JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

M. VAN DER PUT

# Les courbes de Shimura

*Journal de Théorie des Nombres de Bordeaux 2^e série*, tome 1, n° 1 (1989), p. 89-102

<http://www.numdam.org/item?id=JTNB_1989__1_1_89_0>

*Séminaire de Théorie des Nombres,*
*Bordeaux,* **1**, *89–102 (1989)*

# Les courbes de Shimura.

par M. VAN DER PUT

## Introduction

L'importance des courbes modulaires $X_0(N)$ pour l'arithmétique est bien connue depuis longtemps. La variété de Jacobi $J_0(N)$ de $X_0(N)$ possède également des propriétés arithmétiques.

On s'intéresse, par exemple, à la "réduction modulo $p$" ($p$ étant un nombre premier) de $X_0(N)$. Dans le cas spécial $N = p$ , la réduction modulo $p$ de $X_0(p)$ est une courbe totalement dégénérée. Cette propriété implique que $X_0(p) \otimes \mathbf{Q}_p$ est une courbe de Mumford. Il existe alors un ouvert analytique $\Omega$ de $\mathbf{P}^1 \otimes \mathbf{Q}_p$ et un sous-groupe discret, sans torsion, de type fini, $\Gamma$ de $PGL(2, \mathbf{Q}_p)$ tel que :

$$\Gamma \setminus \Omega \simeq X_0(p) \otimes \mathbf{Q}_p.$$

Cettte uniformisation $p$-adique n'est pas connue explicitement. Par contre l'uniformisation complexe $X_0(N) \otimes \mathbf{C} = \Gamma_0(N) \backslash \mathbf{H} \cup \{\text{pointes}\}$ est explicite.

Cet exposé a pour but d'expliquer la situation analogue pour les courbes de Shimura $S_{d,f}$ (§2). L'idée de ces courbes est proche des courbes modulaires. $S_{d,f}$ est donnée par une uniformisation complexe. $S_{d,f}$ est l'espace des modules de certaines surfaces abéliennes. Pour un nombre premier $p$, $p|d$, la réduction $S_{d,f} \otimes \mathbf{F}_p$ est une courbe totalement dégénérée. L'uniformisation $p$-adique de $S_{d,f} \otimes \mathbf{Q}_p$ est explicitement décrite par le théorème de Čerednik et Drinfeld (§3). On donne une indication de la démonstration.

Un lien entre la variété de Jacobi de $S_{d,f}$ et certains $J_0(N)$ a été découvert par K. Ribet (§4). Ce lien est une partie essentielle de sa démonstration de : "La conjecture de Taniayama-Weil implique le dernier théorème de P. de Fermat".

Finalement, rien dans cet exposé n'est original sauf peut-être les erreurs.

## 1. Algèbres de quaternions sur Q.

Une algèbre de quaternions $D$ sur un corps $k$ est une algèbre simple (i.e. il n'existe pas d'idéaux bilatères différents de 0) avec centre $= k$ et

Manuscrit reçu le 10 avril 1989

$dim_k\ D = 4$. Dans le cas où car $k \neq 2$, $D$ possède une base $\{1, e_1, e_2, e_3\}$ sur $k$ telle que la multiplication est donnée par les formules :

$$e_1e_2 = e_3\ ;\ e_2e_1 = -e_3\ ;\ e_1^2 = a\ ;\ e_2^2 = b\ ;\ e_3^2 = -ab \text{ avec } a,\ b \in k^*\ .$$

*Exemples :*

**1.1** $k = \mathbf{R}$. Il existe deux possibilités : $D = M(2 \times 2, \mathbf{R})$ et $D =$ le corps des quaternions de Hamilton, donné par $a = b = -1$.

**1.2** $k = \mathbf{Q}_p$. Il y a encore deux possibilités : $D = M(2 \times 2, \mathbf{Q}_p)$ et D= le corps non commutatif qu'on peut décrire comme suit : $D = \mathbf{Q}_{p^2}1 + \mathbf{Q}_{p^2}u$ avec règles de multiplication $u^2 = p$ ; $\lambda u = uFr(\lambda)$ pour $\lambda \in \mathbf{Q}_{p^2}$. On a écrit ici $\mathbf{Q}_{p^2}$ pour l'unique extension non ramifiée de degré 2 de $\mathbf{Q}_p$ et $Fr$ pour l'action de Frobenius sur $\mathbf{Q}_{p^2}$ .

**1.3** Soit $D$ une algèbre de quaternions sur $\mathbf{Q}$ et $v$ une place (alors $v$ est un nombre premier ou bien $v = \infty$). On dit que $D$ est ramifiée en $v$ si $D \otimes \mathbf{Q}_v$ est un corps non commutatif. Le nombre des places ramifiées est pair. En outre, pour tout ensemble fini de places $S$ de cardinalité paire, il existe une algèbre de quaternions unique (à isomorphisme près) avec $S$ comme ensemble des places ramifiées. Le *discriminant* $d$ d'une algèbre de quaternions $D/\mathbf{Q}$ est donné par :

$$d = \pm \prod_{p \text{ ramifié}} p$$

le signe + équivaut à "$D$ n'est pas ramifiée en $\infty$".

**1.4** *Exemples.* Le discriminant de $M(2 \times 2, \mathbf{Q})$ est 1. Le discriminant du corps $H$ des quaternions de Hamilton sur $\mathbf{Q}($ avec $a = b = -1)$ est égal à -2.

**1.5** Soit $D/\mathbf{Q}$ une algèbre de quaternions avec discriminant $d$ et soit $f \in \mathbf{Z}$, $f > 0$ et $(d, f) = 1$. Un *ordre d'Eichler* $\theta \subset D$ de niveau $f$ est un sous-anneau de $D$, libre de rang 4 comme $\mathbf{Z}$ -module, tel que :

* pour $p|d$, $\theta \otimes \mathbf{Z}_p$ est l'unique ordre maximal $\mathbf{Z}_{p^2}[u]$ du corps non commutatif $\mathbf{Q}_{p^2}[u]$.

* pour $p \nmid d$, $\theta \otimes \mathbf{Z}_p$ est conjugué à

$$\left\{\begin{pmatrix} a & b \\ fc & d \end{pmatrix}; a,b,c,d \in \mathbf{Z}_p\right\} \subset M(2\times 2, \mathbf{Q}_p) \simeq D \otimes \mathbf{Q}_p.$$

On note que "$f = 1$" est équivalent à "l'ordre d'Eichler est maximal." Pour $d > 0$, il existe une seule classe de conjugaison d'ordres d'Eichler de niveau $f$ dans $D$. Pour $d < 0$, les ordres d'Eichler de niveau $f$ dans $D$ forment un nombre fini de classes de conjugaison.

## 2. Définitions de la courbe de Shimura $S_{d,f}$

Soit $D/\mathbf{Q}$ une algèbre de quaternions indéfinie (i.e. $d > 0$) et soit $\theta \subset D$ un ordre d'Eichler de niveau $f$. Alors $\theta^* \subset (D \otimes \mathbf{R})^* \simeq GL(2,\mathbf{R})$ opère sur $\Omega = \mathbf{C} - \mathbf{R}$. La courbe de Shimura complexe $S_{d,f} \otimes \mathbf{C}$ est définie comme quotient $\theta^* \backslash \Omega$.

Pour $d > 1$, ce quotient est une surface de Riemann, connexe et compacte. Le groupe $\theta^*$ possède des éléments avec un déterminant négatif. Alors :

$$\theta^* \backslash \Omega = \theta_+^* \backslash \mathbf{H}, \text{ où}$$

$$\mathbf{H} = \{z \in \mathbf{C} | \ im\ z > 0\} \text{ et } \theta_+^* = \{\gamma \in \theta^* | \ det\ \gamma > 0\}.$$

Pour $d = 1$, le quotient est égal à $\Gamma_0(f)\backslash \mathbf{H}$. Ce quotient n'est pas compact et la compactification est la courbe modulaire complexe $X_0(f) \otimes \mathbf{C}$. $\theta^*$ est associé au problème suivant de modules :

**2.1** Les surfaces abéliennes $A$ avec les structures supplémentaires :

(1) $i : \theta \hookrightarrow End(A)$

(2) un sous-groupe $B \subset A[f] :=$ {les points d'ordre $f$ de $A$} tel que $B$ est un $\theta$-module cyclique d'ordre $f$.

(3) l'application $\theta \xrightarrow{i} End(A) \longrightarrow End(T_e A) = M(2\times 2, -)$ a la propriété

$$Tr(i(d)) = Tr_{D/\mathbf{Q}}(d) := \textit{la trace réduite de } d := d + \overline{d}.$$

**2.2** *Remarques :*

1) Pour $d = 1$ on retrouve le problème usuel de modules associé à $X_0(f)$.En effet

$$D = M(2 \times 2, \mathbf{Q}) \supset \theta = \left\{ \begin{pmatrix} a & b \\ fc & d \end{pmatrix}; a, b, c, d \in \mathbf{Z} \right\}$$

Il s'ensuit que $A = E_1 \times E_2 =$ le produit de deux courbes elliptiques. En plus, $E_1$ et $E_2$ sont isogènes d'ordre $f$.

*Dans la suite on supposera que* $d > 1$.

2) La condition (2) de (2.1) est une structure de niveau $f$. La condition (3) de (2.1) est un peu technique. Cette condition est superflue en caractéristique 0.

3) On suppose $d > 1$. D'après un théorème de Drinfeld [1], le problème de modules (2.1) possède comme solution un schéma $S_{d,f}$ de type fini et projectif sur $\mathbf{Z}[1/f]$. Pour $f \geq 3$, le schéma $S_{d,f}$ représente le foncteur associé à (2.1).

**2.3** Montrons maintenant que $\theta^* \backslash \Omega$ représente le problème de modules (2.1) sur $\mathbf{C}$. On fixe une immersion $\theta \hookrightarrow M(2 \times 2, \mathbf{R})$ et on associe à $z \in \mathbf{C} - \mathbf{R}$ le réseau

$$\Lambda(z) = \left\{ m \begin{pmatrix} z \\ 1 \end{pmatrix} \in \mathbf{C}^2; m \in \theta \right\} \subset \mathbf{C}^2.$$

Le quotient $A(z) = \mathbf{C}^2/\Lambda(z)$ est *a priori* un tore analytique. Utilisant la norme réduite de $D$ on produit une polarisation sur $A(z)$. Alors $A(z)$ est une surface abélienne sur $\mathbf{C}$. L'immersion $i : \theta \hookrightarrow End(A(z))$ est évidente. Le sous-groupe $B(z)$ de $A(z)$ est donné par $\theta \begin{pmatrix} f^{-1}z \\ 1 \end{pmatrix} \Big/ \Lambda(z)$.

On a construit ainsi une famille $(A(z), i(z), B(z))$ sur $\mathbf{C}$-$\mathbf{R}$. Cette famille possède une $\theta^*$-action naturelle et il n'est pas difficile de montrer que le quotient par $\theta^*$ est une famille universelle (pour les structures (2.1)) au-dessus de la courbe $\theta^* \backslash \Omega$. Cela justifie la notation $S_{d,f} \otimes \mathbf{C}$ pour $\theta^* \backslash \Omega$.

## 3. Le théorème de Čerednik et Drinfeld

D'abord on donne un énoncé faible (et légèrement faux) de ce théorème. Utilisons les notations suivantes :

$\mathbf{C}_p =$ le complété de la clôture algébrique de $\mathbf{Q}_p$.

$$\Omega = \mathbf{C}_p - \mathbf{Q}_p = \mathbf{P}^1(\mathbf{C}_p) - \mathbf{P}^1(\mathbf{Q}_p)$$

L'espace topologique $\Omega$ (pour la topologie induite par $\mathbf{C}_p$) possède une structure d'espace analytique connexe sur $\mathbf{C}_p$. Dans un autre langage $\Omega$ est un schéma formel sur $\mathbf{Z}_p$. Le groupe $PGL(2, \mathbf{Q}_p)$ opère sur $\Omega$. Soit $\Gamma$ un sous-groupe discret et co-compact de $PGL(2, \mathbf{Q}_p)$. Alors Le quotient $\Gamma\backslash\Omega$ existe comme courbe analytique propre sur $\mathbf{Q}_p$ et $\Gamma\backslash\Omega$ est alors une courbe algébrique sur $\mathbf{Q}_p$. En d'autres termes $\Gamma\backslash\Omega$ est un schéma formel sur $\mathbf{Z}_p$, propre, de type fini, de dimension relative 1. Alors $\Gamma\backslash\Omega$ est le complété formel d'une courbe projective sur $\mathbf{Z}_p$ par rapport à la fibre spéciale "$p = 0$"

.

**3.1** THÉORÈME (Čerednik, Drinfeld [1]). *Supposons $p|d$. Alors $S_{d,f}\otimes\mathbf{F}_p$ = la réduction de $S_{d,f}$ modulo $p$ est totalement dégénérée. Il existe un sous-groupe discret, co-compact $\Gamma$ de $PGL(2, \mathbf{Q}_p)$, provenant d'une algèbre de quaternions $D'$, tel que $\Gamma \setminus \Omega$ est isomorphe à $S_{d,f} \otimes \mathbf{Z}_p$*

Dans les pages suivantes on précisera l'énoncé (3.1).

**3.2** *L'algèbre de quaternions $D'$* est obtenue de $D$ en échangeant $p$ et $\infty$. Cela veut dire que le discriminant $d'$ de $D'$ est égal à $d' = -d/p$.

Soit $\theta' \subset D'$ un ordre d'Eichler de niveau $f$ (en général $\theta'$ n'est plus unique à conjugaison près). Alors le groupe $\Gamma$(comme sous-groupe de $GL(2,\mathbf{Q}_p)$ est égal à :

$$\theta'\left[\frac{1}{p}\right]^* \subset (D' \otimes \mathbf{Q}_p)^* \simeq GL(2,\mathbf{Q}_p)$$

Le théorème d'approximation pour les groupes algébriques sur $\mathbf{Q}$ implique que $\Gamma$ est discret et co-compact.

Posons $\Gamma_+ = \{\gamma \in \Gamma \mid v_p(det\gamma) \equiv 0 \ mod\ 2\}$, où $v_p$ est la valuation additive de $\mathbf{Q}_p$.

**3.3** *Le schéma formel* $\Omega$ est associé à l'immeuble de Bruhat-Tits $\Delta$ de $PGL(2,\mathbf{Q}_p)$. Cet immeuble est un arbre qu'on peut décrire comme suit. Les sommets de $\Delta$ sont les classes d'équivalence [M] des $\mathbf{Z}_p$-réseaux M de $\mathbf{Q}_{p^2}$(i.e. $\mathbf{Q}_{p^2}$ est l'extension non ramifiée de degré 2 de $\mathbf{Q}_p$ et $M \subset \mathbf{Q}_{p^2}$ est un $\mathbf{Z}_p$-sous-module, libre de rang 2). L'équivalence $M_1 \sim M_2$ signifie $M_1 = p^n M_2$ pour certain $n \in \mathbf{Z}$. Les arêtes de $\Delta$ sont des paires $\{[M_1], [M_2]\}$ telles que $M_2 \subset M_1$ et $M_1/M_2 \simeq \mathbf{F}_p$. Pour $e_1, e_2 \in \mathbf{Q}_{p^2}$ bien choisis on a $M_1 =< e_1, e_2 >$ et $M_2 =< e_1, pe_2 >$. Alors $\Delta$ est un

arbre régulier avec valence $p+1$. On associe à $\Delta$ un schéma formel $\Omega$, localement de type fini. Soit $\delta = \{< e_1, e_2 >, < e_1, pe_2 >\}$ une arête de $\Delta$. On écrit $X_1, X_2$ pour les coordonnés homogènes par rapport à $\{e_1, e_2\}$. Alors $\Omega(\delta)$ est le spectre formel d'un anneau complet pour la topologie p-adique :

$$\mathbf{Z}_p < \frac{X_2}{X_1}, p\frac{X_1}{X_2}, U > \Big/ \left(U\left(\left(\frac{X_2}{X_1}\right)^{p-1} - 1\right)\left(\left(p\frac{X_1}{X_2}\right)^{p-1} - 1\right) - 1\right).$$

Cet anneau est le complété p-adique de l'anneau

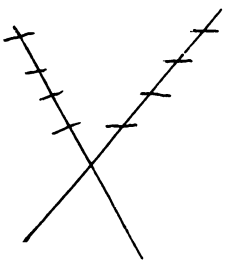
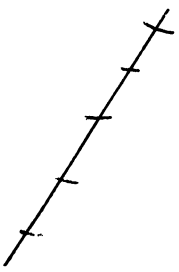
$$\mathbf{Z}_p\left[\frac{X_2}{X_1}, p\frac{X_1}{X_2}, U\right] \Big/ \left(U\left(\left(\frac{X_2}{X_1}\right)^{p-1} - 1\right)\left(\left(p\frac{X_1}{X_2}\right)^{p-1} - 1\right) - 1\right).$$

A chaque sommet $v = [< e_1, e_2 >]$ on associe $\Omega(v) =$ le spectre formel de l'anneau complet

$$\mathbf{Z}_p < \frac{X_2}{X_1}, U > \Big/ \left(U\left(\left(\frac{X_2}{X_1}\right)^{p} - \left(\frac{X_2}{X_1}\right)\right) - 1\right).$$

Alors $\Omega$ est obtenu comme recollement des $\Omega(\delta)$ suivant l'arbre $\Delta$. Pour deux arêtes $\delta_1, \delta_2$ ayant $v$ comme sommet commun on recolle $\Omega(\delta_1)$ et $\Omega(\delta_2)$ sur l'ouvert commun $\Omega(v)$.

Les formules explicites ci-dessus montrent que

$\Omega(\delta) \otimes \mathbf{F}_p =$  et $\Omega(v) \otimes \mathbf{F}_p =$ 

Il s'ensuit que $\Omega \otimes \mathbf{F}_p$ est un arbre de droites (i.e. des $\mathbf{P}^1 \otimes \mathbf{F}_p$). Le graphe dual de $\Omega \otimes \mathbf{F}_p$ est égal à $\Delta$.

L'action de $PGL(2, \mathbf{Q}_p)$ sur $\Omega$ est évidente par la définition de $\Omega$. Un sous-groupe $\Gamma$ de $PGL(2, \mathbf{Q}_p)$ est discret et co-compact si et seulement si les stabilisateurs de $\Gamma$ sur $\Delta$ sont finis et que $\Gamma\backslash\Delta$ est un graphe fini.

Pour un tel $\Gamma$ il est facile de vérifier que le quotient $\Gamma\backslash\Omega$ est un schéma formel de type fini. De plus, $(\Gamma\backslash\Omega)\otimes\mathbf{F}_p$ est constitué de droites rationnelles sur $\mathbf{F}_p$ et les singularités de $(\Gamma\backslash\Omega)\otimes\mathbf{F}_p$ sont des points doubles ordinaires. Le graphe dual de $(\Gamma\backslash\Omega)\otimes\mathbf{F}_p$ s'identifie à $\Gamma\backslash\Delta$.

**3.4** *Le "twist" de Frobenius.* Le quotient $\Gamma\backslash\Omega$ n'est pas tout à fait ce qu'il faut dans le théorème (3.1). Il faut incorporer un "twist" de Frobenius. On utilise les notations suivantes :

$\mathbf{Z}_{p^2} = W(\mathbf{F}_{p^2})$= l'anneau des entiers de $\mathbf{Q}_{p^2}$

$\mathbf{Z}_{p^\infty} = W(\overline{\mathbf{F}}_p)$= (le complété de) l'extension non ramifiée, maximale de $\mathbf{Z}_p$.

$Fr$= l'action de Frobenius sur $\mathbf{Z}_{p^2}$ et $\mathbf{Z}_{p^\infty}$.

$\Omega\hat{\otimes}\mathbf{Z}_{p^\infty}$= le schéma formel déduit de $\Omega$ par l'extension de scalaires $\mathbf{Z}_p \subset \mathbf{Z}_{p^\infty}$.

Le groupe $\Gamma = \left(\theta'\left[\frac{1}{p}\right]\right)^*$ opère sur $\Omega\hat{\otimes}\mathbf{Z}_{p^\infty}$ par la formule (abus de langage !) :

$$\gamma(\omega \otimes \lambda) = ([\gamma]\omega) \otimes Fr^{n(\gamma)}(\lambda)$$

où "$\omega \in \Omega$" , $\lambda \in \mathbf{Z}_{p^\infty}$ , $[\gamma]$= l'image de $\gamma$ dans $PGL(2, \mathbf{Q}_p)$ *et* $n(\gamma) = v_p(det\gamma)$.

**3.5** *La version correcte de (3.1) est :*

*Les schémas formels sur* $\mathbf{Z}_p$, $S_{d;f} \otimes \mathbf{Z}_p$ *et* $\Gamma\backslash(\Omega\hat{\otimes}\mathbf{Z}_{p\infty})$ *sont isomorphes.*

**3.6** *Variation sur (3.5).*

On note que

$$\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \in \Gamma_+$$

et alors

$$\Gamma_+\backslash(\Omega\hat{\otimes}\mathbf{Z}_{p\infty}) = ([\Gamma_+]\backslash\Omega) \otimes \mathbf{Z}_{p^2}$$

où

$$[\Gamma_+] = \Gamma_+ \Big/ \left\{ \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}^n ; n \in \mathbf{Z} \right\}$$

est l'image de $\Gamma_+$ dans $PGL(2, \mathbf{Q}_p)$. Le groupe $\Gamma/\Gamma_+ = \{1, \omega\}$ opère sur $[\Gamma_+]\backslash\Omega$ par $[\omega]$ et sur $\mathbf{Z}_{p^2}$ par $Fr$.

Alors $S_{d,f} \otimes \mathbf{Z}_p$ est un twist de Frobenius de $[\Gamma_+]\backslash\Omega$ donné par

$$\{1, w\}\backslash([\Gamma_+]\backslash\Omega) \otimes \mathbf{Z}_{p^2}.$$

En particulier $S_{d,f} \otimes \mathbf{Z}_{p^2} \simeq ([\Gamma_+]\backslash\Omega) \otimes \mathbf{Z}_{p^2}$. Cela corrige l'énoncé (3.1).

Soit G le graphe dual de $S_{d,f} \otimes \mathbf{F}_p$. Cela veut dire : les sommets de G sont les composantes irréductibles de $S_{d,f} \otimes \overline{\mathbf{F}}_p$ et les arêtes de G sont les points doubles de $S_{d,f} \otimes \overline{\mathbf{F}}_p$. *Alors* G *est isomorphe à* $\Gamma_+\backslash\Delta$ *et l'action de Frobenius sur* G *s'identifie à l'action de* $\omega$ *sur* $\Gamma_+\backslash\Delta$.

Utilisant cette description de G on peut déterminer les corps $K \supset \mathbf{Q}_p$ pour lesquels $S_{d,f}(K)$ n'est pas vide. ([2]).

**3.7** *Variation sur* $\Omega$. Le schéma formel $\Omega$ peut être vu comme éclatement de la façon suivante :

Soit $\Omega_1$ l'éclatement de $\mathbf{P}^1 \otimes \mathbf{Z}_p$ en les $(p+1)$ points rationels de la fibre spéciale $\mathbf{P}^1 \otimes \mathbf{F}_p$. Ensuite $\Omega_2$ est l'éclatement de $\Omega_1$ en les points rationels de $\Omega_1 \otimes \mathbf{F}_p$ et ainsi de suite.

Soit $\Omega_n^* = \Omega_n - \{$les nouvelles droites exceptionnelles$\}$.

Alors $\Omega = \varinjlim \Omega_n^*$ comme schéma formel.

**3.8** *L'idée de la démonstration de (3.1) et (3.5).*

$S_{d,f}(\overline{\mathbf{F}}_p)$ = l'ensemble des classes d'isomorphisme des triplets $(A, i, B)$ tels que:

(1) $A$ est une surface abélienne sur $\overline{\mathbf{F}}_p$

(2) $i : \theta \hookrightarrow End(A)$

(3) $B \subset A[f]$

(4) les conditions de (2.1).

On prend un triplet $(A, i, B)$. Le module de Tate (usuel)

$$T_p(A) = \varprojlim A[p^n] \simeq \mathbf{Z}_p^r$$

avec $r \in \{0, 1, 2\}$. Le corps non commutatif $\theta \otimes \mathbf{Q}_p = D \otimes \mathbf{Q}_p$ opère sur $T_p(A) \otimes \mathbf{Q}_p$ et alors $r = 0$. On dit dans ce cas là que $A$ est supersingulière.

Soit $\alpha_p$ le schéma en groupes fini donné par $\alpha_p = Spec(\mathbf{F}_p[t]/(t^p))$ et $t \mapsto t \otimes 1 + 1 \otimes t$ (la comultiplication). D'après F. Oort il y a deux possibilités pour une surface abélienne supersingulière.

(i) $A \simeq E \times E$ avec E une courbe elliptique supersingulière fixée .

(ii) $A \simeq E \times E \ / \ M$ où $M$ est un sous-groupe de $E \times E$ isomorphe à $\alpha_p$.

Les familles de surfaces abéliennes supersingulières sont étudiées dans [3].

On considère le groupe formel $\widehat{A}$ de $A$. Comme $A$ est supersingulière cela coïncide avec le groupe $p$-divisible de $A$. Ce qui précède montre que $\widehat{A} \simeq G_{1,1} \times G_{1,1} \ / \ M$ où $G_{1,1}$ est le groupe formel standard de dimension 1 et hauteur 2 et où $M$ est isomorphe a $\alpha_p$.

On utilise maintenant la propriété fonctorielle de $S_{d,f} \otimes \mathbf{Z}_p$ vu comme schéma formel sur $\mathbf{Z}_p$. Cela représente les triplets $(A, i, B)$ sur des schémas $X$ où $p$ est nilpotent. Pour un tel schéma on peut remplacer $A$ par son groupe formel $\widehat{A}$.

Utilisant un théorème de Serre et Tate, à savoir :"il existe une bijection entre l'ensemble des relèvements d'un schéma abélien et l'ensemble des relèvements de son groupe p-divisible", on constate que $S_{d,f} \otimes \mathbf{Z}_p$ représente les familles de groupes formels $G$ avec $\theta$-action et structure de niveau $f$ (sur un $X$ où $p$ est nilpotent) telles que

$$G \otimes \overline{\mathbf{F}}_p \simeq G_{1,1} \times G_{1,1} \ / \ M$$

(*) On considère maintenant l'espace des déformations de $(\theta, G_{1,1} \times G_{1,1} \ / \ M)$. D'après Drinfeld cet espace de déformations est égal à $\Omega \widehat{\otimes} \mathbf{Z}_{p^\infty}$. Au dessus de cet espace il existe une famille $(\theta, G)$. Le groupe $\Gamma = (\theta'[1/p])^*$ opère sur $(\theta, G)$ et $\Omega \widehat{\otimes} \mathbf{Z}_{p^\infty}$. La famille, divisée par l'action de $\Gamma$, est une famille universelle sur $\Gamma \backslash \Omega \otimes \mathbf{Z}_{p^\infty}$ . Cela montre que

$$S_{d,f} \otimes \mathbf{Z}_p \simeq \Gamma \backslash \Omega \otimes \mathbf{Z}_{p^\infty}.$$

Pour la partie (*) il n'existe pas de référence explicite. Remarquons finalement que le lien entre $\theta$ et $\theta$' (ou bien $D$ et $D'$) est donné par le suivant. Prenons le cas $A = E \times E$, alors

finalement que le lien entre $\theta$ et $\theta$' (ou bien $D$ et $D'$) est donné par le suivant. Prenons le cas $A = E \times E$, alors

$$End_\theta (A) \subset End (E \times E) = M(2 \times 2, \theta_{-p})$$

où $\theta_{-p}$ est l'ordre maximal de l'algèbre de quaternions $H_{-p}$ avec discriminant -p. Un calcul explicite montre alors que $End_\theta (A)$ s'identifie à $\theta$'.

**3.9** *Le graphe dual* $\Gamma_+\backslash\Delta$ *de* $S_{d,f} \otimes \mathbf{F}_p$ *en termes de l'arithmétique de* $\theta$' *et* D'.

La méthode est la suivante. L'immeuble de Bruhat-Tits $\Delta$ peut être identifié à l'arbre des $\theta$'-idéaux à gauche de $D'$ (modulo $p^{\mathbf{Z}}$). Un $\theta$'-idéal à gauche $M$ de $D'$ est normalisé si $M \otimes \mathbf{Z}_\ell = \theta' \otimes \mathbf{Z}_\ell$ pour tout $\ell \neq p$. De plus $\{[M_1], [M_2]\}$ est une arête si l'ordre de $M_1/M_2$ est égal à $p^2$.

Ensuite $\Gamma = (\theta'[1/p])^*$ opère par multiplication à gauche. L'ensemble $(\Gamma\backslash\Delta)_0$ des sommets de $\Gamma\backslash\Delta$ est fini et son cardinal $= h =$ le nombre des classes de $\theta'$.

Alors $(\Gamma_+\backslash\Delta)_0 = \{X_1, ..., X_h, X_1', ..., X_h'\}$ et $\omega$ opère avec $\omega(X_i) = X_i'$ ; $\omega^2 = id$.

A chaque arête $y \in (\Gamma_+\backslash\Delta)_1$ on peut donner une longueur $\ell(y) \geq 1$. Soit $a$ le point double correspondant à $y$. Alors le complété de l'anneau local en $a$ possède la forme $\mathbf{Z}_{p^\infty}[[X,Y]]/(XY - p^n)$. Par définition $\ell(y) = n$.

On peut montrer que $\ell(y) =$ l'ordre du stabilisateur de $y$.

Les nombres $h$ et $\ell(y)$ sont connus par des formules d'Eichler.

**3.10** *Un exemple.*

Soit p un nombre premier, $p \equiv 1 mod.12$. On prend $d = 2p$ et $f = 1$. Alors $d' = -2$ , $D' =$ l'algèbre des quaternions de Hamilton, $h(\theta') = 1$ et $|(\theta')^*| = 24$.

Alors $(\Gamma_+\backslash\Delta)_0 = \{X, X'\}$. Un calcul montre que

$$(\Gamma_+\backslash\Delta)_1 = \{y_0, y_1, ..., y_g\}$$

avec $\ell(y_0) = 2$ , $\ell(y_1) = \ell(y_2) = 3$ , $\ell(y_3) = \cdots = \ell(y_g) = 1$.

Le groupe $(\theta')^*/\{\pm 1\}$, stabilisateur du sommet $[\theta'] \in (\Delta)_0$, permute les $(p+1)$ arêtes avec sommet $(\Delta)_0$.

Alors :

$$p+1 = \frac{12}{2} + \frac{12}{3} + \frac{12}{3} + (g-2)\frac{12}{1}$$

et

$$g = \text{ le genre de } S_{2p,1} = \frac{p+11}{12}\,.$$

## 4. Le théorème de Ribet

### 4.1 *La variété de Jacobi d'une courbe admissible*

Soit $C/\mathbf{Z}_\ell$ ($\ell$ un nombre premier) une courbe admissible. Cela veut dire:

(i) $C \otimes \mathbf{Q}_\ell$ est une courbe projective, connexe et non-singulière.

(ii) Les singularités de $C \otimes \mathbf{F}_\ell$ sont des points doubles ordinaires.

Alors la variété de Jacobi de $C \otimes \mathbf{Q}_\ell$ possède un modèle minimal de Néron $J/\mathbf{Z}_\ell$. On sait que la condition "$C$ admissible" implique que J possède une réduction stable. Cela veut dire que la composante $(J \otimes \mathbf{F}_\ell)^0$ de l'élément neutre de $J \otimes \mathbf{F}_\ell$ est une extension d'une variété abélienne $A/\mathbf{F}_\ell$ par un tore $T/\mathbf{F}_\ell$.

Il existe donc une suite exacte de groupes algébriques

$$0 \longrightarrow T \longrightarrow (J \otimes \mathbf{F}_\ell)^0 \longrightarrow A \longrightarrow 0.$$

Le groupe des caractères de $T$ sera appelé le groupe des caractères de $C \otimes \mathbf{Q}_\ell$. Soit $G$ le graphe dual de $C \otimes \mathbf{F}_\ell$. On peut montrer que le groupe des caractères de $C \otimes \mathbf{Q}_\ell$ est canoniquement isomorphe à $H_1(G, \mathbf{Z})$.

Le théorème suivant, montré par Ribet, complète la démonstration (proposée par G. Frey et J.P. Serre) de :

"La conjecture de Taniayama-Weil implique le dernier théorème de Fermat".

**4.2** THÉORÈME (K. Ribet 87/88). *Soient $p \neq q$ des nombres premiers et $M \geq 1$ un entier avec $(M, pq) = 1$ . Soient $Y$, $L$ et $X$ les groupes des caractères des courbes $S_{pq,M} \otimes \mathbf{Q}_p$, $X_0(M_{pq}) \otimes \mathbf{Q}_q$ et $X_0(M_q) \otimes \mathbf{Q}_q$ .*

*Alors il existe une suite exacte naturelle :*

$$0 \longrightarrow Y \longrightarrow L \longrightarrow X \oplus X \longrightarrow 0,$$

*où naturelle veut dire que les morphismes commutent avec l'action des opérateurs de Hecke sur* $Y$, $L$ *et* $X$ .

DÉMONSTRATION.

$Y \simeq H_1$ (graphe dual de $S_{pq,M} \otimes \overline{\mathbf{F}}_p$, $\mathbf{Z}$) et d'après Drinfeld-Čerednik ce graphe dual est $\Gamma_+ \backslash \Delta$ où

$\Delta$ = l'immeuble de Bruhat- Tits de $PGL(2, \mathbf{Q}_p)$;
$\Gamma_+ \subset_2 \Gamma = (\theta_{-q,M}\ [1/p])^* \subset GL(2, \mathbf{Q}_p)$;
$\theta_{-q,M}$ est un ordre d'Eichler de niveau dans
$D_{-q}$ = l'algèbre des quaternions sur $\mathbf{Q}$ ramifiée en $\{\infty, q\}$.

On fait maintenant une *traduction de* $\Delta$ *et* $\Gamma_+ \backslash \Delta$. Fixons $\mathcal{E}_0 = (E_0, B_0) \in X_0(M)(\overline{\mathbf{F}}_q)_{ss}$. C'est-à-dire, $E_0$ est une courbe elliptique supersingulière sur $\overline{\mathbf{F}}_q$ et $B_0$ est un sous-groupe cyclique de $E_0$ d'ordre M.

Alors $\mathrm{End}(\mathcal{E}_0) = \theta_{-q,M}$.

On pose $V_p(\mathcal{E}_0) := T_p(E_0) \otimes \mathbf{Q}_p$ ; c'est un espace vectoriel de dimension 2 sur $\mathbf{Q}_p$.

On considère des paires $(\mathcal{E},\ \alpha)$ avec $\mathcal{E} \in X_0(M)(\overline{\mathbf{F}}_q)_{ss}$ et $\alpha \in Hom(\mathcal{E}, \mathcal{E}_0) \otimes \mathbf{Q}$ tel que $\alpha$ induit un isomorphisme $T_\ell(\mathcal{E}) \longrightarrow T_\ell(\mathcal{E}_0)$ pour tout $\ell \neq p$. (Pour $\ell = q$ il faut lire pour $\mathrm{T}_q$ le module de Dieudonné de la courbe elliptique en question).

La condition sur $\alpha$ est équivalente à :

$$Hom(\mathcal{E},\ \mathcal{E}_0) \otimes \mathbf{Z}\left[\frac{1}{p}\right] = \alpha\, \theta_{-q,M}\left[\frac{1}{p}\right].$$

La paire $(\mathcal{E},\ \alpha)$ induit un réseau $\alpha(T_p(\mathcal{E})) \subset V_p(\mathcal{E}_0)$ (modulo $p^{\mathbf{Z}}$), et donc un élément de $(\Delta)_0$. L'image dans $(\Gamma \backslash \Delta)_0$ ne dépend pas du choix de $\alpha$. On obtient ainsi une bijection $X_0(M)(\overline{\mathbf{F}}_q)_{ss} = \{$ *classes des* $\mathcal{E}\} \longrightarrow (\Gamma \backslash \Delta)_0$.

Le degré d'un $\alpha$ pour une paire $(\mathcal{E},\ \alpha)$ est une puissance de p. En faisant la distinction entre les puissances paires et les puissances impaires on trouve une bijection entre $(\Gamma_+ \backslash \Delta)_0$ et

$$\{ \text{ les paires}(\mathcal{E},\ \alpha),\ \text{degré } \alpha = p^{\ \text{pair}} \}/\approx \amalg \{ \text{ idem}, p^{\ \text{impair}} \}/\approx.$$

Ensuite on donne une description de $(\Gamma_+\backslash\Delta)_1$= les arêtes de $\Gamma_+\backslash\Delta$. Soit $M_1 \subsetneq M_2$ une arête de $\Delta$. Pour un choix convenable des paires $(\mathcal{E}_1, \alpha_1)$, $(\mathcal{E}_2, \alpha_2)$ cela veut dire :

$$\alpha_1\, T_p(\mathcal{E}_1) \subset_p \alpha_2\, T_p(\mathcal{E}_2) \subset V_p(\mathcal{E}_0)\ .$$

On peut supposer dans ce cas degré $\alpha_1 = p^{pair}$ et degré $\alpha_2 = p^{impair}$. Il s'ensuit qu'une arête (orientée) de $\Gamma_+\backslash\Delta$ est une classe d'isomorphie d'une isogénie $\lambda : \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ de degré p. Parce que $\mathcal{E}_1 = (E_1, B_1)$ et $\mathcal{E}_2 = (E_2, B_2)$, $\lambda$ définit un élément $(E_1, \lambda^{-1}(B_2)) \in X_0(Mp)(\overline{\mathbf{F}}_q)_{ss}$. On trouve ainsi une bijection entre $(\Gamma_+\backslash\Delta)_1$ et $X_0(Mp)(\overline{\mathbf{F}}_q)_{ss}$. De plus toutes les arêtes de $\Gamma_+\backslash\Delta$ ont une orientation fixée.

Soit $G$ un graphe fini, connexe où pour chaque arête $z$ est donnée une orientation par l'ordre $z(0)$, $z(1)$ des sommets de $z$. Il existe une suite exacte :

$$0 \longrightarrow H_1(G, \mathbf{Z}) \xrightarrow{a} \mathbf{Z}^{(G)_1} \longrightarrow \mathbf{Z}^{(G)_0} \longrightarrow \mathbf{Z} \longrightarrow 0$$

où les morphismes sont :

$$\Sigma n_i z_i \ \mapsto\ \Sigma n_i(z_i(0) - z_i(1))$$

et

$$\Sigma m_i a_i \ \mapsto\ \Sigma m_i.$$

Dans notre cas spécial $Y = H_1(G, \mathbf{Z})$ , $(G)_1 = X_0(Mp)(\overline{\mathbf{F}}_q)_{ss}$ et $(G)_0$ est la réunion disjointe de deux copies de $X_0(M)(\overline{\mathbf{F}}_q)_{ss}$.

Nous comparons cela avec la réduction $X_0(Mpq) \otimes \overline{\mathbf{F}}_q$. Cette courbe a deux composantes, chacune isomorphe à $X_0(Mp) \otimes \overline{\mathbf{F}}_q$. Les points doubles de la réduction sont obtenus en identifiant les points de $X_0(Mp)(\overline{\mathbf{F}}_q)_{ss}$ de deux composantes par la loi $x \leftrightarrow x^{(p)} = Fr(x)$.

Cette description de $X_0(Mp) \otimes \overline{\mathbf{F}}_q$ montre que $L := H_1$ (le graphe dual de $X_0(Mpq) \otimes \overline{\mathbf{F}}_q$, $\mathbf{Z}$) s'identifie au sous-groupe des éléments de degré 0 de $\mathbf{Z}^{X_0(M\times p)(\overline{\mathbf{F}}_q)_{ss}}$ . De même, $X := H_1$ (le graphe dual de $X_0(Mq) \otimes \overline{\mathbf{F}}_q$, $\mathbf{Z}$) s'identifie au sous-groupe des éléments de degré 0 de $\mathbf{Z}^{X_0(M)(\overline{\mathbf{F}}_q)_{ss}}$. Le morphisme $a$ ci-dessus satisfait $a(Y) \subset L$ et l'on trouve ainsi la suite exacte du théorème (4.2). L'action des opérateurs de Hecke sur $Y$, $L$ et $X$ se traduit facilement en termes de $\Gamma_+\backslash\Delta$, $X_0(M)(\overline{\mathbf{F}}_q)_{ss}$, $X_0(Mp)(\overline{\mathbf{F}}_q)_{ss}$et l'on peut vérifier que la suite exacte (4.2) est naturelle.

Finalement, il faut admettre une faiblesse dans la démonstration. Les composantes irréductibles de la courbe $S_{pq,M} \otimes \overline{\mathbf{F}}_p$ sont définies sur $\mathbf{F}_{p^2}$ au lieu de $\mathbf{F}_p$. Cela ne semble pas trop gêner.

## Bibliographie

[1] V.G. DRINFELD. *Coverings of p-adic symmetric regions,* Funct. Analysis and its appl. **10** (1976) n ° 2, 107-115.

[2] B.W. JORDAN & R.A. LIVNÉ. *Local Diophantine Properties of Shimura curves.* Math. Ann. **270**, 235-248 (198).

[3] T. KATSURA & F. OORT. *Families of supersingular abelian surfaces.* Compositio Math. **62**, 107-167 (1987).

[4] K.A. RIBET. *On modular representations of Gal($\overline{\mathbf{Q}}$/$\mathbf{Q}$) arising from modular forms.* (Preprint Sept. 19, 1988).

[5] K.A. RIBET. *Bimodules and abelian surfaces.* (Preprint, August 10, 1988, PAM-423, Berkeley).

Mathematisch Instituut, Univ. Gröningen
Postbus 800
9700 AV Gröningen
PAYS-BAS