a,b)_{41,5} = (a/41)_5^{\mathrm{ord}_{41}(b)}$$

avec $(a/41)_5 \equiv a^{\frac{41-1}{5}}(41) \equiv a^8(41)$. Montrons que $\mathrm{rang}(\Xi) = 1$. Comme 2 et 19 engendrent $[\mathcal{A}]$ et 41 engendre $[\mathcal{B}]$, il suffit de montrer que $\Xi(2,41) \neq 1$. Supposons par l'absurde que $\Xi(2,41) = 1$, alors on aurra $1 = \Xi(2,41) = (2,41)_{41,5} = (2/41)_5^{\mathrm{ord}_{41}(41)} \equiv 2^8(41)$, ce qui nous donne $2^8 = 256 = 5 \times 51 + 1 \equiv 1(41)$ contradiction. Donc $\mathrm{rang}(\Xi) = 1$, d'où $|\mathcal{A}| + |\mathcal{B}| - 1 - 2\mathrm{rang}(\Xi) = 0$, ce qui implique $r = 0$. On en déduit que $C_{38}(\mathbf{Q}) = 0$, $D_{38}(\mathbf{Q}) = \mathbf{Z}/5\mathbf{Z}$ et $\coprod(C_{38}/\mathbf{Q})[5] = \coprod(D_{38}/\mathbf{Q})[5] = 0$.

3.1.4.2 Exemple

Soit $n = 7$ et $\lambda = 8$. Donc $\mathcal{A} = \{2,7\}$ et $\mathcal{B} = \emptyset$ ce qui donne $\mathrm{rang}(\Xi) = 0$. A l'aide de "mwrank" on trouve un point $(x,y) = (30,198)$ d'ordre infini dans D_8. D'où $C_8(\mathbf{Q}) = \mathbf{Z}$, $D_8(\mathbf{Q}) = \mathbf{Z}/7\mathbf{Z} \times \mathbf{Z}$ et $\coprod(C_8/\mathbf{Q})[7] = \coprod(D_8/\mathbf{Q})[7] = 0$.

On peut utiliser le théorème (3.1.3.1) avec le programme de Cremona "mwrank" pour exhiber quelques éléments du groupe de Tate-Shafarevich. Ces éléments sont explicites dans le sens qu'on est capable de donner des équations dans $\mathbf{P}^{n-1}$ pour les courbes correspondantes qui ne respectent pas le principe de Hasse.

3.1.4.3 Exemple

Soit $n = 5$ et $\lambda = -60, -42, -30, 30, 60$ ou 90. Dans tous ces cas on a $|\mathcal{A}| = 3$ et $\mathcal{B} = \emptyset$. A l'aide de "mwrank" on trouve rang $D_\lambda(\mathbf{Q}) = 0$. On a, d'après le théorème (3.1.3.1), $\dim_5 S^{\widehat{\phi}}(D_\lambda/\mathbf{Q}) = |\mathcal{B}| - \mathrm{rang}(\Xi) = 0$, et la 2^{eme} suite exacte de (3.14) nous donne $\dim_5 \coprod(D_\lambda/\mathbf{Q})[\widehat{\phi}] = \dim_5 C_\lambda(\mathbf{Q})/\widehat{\phi}D_\lambda(\mathbf{Q}) = 0$. La première suite exacte de (3.14) et (3.13) nous donnent $\dim_5 \coprod(C_\lambda/\mathbf{Q})[\phi] = |\mathcal{A}| - 1 = 2$, d'après (3.16) $\dim_5 \coprod(C_\lambda/\mathbf{Q})[\phi] = \dim_5 \coprod(C_\lambda/\mathbf{Q})[5] = 2$. D'où l'on en déduit $\coprod(C_\lambda/\mathbf{Q})[5] \cong (\mathbf{Z}/5\mathbf{Z})^2$.

3.1.4.4 Exemple

Soit $n = 7$ et $\lambda = -6, -5, 6, 7, 10$ ou 11. Dans tous ces cas on a $|\mathcal{A}| = 3$ et $\mathcal{B} = \emptyset$. A l'aide de "mwrank" on trouve rang $D_\lambda(\mathbf{Q}) = 0$, et en utilisant le théorème (3.1.3.1) on trouve (comme dans l'exemple précédent) $\coprod(C_\lambda/\mathbf{Q})[7] \cong (\mathbf{Z}/7\mathbf{Z})^2$.

On donne maintenant quelques exemples de groupes non triviaux $\coprod$ pour des courbes elliptiques de rang de Mordell-Weil positif.

3.1.4.5 Exemple

Soit $n = 5$ et $\lambda = \pm 30/7, \pm 35/6, \pm 14/15$. Dans tous ces cas $\mathcal{A} = \{2,3,5,7\}$ et $\mathcal{B} = \emptyset$. A l'aide de "mwrank" on trouve $\text{rang} D_\lambda(\mathbf{Q}) = 1$, et en utilisant le théorème (3.1.3.1) on trouve: $\text{Ш}(C_\lambda/\mathbf{Q})[5] \cong (\mathbf{Z}/5\mathbf{Z})^2$.

3.2 Quelques résultats géométriques

3.2.1 La géométrie d'une courbe elliptique

Soit K un corps algébriquement clos et n un entier ≥ 3. On suppose que $\text{car}(K) \not| \, n$ et on fixe une racine primitive n^{eme} de l'unité $\zeta = \zeta_n$.

3.2.1.1 Définition

1. Une courbe elliptique normale de degré n est une courbe elliptique $E \hookrightarrow \mathbf{P}^{n-1}$ de degré n qui n'est contenue dans aucun hyperplan.

2. Un polygone de Néron de degré n est une collection de n droites $l_0,...,l_{n-1} \in \mathbf{P}^{n-1}$ qui ne sont contenues dans aucun hyperplan et arrangées de sorte que l_i rencontre l_j si et seulement si $i - j \equiv \pm 1 \mod (n)$.

3.2.1.2 Lemme

Soit $E \hookrightarrow \mathbf{P}^{n-1}$ une courbe elliptique normale ou un polygone de Néron. Alors E est contenue dans $n(n-3)/2$ quadriques et pour $n \geq 4$ ces quadriques sont suffisantes pour définir E.

Preuve. voir [5] lemme 2.2.

La courbe modulaire $Y(n) = X(n) \setminus \{\text{les pointes}\}$ paramétrise les triplets (E,P,Q) où E est une courbe elliptique et $P,Q \in E[n]$ satisfont $e_n(P,Q) = \zeta_n$. Notons qu'il existe une action de μ_n sur $X(n)$ donnée par

$$\zeta_n : (E,P,Q) \to (E,P,Q+P) \tag{3.17}$$

de quotient $X_1(n)$.

3.2.1.3 Proposition

Soit (E,P,Q) comme ci-dessus. Si on plonge $E \hookrightarrow \mathbf{P}^{n-1}$ grâce à un système linéaire complet, alors on peut choisir des coordonnées dans $\mathbf{P}^{n-1}$ telles que les

translations τ_P et τ_Q soient données par:

$$M_P := \begin{pmatrix} 1 & 0 & 0 & ... & 0 \\ 0 & \zeta & 0 & ... & 0 \\ 0 & 0 & \zeta^2 & ... & 0 \\ . & . & . & & . \\ . & . & . & & . \\ . & . & . & & . \\ 0 & 0 & 0 & ... & \zeta^{n-1} \end{pmatrix} \qquad M_Q := \begin{pmatrix} 0 & 0 & ... & 0 & 1 \\ 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ . & . & & . & . \\ . & . & & . & . \\ . & . & & . & . \\ 0 & 0 & ... & 1 & 0 \end{pmatrix}$$

Preuve. voir [5] proposition 2.3.

3.2.1.4 Proposition

Soit n un entier impair ≥ 3 et soit (E,P,Q) comme ci-dessus. Si on plonge $E \hookrightarrow \mathbf{P}^{n-1}$ grâce à un système linéaire complet $|D|$ avec $[-1]^\star D \sim D$ alors il existe un unique choix de coordonnées dans $\mathbf{P}^{n-1}$ telles que τ_P,τ_Q et $[-1]$ sont données par M_P,M_Q et:

$$[-1] := \begin{pmatrix} 1 & 0 & ... & 0 & 0 \\ 0 & 0 & ... & 0 & 1 \\ 0 & 0 & ... & 1 & 0 \\ . & . & & . & . \\ . & . & & . & . \\ . & . & & . & . \\ 0 & 1 & ... & 0 & 0 \end{pmatrix}$$

Preuve. voir [5] proposition 2.4.

On se restreint à n impair ≥ 5, de sorte que E soit définie par des quadriques. Soit (E,P,Q) un triplet comme ci-dessus, on plonge $E \hookrightarrow \mathbf{P}^{n-1}$ via le système linéaire complet $|n.0|$ et on choisit des coordonnées comme dans la proposition (3.2.1.4). Alors (E,P,Q) est déterminé de manière unique par les coordonnées de $0 \in \mathbf{P}^{n-1}$. En effet, en se donnant les coordonnées de ce point, l'action de M_P et M_Q nous permet de trouver n^2 points de E, et comme E est définie par des quadriques alors d'après le théorème de Bezout, ces quadriques sant suffisantes pour déterminer E. Ainsi, la procédure précédante donne un plongement $X(n) \hookrightarrow \mathbf{P}^{n-1}$. On va décrire l'image de cette application dans les cas $n = 5$ et $n = 7$. On écrit x_0,x_1,...,x_{n-1} pour les coordonnées dans $\mathbf{P}^{n-1}$ et on suppose que tous les indices sont modulo n. Notre hypothèse n est impair nous dit

$$n.0 \sim 0 + P + 2P + ... + (n-1)P. \tag{3.18}$$

donc 0 appartient à un seul des hyperplans fixés par M_P. Mais 0 est fixé par $[-1]$, donc on a l'un des cas suivants:

$$\begin{array}{ll} 0 = (0 : a_1 : a_2 : ... : a_2 : a_1) & (+) \\ 0 = (0 : a_1 : a_2 : ... : -a_2 : -a_1) & (-) \end{array}$$

avec a_1,...,$a_{(n-1)/2}$ non nuls. On concidère les espaces vectoriels suivants:

$$V := H^0(\mathbf{P}^{n-1},\mathcal{I}_E(2)) \subset W := H^0(\mathbf{P}^{n-1},\mathcal{O}_{\mathbf{P}^{n-1}}(2)) = \langle x_i x_j, 0 \leq i,j \leq (n-1)\rangle.$$

L'action de M_P nous permet d'écrire V et W sous forme de sommes directes $V = \oplus_i V_i$ et $W = \oplus_i W_i$ avec $V_i \subset W_i = \langle x_i^2, x_{i-1}x_{i+1}, ...\rangle$. Comme n est impair, on en déduit de l'action de M_Q que $\dim V_i = (n-3)/2$ et $\dim W_i = (n+1)/2$. Le point 0 et ses translatés sous l'action de M_Q impose quelques conditions de linéarité sur les coefficients des quadriques de V_0. Cela nous mène à exclure le cas $(+)$ et de donner la définition suivante.

3.2.1.5 Définition

Soit n impair ≥ 5, et soit $A(n) \subset \mathbf{P}^{n-1}$ le sous schéma défini par

$$a_0 = 0,\ a_{n-i} = -a_i \quad \text{et} \quad \operatorname{rang}(a_{i-j}a_{i+j})_{i,j=0}^{n-1} \leq 2. \tag{3.19}$$

La construction précédente montre que $X(n) \subset A(n)$. En fait, pour tout premier p on a, d'après le théorème de Vélu, $X(p) = A(p)$. En d'autres termes, les quadriques (3.19) suffisent pour définir $X(p)$.

3.2.1.6 Equations pour $X(5)$.

Soit $0 = (o : a : b : -b : -a)$. La variété $A(5)$ est définie par

$$\operatorname{rang} \begin{pmatrix} 0 & -a^2 & -b^2 \\ a^2 & 0 & ab \\ b^2 & -ab & 0 \end{pmatrix} \leq 2.$$

Donc $X(5) = A(5)$ est une copie de $\mathbf{P}^1$, et $V = \oplus V_i$ est engendré par l'équation:

$$abx_0^2 + b^2x_1x_4 - a^2x_2x_3 = 0 \tag{3.20}$$

et ses permutations cycliques.

Les points $(a : b) = (1 : 0),(0 : 1)$ sont les pointes rationnelles de $X(5)$.

3.2.1.7 Equations pour $X(7)$.

Soit $0 = (0 : a : b : -c : c : -b : -a)$. La variété $A(7)$ est définie par:

$$\text{rang} \begin{pmatrix} 0 & -a^2 & -b^2 & -c^2 \\ a^2 & 0 & ac & -bc \\ b^2 & -ac & 0 & ab \\ c^2 & bc & -ab & 0 \end{pmatrix} \leq 2.$$

Donc $X(7) = A(7)$ est la quadrique de Klein, et $V = \oplus_i V_i$ est engendré par les équations:

$$\begin{aligned} abx_1x_6 + bcx_2x_5 + cax_3x_4 &= 0 \\ abx_0^2 + c^2x_2x_5 - b^2x_3x_4 &= 0 \\ bcx_0^2 - c^2x_1x_6 + a^2x_3x_4 &= 0 \\ cax_0^2 + b^2x_1x_6 - a^2x_2x_5 &= 0 \end{aligned} \tag{3.21}$$

et leurs permutations cycliques.

Les points $(a : b : c) = (1 : 0 : 0),(0 : 1 : 0),(0 : 0 : 1)$ sont les pointes rationnelles de $X(7)$.

3.2.2 Equations des torseurs

Soit $n = 5$ ou 7. On va donner des équations explicites des torseurs $C_{\lambda,\theta}$ comme courbes dans $\mathbf{P}^{n-1}$. On travaille sur un corps parfait K et on suppose que $\text{car}(K) \neq n$.

Soit $T \hookrightarrow \mathbf{P}^{n-1}$ une courbe lisse de genre 1 et de degré n invariante sous l'action de $\mu_n \hookrightarrow \mathrm{Aut}(\mathbf{P}^{n-1})$ donnée par

$$\zeta \mapsto \mathrm{Diag}(1 : \zeta : ... : \zeta^{n-1}). \tag{3.22}$$

On écrit $(x_0 : ... : x_{n-1})$ pour les coordonnées d'un point dans $\mathbf{P}^{n-1}$ et on suppose que tous les indices sont modulo n. Les hyperplans fixés par (3.22) sont les $H_i := \{x_i = 0\}$. L'action de $\mathrm{Jac}(T)[n]$ sur T se prolonge à $\mathbf{P}^{n-1}$. Comme n est premier on sait que cette action est engendrée par:

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & ... & 0 \\ 0 & \zeta & 0 & ... & 0 \\ 0 & 0 & \zeta^2 & ... & 0 \\ . & . & . & & . \\ . & . & . & & . \\ . & . & . & & . \\ 0 & 0 & 0 & ... & \zeta^{n-1} \end{pmatrix} \qquad M_2 := \begin{pmatrix} 0 & 0 & ... & 0 & \star \\ \star & 0 & ... & 0 & 0 \\ 0 & \star & ... & 0 & 0 \\ . & . & & . & . \\ . & . & & . & . \\ . & . & & . & . \\ 0 & 0 & ... & \star & 0 \end{pmatrix}$$

où $\star$ désigne un élément non nul de $\overline{K}$. d'après le lemme (3.2.1.2) la courbe T est définie par 5 quadriques, respectivement 14 quadriques. L'action de M_1 divise ces quadriques en n espaces propres, et l'action de M_2 nous dit que tous ces espaces ont la même dimension. De façon plus explicite, on a

$$H^0(\mathbf{P}^{n-1},\mathcal{I}_T(2)) = \oplus_i V_i \qquad \text{avec} \qquad V_i \subset \langle x_i^2, x_{i-1}x_{i+1}, ... \rangle.$$

3.2.2.1 Lemme

Soit $T \hookrightarrow \mathbf{P}^{n-1}$ une courbe satisfaisant les hypothèses précédentes.

1. La courbe T rencontre les hyperplans H_i en n^2 points.

2. Toute quadrique non nulle contenant T a au moins trois termes non nuls.

Preuve. voir [5] lemme 2.6.

3.2.2.2 Définition

Soient $\lambda,\tau_0,...,\tau_{n-1} \in K$ tels que $\alpha(\lambda) = \prod \tau_i \neq 0$. On définit le sous schéma $T[\lambda; \tau_0,...,\tau_{n-1}]$ de $\mathbf{P}^{n-1}$ avec les équations:

$n = 5 \qquad \tau_0 x_0^2 + x_1 x_4 - \tau_2\tau_3 x_2 x_3 = 0 \qquad$ et ses permutations cycliques

$$n = 7 \begin{cases} \tau_0 x_0^2 + x_1 x_6 - (1/\lambda^2)\tau_2\tau_3\tau_4\tau_5 x_2 x_5 = 0 \\ \\ \tau_0 x_0^2 + \lambda x_1 x_6 - (1/\lambda^3)\tau_2\tau_3^2\tau_4^2\tau_5 x_3 x_4 = 0 \end{cases} \text{ et leurs permutations cycliques}$$

3.2.2.3 Proposition

Toute courbe $T \hookrightarrow \mathbf{P}^{n-1}$ satisfaisant les hypothèses précédentes est égale à $T[\lambda;\tau_0,...,\tau_{n-1}]$ pour des $\lambda,\tau_0,...,\tau_{n-1} \in K$.

Preuve. voir [5] proposition 2.8.

3.2.2.4 Lemme

Les schémas $T[\lambda;\tau_0,...,\tau_{n-1}]$ définis sur K sont uniquement déterminés par $\lambda \in K$ et $\theta = \prod \tau_i^{-i} \in K^\star/(K^\star)^n$.

Preuve.

Cela revient à démontrer que si les n-uples $(\tau_0,...,\tau_{n-1})$ et $(\xi_0,...,\xi_{n-1})$ vérifient $\alpha(\lambda) = \prod \tau_i = \prod \xi_i$ et $(\prod \tau_i^{-i})/(\prod \xi_i^{-i}) \in (K^\star)^n$ alors

$$T[\lambda;\tau_0,...,\tau_{n-1}] \cong T[\lambda;\xi_0,...,\xi_{n-1}].$$

Montrons d'abord que si les n-uples $(\tau_0,...,\tau_{n-1})$ et $(\sigma_0,...,\sigma_{n-1})$ vérifient $\alpha(\lambda) = \prod \tau_i = \prod \sigma_i$ et $\theta = \prod \tau_i^{-i} = \prod \sigma_i^{-i}$ alors $T[\lambda;\tau_0,...,\tau_{n-1}] \cong T[\lambda;\sigma_0,...,\sigma_{n-1}]$.

Pour $n = 5$ considérons l'isomorphisme de $\mathbf{P}^4 \to \mathbf{P}^4$ donné par:

$$(x_0 : x_1 : x_2 : x_3 : x_4) \mapsto (wx_0 : x_1 : x_2 : ux_3 : vx_4) \qquad \text{avec } u,v \text{ et } w \in K^\star.$$

L'image de $T[\lambda;\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4]$ par cet isomorphisme est

$$T[\lambda; w^{-2}v\sigma_0, v\sigma_1, u\sigma_2, vu^{-2}\sigma_3, wv^{-2}u\sigma_4],$$

et en prenant $u = \dfrac{\tau_2}{\sigma_2}, v = \dfrac{\tau_2^2\tau_3}{\sigma_2^2\sigma_3}$ et $w = \dfrac{\tau_2^3\tau_3^2\tau_4}{\sigma_2^3\sigma_3^2\sigma_4}$ on obtient l'isomorphisme

$$T[\lambda;\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4] \cong T[\lambda; w^{-2}v\sigma_0, w\sigma_1, \tau_2, \tau_3, \tau_4].$$

Donc il reste à montrer que

$$T[\lambda;\tau_0,\tau_1,\tau_2,\tau_3,\tau_4] \cong T[\lambda;\sigma'_0,\sigma'_1,\tau_2,\tau_3,\tau_4] \quad \text{avec} \quad \sigma'_0 = w^{-2}v\sigma_0 \text{ et } \sigma'_1 = w\sigma_1.$$

Mais comme $\tau_0\tau_1\tau_2\tau_3\tau_4 = \sigma'_0\sigma'_1\tau_2\tau_3\tau_4$ et $\tau_1^{-1}\tau_2^{-2}\tau_3^{-3}\tau_4^{-4} = \sigma_1'^{-1}\tau_2^{-2}\tau_3^{-3}\tau_4^{-4}$ alors $\sigma'_0 = \tau_0$ et $\sigma'_1 = \tau_1$.

Même démonstration pour $n = 7$ en considérant l'isomorphisme $\mathbf{P}^6 \to \mathbf{P}^6$ donné par

$$(x_0 : x_1 : x_2 : x_3 : x_4 : x_5 : x_6) \mapsto (sx_0 : x_1 : x_2 : ux_3 : vx_4 : wx_5 : rx_6)$$

et en prenant $u = \dfrac{\tau_2}{\sigma_2}$,$v = \dfrac{\tau_2^2\tau_3}{\sigma_2^2\sigma_3}$,$w = \dfrac{\tau_2^3\tau_3^2\tau_4}{\sigma_2^3\sigma_3^2\sigma_4}$,$r = \dfrac{\tau_2^4\tau_3^3\tau_4^2\tau_5}{\sigma_2^4\sigma_3^3\sigma_4^2\sigma_5}$ et $s = \dfrac{\tau_2^5\tau_3^4\tau_4^3\tau_5^2\tau_6}{\sigma_2^5\sigma_3^4\sigma_4^3\sigma_5^2\sigma_6}$,

l'image de $T[\lambda;\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6]$ étant

$$T[\lambda; s^{-2}r\sigma_0, s\sigma_1, u\sigma_2, vu^{-2}\sigma_3, wv^{-2}\sigma_4, rw^{-2}v\sigma_5, sr^{-2}w\sigma_6].$$

Soit maintenant $u \in K^\star$ tel que $\prod \tau_i^{-i} = u^n \prod \xi_i^{-i}$. Les n-uples $(u^{-n}\tau_0, u^n\tau_1, \tau_2, ..., \tau_{n-1})$ et $(\xi_0, ..., \xi_{n-1})$ ont les mêmes λ et θ, donc d'après ce qu'on vient de voir on a

$$T[\lambda; u^{-n}\tau_0, u^n\tau_1, \tau_2, ..., \tau_{n-1}] \cong T[\lambda; \xi_0, ..., \xi_{n-1}].$$

Il reste à montrer

$$T[\lambda; \tau_0, ..., \tau_{n-1}] \cong T[\lambda; u^{-n}\tau_0, u^n\tau_1, \tau_2, ..., \tau_{n-1}].$$

Pour cela il suffit de considérer l'isomorphisme de $\mathbf{P}^{n-1} \to \mathbf{P}^{n-1}$ défini par

$$(x_0 : ... : x_{n-1}) \mapsto (u^n x_0 : ux_1 : ... : u^{n-1}x_{n-1}).$$

l'image de $T[\lambda; \tau_0, ..., \tau_{n-1}]$ par cet isomorphisme étant $T[\lambda; u^{-n}\tau_0, u^n\tau_1, \tau_2, ..., \tau_{n-1}]$. □

3.2.2.5 Proposition

Soient $\lambda, \tau_0, ..., \tau_{n-1} \in K$ avec $\alpha(\lambda) = \prod \tau_i \neq 0$.

1. Si $\beta(\lambda) \neq 0$ alors T est une courbe lisse de genre 1.
2. Si $\beta(\lambda) = 0$ alors T est un polygone de Néron.

Preuve. voir [5] proposition 2.10.

3.2.2.6 Lemme

Le schéma $T[\lambda;\tau_0,...,\tau_{n-1}]$ rencontre les hyperplans H_i en n^2 points. Les points d'intersection avec H_i sont définis sur $K(\zeta, \sqrt[n]{\alpha(\lambda)^i\theta})$ où $\theta = \prod \tau_i^{-i}$.

Preuve. voir [5] lemme 2.11.

3.2.2.7 Proposition

Soit $\lambda \in K \setminus \{\text{les pointes de } X_1(n)\}$.

1. Si $\tau_0,...,\tau_{n-1} \in K$ avec $\alpha(\lambda) = \prod \tau_i$ et $\theta = \prod \tau_i^{-i}$ alors

$$T[\lambda;\tau_0,...,\tau_{n-1}] \cong C_{\lambda,\theta}.$$

2. L'image de $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda(K)$ est engendrée par $\alpha(\lambda)$.

Preuve. voir [5] proposition 2.12.

3.2.2.8 Remarque

On a les isomorphismes $C_{\lambda,\theta} \cong C_{-1/\lambda,\theta^2}$ pour $n = 5$ et $C_{\lambda,\theta} \cong C_{(\lambda-1)/\lambda,\theta^2}$ pour $n = 7$. Par exemple pour $n = 5$ on a

$$T[\lambda;\tau_0,\tau_1,\tau_2,\tau_3,\tau_4] \cong T[-1/\lambda; -\tau_0/(\tau_2\tau_3),..., -\tau_3/(\tau_0\tau_1)]$$

$$(x_0 : x_1 : x_2 : x_3 : x_4) \mapsto (x_0 : x_2 : x_4 : x_1 : x_3).$$

Enfin, on abandonne notre hypothèse $\text{car}(K) \neq n$. Les équations qui apparaissent dans la formulation de la proposition suivante sont obtenues à partir des équations de $T[\lambda;\tau_0,...,\tau_{n-1}]$ en travaillant sous l'hypothèse $\alpha(\lambda) = \prod \tau_i \neq 0$ puis en choisissant $\lambda = 0$, respectivement $\lambda = 1$.

On écrit $P_0 = (1 : 0 : 0 : ...)$, $P_1 = (0 : 1 : 0 : ...)$... .

3.2.2.9 Proposition

Soient $\tau_0,...,\tau_{n-1} \in K$ avec $I = \{i \mid \tau_i = 0\} \neq \emptyset$. Alors le sous-schéma de $\mathbf{P}^{n-1}$ donné par les équations

$n = 5$ $\qquad$ $\tau_0 x_0^2 + x_1x_4 - \tau_2\tau_3x_2x_3 = 0$ $\qquad$ et ses permutations cycliques

$$n=7 \quad \begin{cases} \tau_0 x_0^2 + x_1 x_6 - \tau_2\tau_3\tau_4\tau_5 x_2 x_5 = 0 \\ \\ \tau_0^2\tau_1\tau_6 x_0^2 - x_2 x_5 + \tau_3\tau_4 x_3 x_4 = 0 \end{cases} \quad \text{et leurs permutations cycliques}$$

est la réunion de $|I|$ courbes rationnelles. Plus précisément, pour toute paire consécutive $i,i+d \in I$ on a une courbe rationnelle de degré d qui joint P_i à P_{i+d}.

Preuve. voir [5] proposition 2.14.

3.2.3 Solubilité locale des torseurs

Dans cette section on travaille sur un corps complet par rapport à une valuation discrète, et de corps résiduel fini. On utilise les résultats de la section (3.2.2) pour donner quelques critères d'existence de points rationnels sur les torseurs $C_{\lambda,\theta}$. On travaille toujours avec les notations (2.1.4.1) où l'on pose ϑ =ord. On note $\mathrm{ord}^\star(\lambda)$ l'entier positif r avec

$$n=5 \quad \{\mathrm{ord}(\lambda),\mathrm{ord}(-1/\lambda)\} = \{-r,r\}$$

$$n=7 \quad \{\mathrm{ord}(\lambda),\mathrm{ord}((\lambda-1)/\lambda),\mathrm{ord}(1/(1-\lambda))\} = \{-r,0,r\}.$$

3.2.3.1 Proposition

Soit $\lambda \in K \setminus \{\text{les pointes de } X_1(n)\}$. On décrit l'image du morphisme de connection $\delta : D_\lambda(K) \to K^\star/(K^\star)^n$.

1. Si $\mathrm{ord}^\star(\lambda) > 0$ alors $\mathrm{im}(\delta) = K^\star/(K^\star)^n$.

2. Si $\mathrm{ord}^\star(\lambda) = 0$ alors $\mathrm{im}(\delta) \subset R^\star/(R^\star)^n$.

3. Si $\mathrm{ord}^\star(\lambda) = 0$ et $\mathrm{car}(k) \neq n$ alors

   (a) Si $\beta(\lambda) \not\equiv 0 \bmod(\pi)$ alors $\mathrm{im}(\delta) = R^\star/(R^\star)^n$.

   (b) Si $\beta(\lambda) \equiv 0 \bmod(\pi)$ alors $\mathrm{im}(\delta) = 0$.

3.2.3.2 Remarque

Si on note par $h : H^1(G_{\overline{K},K},E[\phi]) \to H^1(G_{\overline{K},K},E)$ le morphisme dans (3.4) alors on a

$$\theta \in \mathrm{im}(\delta) \Leftrightarrow \theta \in \ker\, h \Leftrightarrow C_{\lambda,\theta}(K) \neq \emptyset.$$

Preuve

1. Il suffit de montrer que $K^\star/(K^\star)^n \subset \mathrm{im}(\delta)$. Soit donc $\theta \in K^\star/(K^\star)^n$, d'après la remarque (3.2.2.8) on peut supposer ord $(\lambda) > 0$, respectivement ord $(\lambda - 1) > 0$. On écrit $C_{\lambda,\theta}$ sous la forme $T[\lambda; \tau_0,...,\tau_{n-1}]$ avec $\mathrm{ord}(\tau_i) \geq 0$ pour tout i. La proposition (3.2.2.9) nous dit que la réduction de cette courbe est une collection de courbes rationnelles définies sur k. Au moins une de ces courbes est de degré impair et donc isomorphe à $\mathbf{P}^1$ sur k. On choisit un point lisse Q sur la réduction et en utilisant le lemme de Hensel, on trouve un point P dans $C_{\lambda,\theta}(K)$ tel que $\widetilde{P} = Q$ et donc $C_{\lambda,\theta}(K) \neq \emptyset$, ce qui équivaut à $\theta \in \mathrm{im}(\delta)$ d'après la remarque (3.2.3.2).

2. Soit $\theta \in K^\star/(K^\star)^n$ avec ord $(\theta) \equiv 1 \bmod(n)$ et montrons que $\theta \notin \mathrm{im}(\delta)$. Supposons que $\theta \in \mathrm{im}(\delta)$, ce qui équivaut à $C_{\lambda,\theta}(K) \neq \emptyset$. Ecrivons $C_{\lambda,\theta}$ sous la forme $T[\lambda; \tau_0,...,\tau_{n-1}]$ avec $\mathrm{ord}(\tau_0) = -1$, $\mathrm{ord}(\tau_{n-1}) = 1$ et $\mathrm{ord}(\tau_i) = 0$ pour tous les autres i. On prend un point $P = (x_0 : ... : x_{n-1}) \in C_{\lambda,\theta}(K)$ avec $\min\{\mathrm{ord}(x_i)\} = 0$.

Soit $n = 5$ et examinant les équations de $T[\lambda; \tau_0,\tau_1,\tau_2,\tau_3,\tau_4]$ qui sont données par:

$$\begin{cases} \tau_0 x_0^2 + x_1x_4 - \tau_2\tau_3 x_2x_3 \\ \tau_1 x_1^2 + x_0x_2 - \tau_3\tau_4 x_3x_4 \\ \tau_2 x_2^2 + x_1x_3 - \tau_0\tau_4 x_0x_4 \\ \tau_3 x_3^2 + x_2x_4 - \tau_0\tau_1 x_0x_1 \\ \tau_4 x_4^2 + x_0x_1 - \tau_1\tau_2 x_1x_2 \end{cases}$$

Comme $\mathrm{ord}(\tau_0) = -1$ et $\mathrm{ord}(x_1x_4 - \tau_2\tau_3x_2x_3) \geq 0$, la 1^{ere} équation donne $\mathrm{ord}(x_0) \geq 1$.

Comme $\mathrm{ord}(\tau_1) = 0$ et $\mathrm{ord}(x_0x_2 - \tau_3\tau_4x_3x_4) \geq 1$, la 2^{eme} équation donne $\mathrm{ord}(x_0) \geq 1$.

Comme $\mathrm{ord}(\tau_2) = 0$ et $\mathrm{ord}(x_1x_3 - \tau_0\tau_4x_0x_4) \geq 1$, la 3^{eme} équation donne $\mathrm{ord}(x_0) \geq 1$.

Comme $\mathrm{ord}(\tau_3) = 0$ et $\mathrm{ord}(x_2x_4 - \tau_0\tau_1x_0x_1) \geq 1$, la 4^{eme} équation donne $\mathrm{ord}(x_0) \geq 1$.

Comme $\mathrm{ord}(\tau_4) = 1$ et $\mathrm{ord}(x_0x_1 - \tau_1\tau_2x_1x_2) \geq 2$, la 5^{eme} équation donne $\mathrm{ord}(x_0) \geq 1$.

D'où $\mathrm{ord}(x_i) > 0$ pour tout i, ce qui contredit $\min\{\mathrm{ord}(x_i)\} = 0$ et donc $\theta \notin \mathrm{im}(\delta)$. D'où $\mathrm{im}(\delta) \subset R^\star/(R^\star)^n$. Même démonstration pour $n = 7$ en considérant les 7 équations: $\tau_i x_i + x_{i+1}x_{i+6} - (1/\lambda^2)\tau_{i+2}\tau_{i+3}\tau_{i+4}\tau_{i+5}x_{i+2}x_{i+5} = 0$ avec $0 \leq i \leq 6$.

3. Soit $\theta \in R^\star/(R^\star)^n$, on écrit $C_{\lambda,\theta}$ sous la forme $T[\lambda; \tau_0,...,\tau_{n-1}]$ avec $\mathrm{ord}(\tau_i) = 0$ pour tout i. La réduction de cette courbe est donnée par la proposition (3.2.2.5).

Dans le cas (a) la réduction est une courbe lisse de genre 1. Soit $Q \in \widetilde{C_{\lambda,\theta}}(k)$, d'après le lemme (2.1.4.6) il existe $P \in C_{\lambda,\theta}(K)$ tel que $\widetilde{P} = Q$ et donc $\theta \in \mathrm{im}(\delta)$.

Dans le cas (b) la réduction est une collection de droites, si $C_{\lambda,\theta}(K) \neq \emptyset$ alors une de ces droites est définie sur k. Cette droite rencontre tous les hyperplans H_i, soit donc, dans le cas $n = 5$, $P = (0 : x_1 : x_2 : x_3 : x_4) \in H_0$ un point de cette droite, alors les coordonnées de ce point vérifient:

$$\begin{cases} x_1x_4 = \tau_2\tau_3x_2x_3 \\ \tau_1x_1^2 = \tau_3\tau_4x_3x_4 \\ \tau_2x_2^2 = x_1x_3 \\ \tau_3x_3^2 = x_2x_4 \\ \tau_4x_4^2 = \tau_1\tau_2x_1x_2 \end{cases}$$

On a $x_4 \neq 0$ car sinon on aurait $x_0 = x_1 = x_2 = x_3 = x_4 = 0 \notin \mathbf{P}^4$. De la 4^{eme} équation on a $\dfrac{x_2}{x_4} = \tau_3(\dfrac{x_3}{x_4})^2$, et de la 1^{ere} équation on obtient $\dfrac{x_1}{x_4} = \tau\tau_3^2(\dfrac{x_3}{x_4})^3$, et la 5^{eme} équation nous donne $\tau_4 = \tau_1\tau_2^2\tau_3^3(\dfrac{x_3}{x_4})^5$, d'où $\theta = \tau_1\tau_2^{-2}\tau_3^{-3}\tau_4^{-4} = (\dfrac{x_3}{x_4\tau_4})^5 \in (k^\star)^5$. Comme $\mathrm{car}(k) \neq 5$, il vient que $\theta \in (K^\star)^5$. Donc $\mathrm{im}(\delta) = 0$. □

Il nous reste à traiter le cas où $\mathrm{car}(k) = n$. On abandonne donc la méthode de l'espace projectif et on utilise la méthode "push out". On a déja vu que l'application

$$\delta : D_\lambda(K) \to K^\star/(K^\star)^n$$

est décrite par une fonction rationnelle $f \in K(D_\lambda)$, donnée explicitement par (3.9). On rappelle (voir [14]) que l'équation de Weierstrass

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

est satisfaite par les séries

$$x(z) = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 - ...$$
$$y(z) = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1 a_3) z + ...$$

En appliquant ceci à la courbe D_λ définie par (3.1) on trouve:

$$n = 5 \begin{cases} x(z) = \dfrac{1}{z^2} - \dfrac{1-\lambda}{z} + \lambda + \lambda z + (\lambda(1-\lambda)) z^2 - ... \\ \\ y(z) = -\dfrac{1}{z^3} + \dfrac{1-\lambda}{z^2} - \dfrac{\lambda}{z} - \lambda - (\lambda(1-\lambda)) z + ... \end{cases}$$

$$n = 7 \begin{cases} x(z) = \dfrac{1}{z^2} - \dfrac{1+\lambda-\lambda^2}{z} - (\lambda^2-\lambda^3) - (\lambda^2-\lambda^3) z - (\lambda^2-\lambda^3)(1+\lambda-\lambda^2) z^2 - ... \\ \\ y(z) = -\dfrac{1}{z^3} + \dfrac{1+\lambda-\lambda^2}{z^2} + \dfrac{\lambda^2-\lambda^3}{z} + (\lambda^2-\lambda^3) + (\lambda^2-\lambda^3)(1+\lambda-\lambda^2) z + ... \end{cases}$$

On calcule les premiers termes de la série $F(z) := \pm z^n f(x(z), y(z))$.

$F(z) = 1 + (2\lambda - 1) z + \lambda(\lambda + 2) z^2 + ...$

$F(z) = 1 + (3\lambda^2 - 2\lambda - 2) z + (\lambda - 1)(3\lambda^3 + 3\lambda^2 - 3\lambda - 1) z^2 + ...$

On s'intéresse au cas $\mathrm{car}(k) = n$. On trouve $\beta(\lambda) \equiv (\lambda - 3)^2 \bmod(\pi)$, respectivement $\beta(\lambda) \equiv (\lambda - 5)^3 \bmod(\pi)$, et $F'(0) \equiv \beta'(\lambda) \bmod(\pi)$. Donc

$$F(\pi R) = 1 + \pi R \qquad \text{si } \beta(\lambda) \not\equiv 0 \bmod(\pi) \tag{3.23}$$

$$F(\pi R) \subset 1 + \pi^2 R \qquad \text{si } \beta(\lambda) \equiv 0 \bmod(\pi) \tag{3.24}$$

car pour $n = 5$ on a $\beta(\lambda) \equiv 0 \bmod(\pi) \Rightarrow \lambda - 3 \equiv 0 \bmod(\pi) \Rightarrow 2\lambda - 1 \equiv 0 \bmod(\pi)$ et pour $n = 7$ on a $\beta(\lambda) \equiv 0 \bmod(\pi) \Rightarrow (\lambda - 5)^2 \equiv 0 \bmod(\pi) \Rightarrow \lambda^2 - 10\lambda + 25 \equiv 0 \bmod(\pi) \Rightarrow 3\lambda^2 - 2\lambda - 2 \equiv 0 \bmod(\pi)$.

Les relations (3.23) et (3.24) nous donnent tout ce dont on a besoin pour $K = \mathbf{Q}_p$.

3.2.3.3 Proposition

Soit $p = n$. Soit $\lambda \in \mathbf{Q}_p \setminus \{\text{les pointes de } X_1(n)\}$. On décrit l'image de

$$\delta : D_\lambda(\mathbf{Q}_p) \to \mathbf{Q}_p^\star/(\mathbf{Q}_p^\star)^n$$

dans le cas $\mathrm{ord}^\star(\lambda) = 0$.

1. Si $\beta(\lambda) \not\equiv 0 \bmod(p)$ alors $\mathrm{im}(\delta) = \mathbf{Z}_p^\star/(\mathbf{Z}_p^\star)^n$.

2. Si $\beta(\lambda) \equiv 0 \bmod(p)$ alors $\mathrm{im}(\delta)$ est engendré par $\alpha(\lambda)$. Donc la condition pour que δ soit l'application nulle est $\lambda \equiv 18 \bmod(25)$, respectivement $\lambda \equiv 5 \bmod(7)$.

3.2.3.4 Remarque

On a déja vu que l'équation de Weierstrass (3.1) est minimale. On écrit $E = D_\lambda$, on a les inclusions suivantes

$$E(\mathbf{Q}_p) \supset E_0(\mathbf{Q}_p) \supset E_1(\mathbf{Q}_p)$$

et la suite exacte

$$0 \to E_1(\mathbf{Q}_p) \to E_0(\mathbf{Q}_p) \to \widetilde{E}^{sm}(k) \to 0$$

où:

$$E_0(\mathbf{Q}_p) = \{P \in E(\mathbf{Q}_p) : \widetilde{P} \in \widetilde{E}^{sm}(k)\} \qquad \text{et} \qquad E_1(\mathbf{Q}_p) = \{P \in E(\mathbf{Q}_p) : \widetilde{P} = \widetilde{O}\}$$

D'après le lemme (3.1.2.13) l'image de δ restreinte à $E_1(\mathbf{Q}_p)$ est engendrée par $F(p\mathbf{Z}_p)$.

Preuve

1. D'après la proposition (3.2.3.1−3) on a $\mathrm{im}\,\delta \subset \mathbf{Z}_p^\star/(\mathbf{Z}_p^\star)^n$. Comme $F(p\mathbf{Z}_p) = 1 + p\mathbf{Z}_p$ engendre $\mathbf{Z}_p^\star/(\mathbf{Z}_p^\star)^n$ alors on a égalité.

2. Comme $1 + p^2\mathbf{Z}_p \subset (\mathbf{Z}_p^\star)^n$, il vient de (3.24) que im δ restreinte à $E_1(\mathbf{Q}_p)$ est triviale. De plus,

   $$E_0(\mathbf{Q}_p)/E_1(\mathbf{Q}_p) \cong \widetilde{E}^{sm}(\mathbf{Z}/n\mathbf{Z}) \cong \mathbf{Z}/n\mathbf{Z},$$

   donc d'après la proposition $(3.2.2.7 - 2)$ l'image de δ restreinte à $E_0(\mathbf{Q}_p)$ est engendrée par $\alpha(\lambda)$. Finalement dans le cas où la réduction est additive,

le nombre de Tamagawa $[E(\mathbf{Q}_p) : E_0(\mathbf{Q}_p)]$ est au plus 4, et donc premier à n. Il vient qu'il n'y a pas de contribution à l'image de δ. Pour la dernière assertion, on calcule

$$\left\{ \begin{array}{l} \lambda \equiv 3(5) \\ \lambda \in (\mathbf{Q}_5^\star)^5 \end{array} \right\} \Leftrightarrow \lambda \equiv 18(25) \quad \text{et} \quad \left\{ \begin{array}{c} \lambda \equiv 5(7) \\ \lambda^4(\lambda - 1) \in (\mathbf{Q}_7^\star)^7 \end{array} \right\} \Leftrightarrow \lambda \equiv 5(7).$$

□

Soient $\mathcal{A}$ et $\mathcal{B}$ les ensembles de premiers définis dans la section (3.1.3). Pour S un ensemble fini de premiers rationnels, on note

$$[S] = \{\theta \in \mathbf{Q}^\star/(\mathbf{Q}^\star)^n | \text{ord}(\theta) \equiv 0 \bmod(n) \quad \text{pour tout } p \notin S\}. \tag{3.25}$$

Comme $C[\phi] \cong \mu_n$, on identifie $H^1(\mathbf{Q}_p, C[\phi]) = \mathbf{Q}_p^\star/(\mathbf{Q}_p^\star)^n$.

3.2.3.5 Proposition

Soit $\lambda \in \mathbf{Q} \setminus \{\text{les pointes de } X_1(n)\}$. Le morphisme de connection

$$\delta_\phi : D_\lambda(\mathbf{Q}_p) \to H^1(\mathbf{Q}_p, C_\lambda[\phi])$$

a pour image

$$\text{im } \delta_\phi = \left\{ \begin{array}{ll} \mathbf{Q}_p^\star/(\mathbf{Q}_p^\star)^n & \text{si } p \in \mathcal{A} \\ \mathbf{Z}_p^\star/(\mathbf{Z}_p^\star)^n & \text{si } p \notin \mathcal{A} \cup \mathcal{B} \\ 0 & \text{si } p \in \mathcal{B} \end{array} \right.$$

Preuve

Soit p un premier rationnel

(i) Si $p \in \mathcal{A}$ alors $\text{ord}_p^\star(\lambda) > 0$ et donc d'après la proposition $(3.2.3.1 - 1)$ on a $\text{im}(\delta) = \mathbf{Q}_p^\star/(\mathbf{Q}_p^\star)^n$.

(ii) Si $p \notin \mathcal{A} \cup \mathcal{B}$ alors $\text{ord}_p^\star(\lambda) = 0$ et $\beta(\lambda) \not\equiv 0 \bmod(p)$. Si $p \neq n$, d'après la proposition $(3.2.3.1 - 3(a))$ on a $\text{im}(\delta) = \mathbf{Z}_p^\star/(\mathbf{Z}_p^\star)^n$ et si $p = n$, alors d'après la proposition $(3.2.3.3 - 1)$ on a $\text{im}(\delta) = \mathbf{Z}_p^\star/(\mathbf{Z}_p^\star)^n$.

(iii) Si $p \in \mathcal{B}$ alors $\beta(\lambda) \equiv 0 \bmod(p)$. Si $p \neq n$ on a d'après la proposition $(3.2.3.1 - 3(b))$ $\mathrm{im}(\delta) = 0$, et si $p = n$ alors d'après $(3.2.3.3. - 2)$ on a $\mathrm{im}(\delta) = 0$. □

La description de $S^{(\phi)}(C_\lambda/\mathbf{Q})$ donnée par le théorème (3.1.3.1) découle directement de la proposition (3.2.3.5).

$$\begin{aligned} S^{(\phi)}(C_\lambda/\mathbf{Q}) &= \{\theta \in \mathbf{Q}^\star/(\mathbf{Q}^\star)^n : C_{\lambda,\theta}(\mathbf{Q}_p) \neq \emptyset \ \text{ pour tous les premiers } p\} \\ &= \{\theta \in [\mathcal{A}] | \theta \in (\mathbf{Q}_p^\star)^n \quad \text{pour tout } p \in \mathcal{B}\}. \end{aligned}$$

On peut utiliser le théorème (3.1.3.1) pour trouver une courbe elliptique $E/\mathbf{Q}$ telle que son groupe de Selmer $S^{(n)}(E/\mathbf{Q})$ soit assez large. Pour cela on choisit $\lambda \in \mathbf{Q}$ de sorte que $|\mathcal{A}|$ soit large et $|\mathcal{B}|$ soit petit , et vice versa. On cite deux corollaires importants.

3.2.3.6 Corollaire

Pour $n = 5$ ou 7, le groupe de Selmer $S^{(n)}(E/\mathbf{Q})$ d'une courbe elliptique $E/\mathbf{Q}$ peut être assez grand.

Preuve. voir [5] corollaire 2.

3.2.3.7 Corollaire

Le sous-groupe de 5-torsion du groupe de Tate-Shafarevich d'une courbe elliptique $E/\mathbf{Q}$ peut être assez grand.

Preuve. voir [5] corollaire 3.

Bibliographie

[1] J.W.S. Cassels and A. Fröhlich. *Algebraic number theory*. Academic Press, 1967.

[2] J.W.S. Cassels. *Local fields*. London mathematical society, 1986.

[3] J.W.S. Cassels. *Lectures on elliptic curves*. LMSST 24: Cambridge University Press, 1991.

[4] H. Cohen. *A course in computational algebraic number theory*. GTM 138. Springer, 1993.

[5] T. Fisher. Some examples of 5 and 7 descent for elliptic curves over Q. Springer EMS, 2001.

[6] K. Irland and M. Rosen. *A classical introduction to Modern number theory*. GTM 84. Springer, 1982.

[7] A.W. Knapp. *Elliptic curves*. Princeton University Press, 1992.

[8] S. Lang. *Algebraic number theory*. GTM 110. Springer, 1986.

[9] S. Lang. *Algebra*. GTM 211. Springer, 2002.

[10] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer, 1990.

[11] J. Nekovář. *Elliptic curves and modular forms*. www.math.jussieu.fr/ nekovar/co/el/, 2004.

[12] J. Neukirch. *Class field theory*. GMW 280. Springer, 1986.

[13] J.P. Serre. *Local fields* GTM 67. Springer, 1979.

[14] J.H. Silverman. *The arithmetic of elliptic curves*. GTM 106. Springer, 1986.

[15] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. GTM 151. Springer, 1994.

[16] J. Tate. Duality theorems in Galois cohomology over number fields. In *Congress math*, pages 288-295, Stockholm, 1962.

[17] J. Vélu. Isogènies entre courbes elliptiques.
pages 238-241, C.R. Acad. Sci. Paris 273, 1971.

[18] L.C. Washington. *Introduction to cyclotomic fields*. GTM 83. Springer, 1982.