

# Formes modulaires modulo 2 et composantes réelles de jacobiniennes modulaires

Loïc Merel

30 avril 2012

## Abstract

The image of a complex conjugation by a two-dimensional representation of  $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$  in characteristic 2 can be trivial or a non-trivial element of order 2. Since such a representation comes from a modular form  $f$ , we attempt to study such an alternative purely in terms of  $f$ . The component group of the real points of the modular jacobian  $J_1(N)$  plays a role in this question. We give an elementary description of that group. Our method to obtain such a description applies to determine the component group at infinity of the jacobian of modular curves over  $\mathbf{R}$  attached to any subgroup of finite index of  $\text{SL}_2(\mathbf{Z})$ . We show that such a group is always «Eisenstein». We derive a few consequences of this last fact for Galois representations and modular parametrisations.

## Introduction

Soit  $\mathbf{F}_q$  un corps fini de caractéristique 2. Notons  $q$  son cardinal. Soit  $V$  un espace vectoriel de dimension 2 sur  $\mathbf{F}_q$ . Soit  $\rho : \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \rightarrow \text{GL}(V)$  une représentation irréductible. Soit  $c \in \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$  une conjugaison complexe. Deux possibilités se présentent :

- (1)  $\rho(c) = \text{Id}$  (de façon équivalente l'extension de  $\mathbf{Q}$  découpée par  $\rho$  est réelle) ou
- (2)  $\rho(c)$  est (unipotent) d'ordre 2.

La représentation  $\rho$  est modulaire au sens de Serre [17] d'après le théorème de Khare-Wintenberger [7, 8]. Il lui est associé une forme modulaire  $f$  modulo 2. Nous nous proposons de répondre à une question qui nous a été posée par G. Wiese en 2010 : Comment discerner si  $\rho$  est de type (1) ou (2) à partir de  $f$ ? Pour cela nous allons étudier le groupe des composantes des jacobiniennes de courbes modulaires. Nous espérons ainsi avancer un argument pour dire que la situation (2) est en un certain sens «générique». Pour cela, remarquons qu'on peut reformuler l'alternative (1) ou (2) ainsi :

- (1)  $\ker(\rho(c) - 1)/\text{Im}(\rho(c) + 1) = V$  ou
- (2)  $\ker(\rho(c) - 1)/\text{Im}(\rho(c) + 1) = 0$ .

Soit  $\Gamma$  un sous-groupe d'indice fini de  $\text{SL}_2(\mathbf{Z})$  contenant  $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ . Notons  $X_\Gamma = \Gamma \backslash \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$  la courbe modulaire associée (où  $\mathcal{H}$  est le demi-plan supérieur). Supposons que la matrice  $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$  normalise  $\Gamma$  dans  $\text{GL}_2(\mathbf{Z})$ . La courbe modulaire  $X_\Gamma$  est alors définie sur  $\mathbf{R}$  de telle sorte que la conjugaison complexe sur  $X_\Gamma(\mathbf{C})$  est obtenue en passant au quotient l'involution  $z \mapsto -\bar{z}$  de  $\mathcal{H}$ . Notons  $J_\Gamma$  la jacobienne de  $X_\Gamma$ . Voici comment on peut décrire le groupe des composante réelles  $C_\infty(J_\Gamma)$  de  $J_\Gamma$ . Notons  $\hat{C}_\infty(J_\Gamma)$  le dual de Pontryagin de  $C_\infty(J_\Gamma)$ .

Notons  $E$  l'ensemble  $\Gamma \backslash \text{SL}_2(\mathbf{Z})$ . Il est muni d'une action à droite de  $\text{SL}_2(\mathbf{Z})$  et d'une action de  $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$  par conjugaison. Cette dernière sera notée  $e \mapsto \bar{e}$ . Posons  $\sigma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ . Posons  $A = \{a \in E/\bar{a} = a\sigma\}$  et  $B = \{b \in E/\bar{b} = b\}$ . Ces ensembles sont invariants par  $\sigma$ . Notons  $A^\sigma$  et  $B^\sigma$  les ensembles formés par les orbites respectives de  $A$  et  $B$  sous  $\sigma$ .

Notons  $P_\Gamma = \Gamma \backslash \mathbf{P}^1(\mathbf{Q})$  l'ensemble des pointes de  $X_\Gamma$ . Notons  $P_\Gamma^+$  l'ensemble des pointes réelles de  $X_\Gamma$  (c'est l'ensemble des classes  $\Gamma u/v$  avec  $u/v \in \mathbf{P}^1(\mathbf{Q})$  et  $\Gamma u/v = \Gamma(-u/v)$ ).

Pour  $X$  ensemble non vide, on notera  $\mathbf{F}_2[X]^0$  l'hyperplan de  $\mathbf{F}_2[X]$  formé par les éléments de degré 0 et  $\mathbf{F}_2[X]_0$  l'espace quotient  $\mathbf{F}_2[X]/(\sum_{x \in X} [x])$ .

Considérons l'application  $\theta : \mathbf{F}_2[A^\sigma \cup B^\sigma]_0 \rightarrow \mathbf{F}_2[P_\Gamma^+]_0$  qui à l'orbite de  $a \in A$  associe le diviseur  $[a1] - [a(-1)]$  et à l'orbite de  $b \in B$  associe le diviseur  $[b\infty] - [b0]$ . (L'image par  $\theta$  d'un élément de  $A \cap B$  via l'une ou l'autre de ces définitions est égale à 0.) Elle est à valeurs dans  $\mathbf{F}_2[P_\Gamma^+]_0$ .

**Théorème 1** *On a une suite exacte :*

$$0 \rightarrow \hat{C}_\infty(J_\Gamma) \rightarrow \mathbf{F}_2[A^\sigma \cup B^\sigma]_0 \xrightarrow{\theta} \mathbf{F}_2[P_\Gamma^+]_0 \rightarrow C_\infty(J_\Gamma) \rightarrow 0.$$

Il en résulte un algorithme pour calculer le groupe  $C_\infty(J_\Gamma)$ . Une version plus précise du théorème 1 est donnée dans la section 1.5. : le groupe  $C_\infty(J_\Gamma)$  est isomorphe à  $\mathbf{F}_2[\mathcal{C}_\Gamma]^0$ , où  $\mathcal{C}_\Gamma$  est le groupe des composantes connexes d'un graphe  $\mathcal{G}_\Gamma$  dont les sommets sont les éléments de  $P_\Gamma^+$  et les arêtes les éléments de  $A^\sigma \cup B^\sigma$ .

Rappelons que, d'après un théorème de Belyi [1], les courbes modulaires  $X_\Gamma$  parcourent précisément les courbes algébriques définies sur les corps de nombres, vues comme revêtement non ramifié de la droite projective privée de trois points. Un tel revêtement donne lieu à un graphe, dit «dessin d'enfant». L. Pharamond a déterminé l'ensemble des composantes réelles de  $X_\Gamma$  à partir de ce graphe [13]. Toutefois, nous n'avons pas établi le lien, qui existe probablement, avec nos propres calculs.

Rappelons qu'il y a une suite exacte courte canonique (voir section 1.1)

$$0 \rightarrow \hat{C}_\infty(J_\Gamma) \rightarrow J_\Gamma[2](\mathbf{R})/(1-c)J_\Gamma[2](\mathbf{C}) \rightarrow C_\infty(J_\Gamma) \rightarrow 0.$$

**Corollaire 1** *Soit  $T$  une correspondance de  $X_\Gamma$  définie sur  $\mathbf{R}$ . Supposons que  $T$  et sa correspondance duale annulent  $P_\Gamma^+$ . Le groupe  $J_\Gamma[2](\mathbf{R})/(1-c)J_\Gamma[2](\mathbf{C})$  est annulé par tout endomorphisme déduit par transport de structure de  $T$ .*

Lorsque  $\Gamma$  est un groupe de congruence, il en résulte que  $J_\Gamma[2](\mathbf{R})/(1-c)J_\Gamma[2](\mathbf{C})$  est un module sous l'algèbre de Hecke dont le support est contenu dans les idéaux maximaux d'Eisenstein (voir section 1.6). On sait, suite à des théorèmes de B. Mazur [11], K. Ribet [14] et S. Edixhoven [5] que le groupe des composantes des fibres spéciales (en les places finies) des modèles de Néron des jacobiniennes des courbes modulaires associées aux groupes de congruence sont de type Eisenstein.

On peut déterminer complètement  $\hat{C}_\infty(J_\Gamma)$  lorsque  $\Gamma$  est le groupe de congruence  $\pm\Gamma_1(N)$ . C'est l'objet de la deuxième section.

**Théorème 2** *Soit  $N$  un entier  $\geq 5$ .*

*Supposons  $N$  impair. Le groupe  $C_\infty(J_1(N))$  est isomorphe à  $\mathbf{F}_2[(\mathbf{Z}/N\mathbf{Z})^*/\pm 2^{\mathbf{Z}}]^0$ , où  $\pm 2^{\mathbf{Z}}$  est le sous-groupe de  $(\mathbf{Z}/N\mathbf{Z})^*$  engendré par  $-1$  et  $2$ . En particulier,  $J_1(N)(\mathbf{R})$  est connexe si et seulement si  $\{-1, 2\}$  engendre  $(\mathbf{Z}/N\mathbf{Z})^*$  (ce qui n'est pas le cas si  $N$  admet un facteur premier congru à 1 modulo 8).*

*Supposons  $N$  pair, mais pas divisible par 4. Le groupe  $C_\infty(J_1(N))$  est isomorphe à  $\mathbf{F}_2[(\mathbf{Z}/(N/2)\mathbf{Z})^*/\pm 2^{\mathbf{Z}}]^0$ , où  $\pm 2^{\mathbf{Z}}$  est le sous-groupe de  $(\mathbf{Z}/(N/2)\mathbf{Z})^*$  engendré par  $-1$  et  $2$ .*

*Supposons  $N$  divisible par 4. Le groupe  $C_\infty(J_1(N))$  est isomorphe à  $\mathbf{F}_2[(\mathbf{Z}/(N/2)\mathbf{Z})^*/\pm]^0$ .*

On peut se rappeler que la question de l'existence d'une infinité de nombres premiers  $N$  tels que 2 engendre  $(\mathbf{Z}/N\mathbf{Z})^*$  est ouverte (conjecture d'Artin).

Nous donnons quelques indications sur la structure de  $C_\infty(J_1(N))$  comme module sous l'algèbre de Hecke dans la section 2.4, en particulier nous verrons que l'opérateur  $T_2$  y agit comme l'identité.

Mentionnons une conséquence notre étude (corollaire 6) : le degré de toute paramétrisation modulaire d'une courbe elliptique sur  $\mathbf{Q}$  sans point rationnel d'ordre 2 et de discriminant  $> 0$  est pair. François Brunault me signale que ce résultat est dû à F. Calegari et M. Emerton [3]. Notons que, pour l'établir, ces auteurs utilisent que le groupe  $C_\infty(J_0(N))$  est trivial lorsque  $N$  est premier, ce qui est prouvé dans [12], corollaire 3 par une méthode qui nous a servi de prototype.

Dans [4], B. Conrad, S. Edixhoven et W. Stein ont noté que  $C_\infty(J_1(N))$  n'est pas trivial lorsque  $N = 17$  et  $N = 41$  (ce sont les deux premiers nombres premiers congrus à 1 modulo 8).

Ce sont les seules investigations sur  $C_\infty(J_1(N))$  qui nous étaient connues lorsque nous avons commencé ce travail.

Alors que je terminais la rédaction de cet article, j'ai appris que A. Snowden a obtenu des résultats proches sur l'ensemble des composantes réelles des courbes modulaires. François Brunault m'indique l'existence des travaux de H. Jaffee sur l'ensemble des composantes réelles des courbes modulaires  $X(N)$  [6].

## 1 Courbes modulaires sur $\mathbf{R}$

### 1.1 Quelques rappels

Soit  $X$  une surface de Riemann compacte, connexe, non vide et définie sur  $\mathbf{R}$ . Notons  $J$  la jacobienne de  $X$ . Posons  $G_\infty = \text{Gal}(\mathbf{C}/\mathbf{R}) = \{1, c\}$ . Voyons comment l'action du groupe  $G_\infty$  sur  $H_1(X, \mathbf{Z}) = H_1(X(\mathbf{C}), \mathbf{Z})$  détermine le groupe des composantes de  $J(\mathbf{R})$ . Il est utile d'élargir légèrement notre cadre.

Lorsque  $P$  est une partie finie de  $X(\mathbf{C})$  stable par  $G_\infty$ , considérons la jacobienne généralisée  $J^\#$  de  $X$  relativement à  $P$ . C'est une variété semi-abélienne définie sur  $\mathbf{R}$ . Notons  $C_\infty(J^\#)$  le groupe des composantes connexes de  $J^\#(\mathbf{R})$ . On le déduit du groupe d'homologie relative  $H_1(X, P, \mathbf{Z}) = H_1(X(\mathbf{C}), P, \mathbf{Z})$  en utilisant les groupes de cohomologie modifiés de Tate ainsi.

**Proposition 1** *On a les identifications*

$$C_\infty(J^\#) \simeq \text{Hom}(\hat{H}^0(G_\infty, H_1(X, P, \mathbf{Z})), \mathbf{F}_2) \simeq \hat{H}^1(G_\infty, H_1(X - P, \mathbf{Z})).$$

*En particulier, on a des isomorphismes canoniques de groupes*

$$C_\infty(J) \simeq \text{Hom}(\hat{H}^0(G_\infty, H_1(X, \mathbf{Z})), \mathbf{F}_2) \simeq \hat{H}^1(G_\infty, H_1(X, \mathbf{Z}))$$

et

$$\hat{C}_\infty(J) \simeq \hat{H}^0(G_\infty, H_1(X, \mathbf{Z})).$$

*Démonstration.*- Le groupe  $J^\#(\mathbf{C})$  s'identifie à  $H_1(X - P, \mathbf{Z}) \otimes \mathbf{R}/\mathbf{Z}$  [15]. Le lecteur vérifiera que cette identification est compatible à l'action de la conjugaison complexe. Le groupe des composantes réelles  $C_\infty(J^\#)$  de  $J^\#$  s'identifie donc à  $\hat{H}^0(G_\infty, H_1(X - P, \mathbf{Z}) \otimes \mathbf{R}/\mathbf{Z})$ . Or la suite exacte  $0 \rightarrow H_1(X - P, \mathbf{Z}) \rightarrow H_1(X - P, \mathbf{R}) \rightarrow H_1(X - P, \mathbf{Z}) \otimes \mathbf{R}/\mathbf{Z} \rightarrow 0$  donne lieu à la suite exacte longue

$$0 = \hat{H}^0(G_\infty, H_1(X - P, \mathbf{R})) \rightarrow \hat{H}^0(G_\infty, H_1(X - P, \mathbf{R}/\mathbf{Z})) \rightarrow \hat{H}_1(G_\infty, H_1(X - P, \mathbf{Z})) \rightarrow \hat{H}^1(G_\infty, H_1(X - P, \mathbf{R})) = 0$$

et donc à un isomorphisme  $C_\infty(J^\#) \simeq \hat{H}^0(G_\infty, H_1(X - P, \mathbf{R}/\mathbf{Z})) \simeq \hat{H}^1(G_\infty, H_1(X - P, \mathbf{Z}))$ .

La dualité parfaite de  $G_\infty$ -modules :  $H_1(X - P, \mathbf{Z}) \times H_1(X, P, \mathbf{Z}) \rightarrow \mathbf{Z}(1)$  fournie par les produits d'intersection définit un accouplement parfait

$$\hat{H}^1(G_\infty, H_1(X - P, \mathbf{Z})) \times \hat{H}^0(G_\infty, H_1(X, P, \mathbf{Z})) \rightarrow \hat{H}^1(G_\infty, \mathbf{Z}(1)) \simeq \mathbf{F}_2$$

qui produit ainsi l'identification cherchée.

**Proposition 2** *On a les suites exactes courtes (duales l'une de l'autre)*

$$0 \rightarrow \hat{C}_\infty(J) \rightarrow \hat{H}^0(G_\infty, J[2]) \rightarrow C_\infty(J) \rightarrow 0$$

et

$$0 \rightarrow C_\infty(J) \rightarrow \hat{H}^1(G_\infty, J[2]) \rightarrow \hat{C}_\infty(J) \rightarrow 0.$$

*Démonstration.*- Comme on a une identification  $J[2](\mathbf{C}) \simeq H_1(X, \mathbf{Z}) \otimes \frac{1}{2}\mathbf{Z}/\mathbf{Z}$ , on a une suite exacte de  $G_\infty$ -modules

$$0 \rightarrow H_1(X, \mathbf{Z}) \xrightarrow{2} H_1(X, \mathbf{Z}) \rightarrow J[2](\mathbf{C}) \rightarrow 0,$$

qui donne lieu à l'hexagone exact

$$\begin{array}{ccc} & \hat{H}^0(G_\infty, H_1(X, \mathbf{Z})) \xrightarrow{2} \hat{H}^0(G_\infty, H_1(X, \mathbf{Z})) & \\ & \nearrow & \searrow \\ \hat{H}^1(G_\infty, J[2](\mathbf{C})) & & \hat{H}^0(G_\infty, J[2](\mathbf{C})) \\ & \nwarrow & \nearrow \\ & \hat{H}^1(G_\infty, H_1(X, \mathbf{Z})) \xleftarrow{2} \hat{H}^1(G_\infty, H_1(X, \mathbf{Z})) & \end{array} \quad (1)$$

Comme les multiplications par 2 sont nulles, on a les identifications cherchées.

## 1.2 L'homologie relative et l'hexagone (2)

Reprenons les notations de l'introduction et de la section 1.1. Posons  $\mathcal{M} = H_1(X_\Gamma, P_\Gamma, \mathbf{Z})$  et  $\mathcal{M}^0 = H_1(X_\Gamma, \mathbf{Z})$ . Le groupe  $\mathcal{M}$  est décrit en terme de symbole modulaires : pour  $(\alpha, \beta) \in \mathbf{P}^1(\mathbf{Q})^2$ , on note  $\{\alpha, \beta\}$  la classe dans  $\mathcal{M}$  d'un chemin continu de  $\mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$  d'origine  $\alpha$  et d'extrémité  $\beta$ . De tels éléments engendrent  $\mathcal{M}$  [10]. On a suite exacte :

$$0 \rightarrow \mathcal{M}^0 \rightarrow \mathcal{M} \rightarrow \mathbf{Z}[P_\Gamma]^0 \rightarrow 0,$$

où l'application  $\mathcal{M} \rightarrow \mathbf{Z}[P_\Gamma]^0$  associée à  $\{\alpha, \beta\}$  le diviseur  $[\Gamma\alpha] - [\Gamma\beta]$ . L'hexagone exact issu de la cohomologie de Tate s'écrit ainsi [16] :

$$\begin{array}{ccc} & \hat{H}^0(G_\infty, \mathcal{M}^0) \longrightarrow \hat{H}^0(G_\infty, \mathcal{M}) & \\ & \nearrow & \searrow \\ \hat{H}^1(G_\infty, \mathbf{Z}[P_\Gamma]^0) = 0 & & \hat{H}^0(G_\infty, \mathbf{Z}[P_\Gamma]^0) = \mathbf{F}_2[P_\Gamma^+]^0 \\ & \nwarrow & \nearrow \\ & \hat{H}^1(G_\infty, \mathcal{M}) \longleftarrow \hat{H}^1(G_\infty, \mathcal{M}^0) & \end{array} \quad (2)$$

Les égalités  $\hat{H}^0(G_\infty, \mathbf{Z}[P_\Gamma]^0) = \mathbf{F}_2[P_\Gamma^+]^0$  et  $\hat{H}^1(G_\infty, \mathbf{Z}[P_\Gamma]^0) = 0$  résultent du fait que  $P_\Gamma^+$  est non vide (il contient  $\Gamma_\infty$ ). On verra que  $\hat{H}^1(G_\infty, \mathcal{M}) = 0$  et on calculera  $\hat{H}^1(G_\infty, \mathcal{M})$  dans la section suivante.

### 1.3 La suite exacte de Manin et l'hexagone (3)

Pour  $g \in \mathrm{SL}_2(\mathbf{Z})$ , on note  $\xi(g)$  le symbole modulaire  $\{g0, g\infty\}$ , qui ne dépend que de  $\Gamma g$ . On note encore  $\xi$  l'application  $\mathbf{Z}[E] \rightarrow \mathcal{M}$  déduite de  $\xi$  par linéarité. Notons  $c$  l'involution de  $E$  définie par  $e \mapsto -\bar{e}\sigma$ . Posons  $\tau = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ , qui est d'ordre 3 dans  $\mathrm{PSL}_2(\mathbf{Z})$ .

Notons  $E^\sigma$  et  $E^\tau$  les ensembles des orbites de  $E$  sous  $\sigma$  et  $\tau$  respectivement. On a un homomorphisme de groupes  $i_\Delta : \mathbf{Z} \rightarrow \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau]$  qui à 1 associe  $\Delta = (\sum_{e \in E} [e], \sum_{e \in E} [e])$ . Enfin, on a l'homomorphisme de groupe antidiagonal  $\delta' : \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau] \rightarrow \mathbf{Z}[E]$  qui à  $(s, t) \in E^\sigma \times E^\tau$  associe  $\sum_{e \in s} [e] - \sum_{f \in t} [f]$ . Tout cela donne lieu à la suite exacte de Manin [10] :

$$0 \rightarrow \mathbf{Z} \xrightarrow{i_\Delta} \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau] \xrightarrow{\delta'} \mathbf{Z}[E] \xrightarrow{\xi} \mathcal{M} \rightarrow 0.$$

Récrivons-la :

$$0 \rightarrow \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau] / \mathbf{Z}[\Delta] \rightarrow \mathbf{Z}[E] \rightarrow \mathcal{M} \rightarrow 0.$$

Observons qu'on a la relation  $\bar{e}\tau = \bar{e}\sigma\tau^2\sigma$  ( $e \in E$ ), car on a l'identité, cruciale pour notre calcul,

$$\sigma\tau^2\sigma = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \tau \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

dans  $\mathrm{PSL}_2(\mathbf{Z})$ . Par conséquent, l'involution  $e \mapsto -\bar{e}\sigma$  relève l'action de  $c$  sur  $\mathcal{M}$  à  $\mathbf{Z}[E]$  (car  $\overline{\xi(e)} = \xi(\bar{e}) = -\xi(\bar{e}\sigma)$ ) et est compatible à la suite exacte de Manin (elle les laisse stable l'ensemble des orbites sous  $\sigma$  et l'ensemble des orbites sous  $\tau$ ). Notons la encore  $c$ .

Nous allons examiner l'hexagone exact qui est issu de l'action de  $G_\infty$  ainsi définie sur la suite exacte de Manin, après quelques préliminaires. Notons que l'involution  $-c$  définit une involution des ensembles  $E^\sigma$  et  $E^\tau$ , encore notée  $-c$ .

**Lemme 1** 1) L'ensemble des orbites de  $E$  sous  $\sigma$  qui sont invariantes par  $-c$  coïncide avec  $A^\sigma \cup B^\sigma$ . Plus précisément, il est constitué par les singletons de  $A \cap B$ , les paires  $\{a, a\sigma\}$  avec  $a \in A$ , les paires  $\{b, b\sigma\}$  avec  $b \in B$ .

2) L'ensemble des orbites de  $E$  sous  $\tau$  qui sont invariantes par  $-c$  est constitué par les singletons  $\{a\}$  avec  $a \in A$  et  $a\tau = a$  d'une part et les triplets  $\{a, a\tau, a\tau^2\}$  avec  $a \in A$ . Ainsi l'application  $A \rightarrow A^\tau$  qui à un élément associe son orbite sous  $\tau$  est bijective.

*Démonstration.* - 1) Soit  $e \in E$  tel que l'orbite de  $e$  sous  $\sigma$  soit invariante par  $-c$ . Si  $e = e\sigma$ , on a  $e = -\bar{e}$  et  $e = -\bar{e}\sigma$  et donc  $e \in A \cap B$ . Si  $e \neq e\sigma$ , on a  $\bar{e} = e$  (et donc  $e \in B$ ) ou  $\bar{e} = e\sigma$  (et donc  $e \in A$ ), mais en aucun cas on a  $e \in A \cap B$ .

2) Soit  $e \in E$  tel que l'orbite de  $e$  sous  $\tau$  soit invariante par  $-c$ . Si  $e\tau = e$ , on a  $\bar{e} = e\sigma$  et donc  $e \in A$ . Supposons désormais que  $e\tau \neq e$ . L'un des trois éléments  $e, e\tau, e\tau^2$  est fixe par l'involution  $f \mapsto \bar{f}\sigma$ . Il appartient donc à  $A$ . Notons le  $a$ . De plus, on a  $\bar{a}\tau = \bar{a}\sigma\tau^2\sigma = a\tau^2\sigma$ , si bien que  $a$  est l'unique élément du triplet  $\{a, a\tau, a\tau^2\}$  fixé par  $f \mapsto \bar{f}\sigma$ .

**Lemme 2** On a  $\hat{H}^0(G_\infty, \mathbf{Z}[E]) = 0$  et  $\hat{H}^1(G_\infty, \mathbf{Z}[E]) = \mathbf{F}_2[A]$ .

*Démonstration.* - La première assertion résulte du fait que  $c$  est l'opposé d'une involution sur  $E$ . Le groupe  $\hat{H}^1(G_\infty, \mathbf{Z}[E])$  est le  $\mathbf{F}_2$ -espace vectoriel de base formé par les éléments de  $E$  qui sont fixes par  $-c$ . C'est bien  $\mathbf{F}_2[A]$ .

**Lemme 3** 1) On a  $\hat{H}^0(G_\infty, \mathbf{Z}[E^\sigma]) = 0$  et  $\hat{H}^0(G_\infty, \mathbf{Z}[E^\tau]) = 0$ .

2) On a de plus  $\hat{H}^1(G_\infty, \mathbf{Z}[E^\sigma]) = \mathbf{F}_2[A^\sigma \cup B^\sigma]$  et  $\hat{H}^1(G_\infty, \mathbf{Z}[E^\tau]) = \mathbf{F}_2[A]$ .

*Démonstration.* - 1) Cela encore du fait que  $c$  est l'opposé d'une involution sur  $E^\sigma$  et sur  $E^\tau$ .

2) Ces groupes de cohomologie sont les  $\mathbf{F}_2$ -espaces vectoriels de bases les éléments de  $E^\sigma$  et  $E^\tau$  respectivement invariants par  $-c$ . On obtient les identités cherchées par application du lemme 1.

Posons dans  $\mathbf{F}_2[A^\sigma \cup B^\sigma] \times \mathbf{F}_2[A]$ ,  $\Delta' = (\sum_{c \in A^\sigma \cup B^\sigma} [c], \sum_{a \in A} [a])$ .

**Lemme 4** On a les identifications :  $\hat{H}^1(G_\infty, \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau] / \mathbf{Z}\Delta) = \mathbf{F}_2[A^\sigma \cup B^\sigma] \times \mathbf{F}_2[A] / \mathbf{F}_2\Delta'$  et  $\hat{H}^0(G_\infty, \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau] / \mathbf{Z}\Delta) = 0$ .

*Démonstration.*- Le  $G_\infty$ -module  $\mathbf{Z}\Delta$  est caractérisé par  $c(\Delta) = -\Delta$ . On a donc  $\hat{H}^1(G_\infty, \mathbf{Z}\Delta) = \mathbf{F}_2\Delta$  et  $\hat{H}^0(G_\infty, \mathbf{Z}\Delta) = 0$ . Considérons la suite exacte courte de  $G_\infty$ -modules

$$0 \rightarrow \mathbf{Z}\Delta \rightarrow \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau] \rightarrow \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau]/\mathbf{Z}\Delta \rightarrow 0.$$

Comme  $\hat{H}^0(G_\infty, \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau]) = 0$  (lemme 3), l'hexagone exact issu de cette suite exacte s'écrit

$$\begin{array}{ccc} \hat{H}^1(G_\infty, \mathbf{Z}\Delta) = \mathbf{F}_2\Delta & \longrightarrow & \hat{H}^1(G_\infty, \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau]) = \mathbf{F}_2[A^\sigma \cup B^\sigma] \times \mathbf{F}_2[A^\tau] \\ \uparrow & & \downarrow \\ \hat{H}^0(G_\infty, \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau]/\mathbf{Z}\Delta) & & \hat{H}^1(G_\infty, \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau]/\mathbf{Z}\Delta) \\ \uparrow & & \downarrow \\ \hat{H}^0(G_\infty, \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau]) = 0 & \longleftarrow & \hat{H}^0(G_\infty, \mathbf{Z}\Delta) = 0. \end{array} \quad (3)$$

Considérons l'application  $\mathbf{F}_2\Delta \rightarrow \mathbf{F}_2[A^\sigma \cup B^\sigma] \times \mathbf{F}_2[A^\tau]$  issue de la ligne supérieure de l'hexagone. Elle associe à  $\Delta$  l'élément  $\Delta'$ , qui est non nul. C'est donc une application injective et on a les isomorphismes annoncés.

Venons-en à l'hexagone exact issu de la suite exacte de Manin, en utilisant les résultats que nous venons d'accumuler :

$$\begin{array}{ccc} \hat{H}^0(G_\infty, \mathbf{Z}[E]) = 0 & \longrightarrow & \hat{H}^0(G_\infty, \mathcal{M}) \\ \uparrow & & \downarrow \\ \hat{H}^0(G_\infty, \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau]/\mathbf{Z}[\Delta]) = 0 & & \hat{H}^1(G_\infty, \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau]/\mathbf{Z}[\Delta]) = \mathbf{F}_2[A^\sigma \cup B^\sigma] \times \mathbf{F}_2[A^\tau]/\mathbf{F}_2\Delta' \\ \uparrow & & \downarrow \delta \\ \hat{H}^1(G_\infty, \mathcal{M}) = 0 & \longleftarrow & \hat{H}^1(G_\infty, \mathbf{Z}[E]) = \mathbf{F}_2[A]. \end{array} \quad (4)$$

La nullité de  $\hat{H}^1(G_\infty, \mathcal{M})$  n'a pas encore été démontrée. C'est l'objet de la proposition suivante. Posons  $\gamma_0 = \sum_{c \in A^\sigma \cup B^\sigma} [c] \in \mathbf{F}_2[A^\sigma \cup B^\sigma]$ . Remarquons que  $B^\sigma$  est non vide (il contient la classe de l'identité), si bien que  $\gamma_0$  est non nul.

Précisons ce qu'est  $\delta$ . Soient  $c \in A \cup B$  et  $a \in A$  d'orbites respectives  $c^\sigma$  et  $a^\tau$  sous  $\sigma$  et  $\tau$  respectivement. L'image par  $\delta$  de la classe de  $([c], [a])$  est  $\sum_{\gamma \in c^\sigma} [\gamma] - \sum_{\gamma \in a^\tau \cap A} [\gamma]$ .

Considérons l'application linéaire  $\iota : \mathbf{F}_2[A^\sigma \cup B^\sigma] \rightarrow \mathbf{F}_2[A^\sigma \cup B^\sigma] \times \mathbf{F}_2[A^\tau]$  caractérisée par

$$\iota([a^\sigma]) = ([a^\sigma], [a^\tau] + [(a^\sigma)^\tau])$$

si  $a \in A$  et

$$\iota([b^\sigma]) = ([b^\sigma], 0),$$

si  $b \in B$ .

On a  $\iota(\gamma_0) = \Delta'$ , si bien qu'on peut considérer l'application  $\tilde{\iota} : \mathbf{F}_2[A^\sigma \cup B^\sigma]_0 \rightarrow \mathbf{F}_2[A^\sigma \cup B^\sigma] \times \mathbf{F}_2[A]/\mathbf{F}_2\Delta'$  obtenue par passage au quotient.

**Proposition 3** *On a une suite exacte*

$$0 \rightarrow \mathbf{F}_2[A^\sigma \cup B^\sigma]_0 \xrightarrow{\tilde{\iota}} \mathbf{F}_2[A^\sigma \cup B^\sigma] \times \mathbf{F}_2[A^\tau]/\mathbf{F}_2\Delta' \xrightarrow{\delta} \mathbf{F}_2[A] \rightarrow 0.$$

*Démonstration.*- Au vu de l'hexagone (4), cela revient à montrer que  $\delta$  est surjective, que l'image de  $\tilde{\iota}$  est le noyau de  $\delta$  et que  $\tilde{\iota}$  est injective. Le dernier point résulte de l'injectivité de  $\iota$ .

D'après le lemme 2,  $\delta : \mathbf{F}_2[A^\sigma \cup B^\sigma] \times \mathbf{F}_2[A^\tau]/\mathbf{F}_2\Delta' \rightarrow \mathbf{F}_2[A]$  associe à la classe de  $(0, a^\tau)$  l'élément  $[a]$  ( $a \in A$ ). D'où la surjectivité de  $\delta$ .

Passons maintenant au noyau de  $\delta$ . Un élément de l'image de  $\tilde{\iota}$  est dans le noyau de  $\delta$ . Soit  $x$  un élément  $\in \mathbf{F}_2[A^\sigma \cup B^\sigma] \times \mathbf{F}_2[A^\tau]$  dont la classe modulo  $\Delta'$  est dans le noyau de  $\delta$ . Il s'écrit  $x = (\sum_{a \in A} \lambda_a [a] + \sum_{b \in B} \mu_b [b], \sum_{a \in A} \nu_a [a^\tau]) \in \mathbf{F}_2[A^\sigma \cup B^\sigma] \times \mathbf{F}_2[A^\tau]$ , avec  $\lambda_a = \lambda_{a^\sigma}$ ,  $\mu_b = \mu_{b^\sigma}$  ( $a \in A$ ,  $b \in B$ ). On a  $\lambda_a = \nu_a$  ( $a \in A$ ,  $a \notin B$ ), si bien que  $x$  est dans l'image de  $\iota$ .

**Corollaire 2** 1) *On a  $\hat{H}^1(G_\infty, \mathcal{M}) = 0$ .*

2) *Le groupe  $\hat{H}^0(G_\infty, \mathcal{M})$  est isomorphe à  $\mathbf{F}_2[A^\sigma \cup B^\sigma]_0$ .*

**Corollaire 3** *Le groupe des composantes réelles  $C_\infty(J_\Gamma^\#)$  de la jacobienne généralisée  $J_\Gamma^\#$  est isomorphe à  $\mathbf{F}_2[A^\sigma \cup B^\sigma]^0$ .*

*Démonstration.*- D'après la proposition 1,  $C_\infty(J_\Gamma^\#)$  est isomorphe à  $\text{Hom}(\hat{H}^0(G_\infty, \mathcal{M}), \mathbf{F}_2)$ . L'hexagone exact (4) et la proposition 3 identifient ce dernier groupe à  $\text{Hom}(\mathbf{F}_2[A^\sigma \cup B^\sigma]_0, \mathbf{F}_2) \simeq \mathbf{F}_2[A^\sigma \cup B^\sigma]^0$ .

**Corollaire 4** *Toute correspondance de  $X_\Gamma$  définie sur  $\mathbf{R}$  qui laisse stable  $P_\Gamma$  agit sur  $C_\infty(J_\Gamma)$  via  $\mathbf{F}_2[P_\Gamma^+]^0$ .*

*Remarques.*- 1) Au vu du théorème 1, les ensembles  $A^\sigma \cup B^\sigma$  et  $P_\Gamma^+$  ont même cardinal. Cela sera confirmé dans le dénombrement de la section 1.5.

2) Les considérations de cette section devraient découler du fait que chaque composante réelle de  $X_\Gamma$  contient une pointe réelle.

## 1.4 Démonstration du théorème 1

L'hexagone (2) se récrit, en utilisant le corollaire 2, comme la suite exacte suivante

$$0 \rightarrow \hat{H}^0(G_\infty, \mathcal{M}^0) \rightarrow \hat{H}^0(G_\infty, \mathcal{M}) \rightarrow \mathbf{Z}[P_\Gamma^+]^0 \rightarrow \hat{H}^1(G_\infty, \mathcal{M}^0) \rightarrow 0.$$

En utilisant les isomorphismes

$$\hat{H}^0(G_\infty, \mathcal{M}) \simeq \text{Ker}(\delta) \simeq \text{Im}(\tilde{i}) \simeq \mathbf{F}_2[A^\sigma \cup B^\sigma]_0,$$

on peut récrire cette suite exacte ainsi

$$0 \rightarrow \hat{H}^0(G_\infty, \mathcal{M}^0) \rightarrow \mathbf{F}_2[A^\sigma \cup B^\sigma]_0 \xrightarrow{\phi} \mathbf{Z}[P_\Gamma^+]^0 \rightarrow \hat{H}^1(G_\infty, \mathcal{M}^0) \rightarrow 0.$$

Au vu de la proposition 1, il suffit de montrer que l'application  $\phi : \mathbf{F}_2[A^\sigma \cup B^\sigma]_0 \rightarrow \mathbf{Z}[P_\Gamma^+]^0$  coïncide avec l'application  $\theta$  de l'introduction.

Soit  $b \in B$ . Notons  $b^\sigma$  son orbite sous  $\sigma$ . On a  $\iota(b^\sigma) = (b^\sigma, 0)$ , dont l'image modulo  $\Delta'$  dans le noyau de  $\delta$ . On a, dans  $\mathbf{Z}[E]$ , l'identité  $(1-c)[b] = [b] + [b\sigma]$ . L'élément  $\xi(b) \in \mathcal{M}$  est donc invariant par  $c$ . L'élément  $[b] + [b\sigma]$  est antiinvariant par  $c$  et a pour classe  $(b^\sigma, 0)$  dans  $\hat{H}^1(G_\infty, \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau]/\mathbf{Z}[\Delta]) = \mathbf{F}_2[A^\sigma \cup B^\sigma] \times \mathbf{F}_2[A^\tau]/\mathbf{F}_2\Delta'$ . Or on a  $\tilde{i}(b^\sigma) = (b^\sigma, 0)$ . Or l'image de  $\xi(b)$  dans  $\mathbf{F}_2[P_\Gamma^+]^0$  est  $\phi(b) = [b\infty] - [b0] = \theta(b)$  (voir section 1.2).

Soit  $a \in A$ . Notons  $a^\sigma$  son orbite sous  $\sigma$ . On a  $\iota(a^\sigma) = (a^\sigma, \sum_{\alpha \in a^\sigma} [\alpha^\tau])$ . On a dans  $\mathbf{Z}[E]$  :

$$\begin{aligned} (1-c)([a\tau] + [a\sigma\tau^2]) &= [a\tau] + [a\sigma\tau^2] + [a\tau^2] + [a\sigma\tau] \\ &= -[a] - [a\sigma] + [a] + [a\tau] + [a\tau^2] + [a\sigma] + [a\sigma\tau] + [a\sigma\tau^2]. \end{aligned} \quad (5)$$

Cela montre que  $\xi(a\tau) + \xi(a\sigma\tau^2)$  est invariant par  $c$  dans  $\mathcal{M}$ . De plus  $-[a] - [a\sigma] + [a] + [a\tau] + [a\tau^2] + [a\sigma] + [a\sigma\tau] + [a\sigma\tau^2]$  est antiinvariant par  $c$  et a pour classe  $(a^\sigma, \sum_{\alpha \in a^\sigma} [\alpha^\tau])$  dans  $\hat{H}^1(G_\infty, \mathbf{Z}[E^\sigma] \times \mathbf{Z}[E^\tau]/\mathbf{Z}[\Delta]) = \mathbf{F}_2[A^\sigma \cup B^\sigma] \times \mathbf{F}_2[A^\tau]/\mathbf{F}_2\Delta'$ . Son image dans  $\hat{H}^0(G_\infty, \mathcal{M}) \simeq \text{Ker}(\delta) \simeq \text{Im}(\tilde{i}) \simeq \mathbf{F}_2[A^\sigma \cup B^\sigma]_0$  est donc la classe de  $(a^\sigma, \sum_{\alpha \in a^\sigma} [\alpha^\tau])$ , qui à son tour a pour image la classe de  $[a^\sigma]$  par  $\tilde{i}$  (si  $a \neq a\tau$  et  $a\sigma \neq a\sigma\tau$ , c'est évident, sinon il faut utiliser les congruences  $[a] \equiv [a] + [a\tau] + [a\tau^2] \pmod{2\mathbf{Z}[E]}$  ou  $[a\sigma] \equiv [a\sigma] + [a\sigma\tau] + [a\sigma\tau^2] \pmod{2\mathbf{Z}[E]}$ ).

Il reste à calculer l'image de  $\xi(a\tau) + \xi(a\sigma\tau^2)$  dans  $\mathbf{F}_2[P_\Gamma^+]^0$ . C'est

$$\begin{aligned} \phi(a^\sigma) &= [a\tau\infty] - [a\tau 0] + [a\sigma\tau^2\infty] + [a\sigma\tau^2 0] \\ &= [a0] - [a1] + [a(-1)] - [a0] \\ &= [a(-1)] - [a1] \\ &= \theta(a^\sigma). \end{aligned} \quad (6)$$

## 1.5 Le graphe $\mathcal{G}_\Gamma$

Soit  $x \in P_\Gamma^+$ . Notons  $i_x$  l'indice de ramification en  $x$  du morphisme canonique  $X_\Gamma \rightarrow X(1)$ . Posons  $A_x = \{a \in A/a1 = x\}$  et  $B_x = \{b \in B/b\infty = x\}$ .

**Proposition 4** 1) *Si  $i_x$  est impair, les ensembles  $A_x$  et  $B_x$  sont des singletons. On dit alors que  $x$  est de type AB. Si  $a \in A_x$ , on a  $b = a\tau^2(\tau^2\sigma)^{(i_x+1)/2} \in B_x$ .*

2) *Si  $i_x$  est pair, les ensembles  $A_x$  et  $B_x$  sont l'un une paire et l'autre vide. Si  $A_x$  est une paire  $\{a, a'\}$  on dit que  $x$  est de type AA et on a  $a' = a\tau^2(\tau^2\sigma)^{i_x/2}\tau$ . Si  $B_x$  est une paire  $\{b, b'\}$  on dit que  $x$  est de type BB et on a  $b' = b(\tau^2\sigma)^{i_x/2}$ .*

*Démonstration.*- On a  $\tau^2\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  dans  $\mathrm{PSL}_2(\mathbf{Z})$ . C'est le générateur du stabilisateur de  $\infty$  dans  $\mathrm{PSL}_2(\mathbf{Z})$ .

Soit  $e_0 \in E$  tel que  $e_0\infty = x$ . On a  $\{e \in E/e\infty = x\} = e_0(\tau^2\sigma)^{\mathbf{Z}}$ . Comme  $x \in P_\Gamma^+$ , il existe un entier  $k$  tel que  $\bar{e}_0 = e_0(\tau^2\sigma)^k$ , où  $k$  est bien défini modulo  $i_x$ . Soit  $n$  un entier. On a

$$\overline{e_0(\tau^2\sigma)^n} = e_0(\tau^2\sigma)^{k-n} = e_0(\tau^2\sigma)^n(\tau^2\sigma)^{k-2n},$$

si bien que  $e_0(\tau^2\sigma)^n \in B_x$  si et seulement si  $k \equiv 2n \pmod{i_x}$ .

Soit  $f_0 \in E$  tel que  $f_01 = x$ . Comme  $\tau^2\infty = 1$ , on a  $f_0\tau^2\infty = x$  si bien qu'on a  $\{f \in E/f1 = x\} = f_0\tau^2(\tau^2\sigma)^{\mathbf{Z}\tau}$ . Comme  $x \in P_\Gamma^+$ , il existe un entier  $l$  tel que  $\bar{f}_0\tau^2 = f_0\tau^2(\tau^2\sigma)^l$ , où  $l$  est bien défini modulo  $i_x$ . Soit  $m$  un entier. On a

$$\overline{f_0\tau^2(\tau^2\sigma)^m\tau} = f_0\tau^2(\tau^2\sigma)^{l-m}\sigma\tau^2\sigma = f_0\tau^2(\tau^2\sigma)^m(\tau^2\sigma)^{l-1-2m}\tau\sigma,$$

si bien que  $f_0\tau^2(\tau^2\sigma)^m\tau \in A_x$  si et seulement si

$$f_0\tau^2(\tau^2\sigma)^m(\tau^2\sigma)^{l-1-2m}\tau\sigma = f_0\tau^2(\tau^2\sigma)^m\tau\sigma$$

ou encore si et seulement si  $(\tau^2\sigma)^{l-1-2m} \in (\tau^2\sigma)^{i_x\mathbf{Z}}$ , c'est-à-dire  $l-1-2m \equiv 0 \pmod{i_x}$ .

1) Supposons  $i_x$  impair. Les entiers  $n$  et  $m$  ci-dessus existent et sont uniques modulo  $i_x$ . C'est pourquoi  $A_x$  et  $B_x$  sont des singletons. Si  $a \in A_x$ , on a  $b = a\tau^2(\tau^2\sigma)^{(i_x+1)/2} \in B_x$ .

2) Supposons  $i_x$  pair. On peut poser  $f_0 = e_0\tau$  dans le calcul ci-dessus. On a alors  $k \equiv l \pmod{i_x}$ , si bien que  $k$  et  $l$  ont même parité. Si  $k$  est pair (resp. impair), il y a deux possibilités pour  $n$  et aucune pour  $m$  (resp. aucune possibilité pour  $n$  et deux possibilités pour  $m$ ) si bien que  $B_x$  (resp.  $A_x$ ) admet exactement deux éléments et  $A_x$  (resp.  $B_x$ ) est vide.

*Remarque.*- Si l'application canonique  $\Gamma \mapsto \mathrm{SL}_2(\mathbf{Z}/2\mathbf{Z})$  est surjective, ce qui revient à dire que les indices de ramification des pointes dans le morphisme  $X_\Gamma \rightarrow X(1)$  sont impairs, toutes les pointes réelles sont de type  $AB$ . C'est le cas si  $\Gamma$  est un sous-groupe de congruence de niveau impair.

Considérons le graphe  $\mathcal{G}_\Gamma$  dont les sommets sont les éléments de  $P_\Gamma^+$  et dont les arêtes sont de la forme  $(a(-1), a1)$  pour  $a \in A$  ou de la forme  $(b0, b\infty)$  pour  $b \in B$ . D'après la proposition 4, c'est un graphe régulier de valence 2. Notons  $\mathcal{C}_\Gamma$  l'ensemble des composantes connexes de  $\mathcal{G}_\Gamma$ . Ainsi l'application  $\theta$  associée à une arête  $\alpha$  de  $\mathcal{G}_\Gamma$  la différence des sommets attachés à  $\alpha$  si bien que le théorème 1 se reformule ainsi.

**Théorème 3** 1) Le groupe  $C_\infty(J_\Gamma)$  est isomorphe à  $\mathbf{F}_2[\mathcal{C}_\Gamma]^0$  (par l'application qui à la classe dans  $C_\infty(J_\Gamma)$  de la différence de deux pointes réelles associe la différence de leurs composantes connexes dans  $\mathcal{G}_\Gamma$ ).

2) Le groupe  $\hat{C}_\infty(J_\Gamma)$  est isomorphe à  $\mathbf{F}_2[\mathcal{C}_\Gamma]_0$  (par l'inverse de l'application qui à la classe dans  $\mathbf{F}_2[\mathcal{C}_\Gamma]_0$  d'une composante connexe  $C$  associe l'image inverse dans  $\hat{C}_\infty(J_\Gamma)$  de la somme des arêtes de  $C$ ).

*Remarque.*- Nous n'avons pas vérifié que ces deux isomorphismes sont compatibles aux accouplements canoniques  $\mathbf{F}_2[\mathcal{C}_\Gamma]^0 \times \mathbf{F}_2[\mathcal{C}_\Gamma]_0 \rightarrow \mathbf{F}_2$  et  $C_\infty(J_\Gamma) \times \hat{C}_\infty(J_\Gamma) \rightarrow \mathbf{F}_2$  (rappelons que, via les accouplements de la section 1.1, ce dernier est issu de l'accouplement

$$\hat{H}^0(G_\infty, \mathcal{M}^0) \times \hat{H}^1(G_\infty, \mathcal{M}^0) \rightarrow \hat{H}^1(G_\infty, \mathbf{F}_2) \simeq \mathbf{F}_2,$$

qui, à la classe de  $(x, y) \in \mathcal{M}^0 \times \mathcal{M}^0$  avec  $cx = x$  et  $cy = -y$ , associe le produit d'intersection  $x \bullet y$  modulo 2.)

## 1.6 Le groupe des composantes est de type Eisenstein

Soit  $T^\#$  (resp.  $T$ ) un sous-anneau commutatif de  $\mathrm{End}(J_\Gamma^\#)$  (resp.  $\mathrm{End}(J_\Gamma)$ ) engendré par des correspondances de  $X_\Gamma$  définies sur  $\mathbf{R}$  et qui respectent  $P_\Gamma$ . Il opère sur la suite exacte  $0 \rightarrow \mathcal{M}^0 \rightarrow \mathcal{M} \rightarrow \mathbf{Z}[P_\Gamma]^0 \rightarrow 0$ , et donc sur  $\mathbf{Z}[P_\Gamma]^0$ . Notons  $I_E$  l'annulateur de  $\mathbf{Z}[P_\Gamma]^0$  dans  $T^\#$ . Un  $T$ -module (resp.  $T^\#$ -module) est dit de type *Eisenstein* si son support dans le spectre maximal de  $T$  (resp.  $T^\#$ ) est contenu dans le support de l'image de  $I_E$  dans  $T$  (resp. dans le support de  $I_E$ ).

**Proposition 5** 1) Le groupe  $C_\infty(J_\Gamma)$  est un  $T$ -module de type *Eisenstein*.

2) Le  $T$ -module  $J_\Gamma[2](\mathbf{R})/(1-c)J_\Gamma[2](\mathbf{C})$  est de type *Eisenstein*.

*Démonstration.*- Soit  $\mathfrak{M}$  un idéal maximal de  $T$  dans le support de  $C_\infty(J_\Gamma)$ . Il annule  $C_\infty(J_\Gamma)$ . Puisqu'on a un homomorphisme de  $T$ -modules  $\mathbf{F}_2[P_\Gamma^+]^0 \rightarrow C_\infty(J_\Gamma)$ , on a un homomorphisme  $T$ -modules  $\mathbf{Z}[P_\Gamma]^0 \rightarrow C_\infty(J_\Gamma)$ , d'où la première assertion. La seconde assertion se déduit de la première et de la suite exacte de  $T$ -modules rappelée dans la section 1.1  $0 \rightarrow \hat{C}_\infty(J_\Gamma) \rightarrow J_\Gamma[2](\mathbf{R})/(1-c)J_\Gamma[2](\mathbf{C}) \rightarrow C_\infty(J_\Gamma) \rightarrow 0$ .

Cette notion trouve principalement une application lorsque  $\Gamma$  est un sous-groupe de congruence et  $T$  est l'algèbre engendrée par les opérateurs de Hecke.

## 2 Application à la courbe $X_1(N)$

### 2.1 Pointes réelles de $X_1(N)$

Soit  $N$  un entier  $\geq 5$ . Posons  $\Gamma = \pm\Gamma_1(N)$ . Notons  $P_1(N)$  (resp.  $P_1(N)^+$ ) l'ensemble des pointes (resp. des pointes réelles) de  $X_1(N)$ .

Soit  $S$  un système de représentants de  $(\mathbf{Z}/N\mathbf{Z})$  dans  $\mathbf{Z}$ . Pour  $\lambda \in (\mathbf{Z}/N\mathbf{Z})^*$  de représentant  $\tilde{\lambda} \in S$ , notons  $\alpha_\lambda$  (resp.  $\beta_\lambda$ ) la classe de  $1/\tilde{\lambda}$  (resp.  $\tilde{\lambda}/N$ ) dans  $P_1(N)$ . Ces pointes ne dépendent que de  $\pm\lambda$ . Les applications  $\pm\lambda \mapsto \alpha_\lambda$  et  $\pm\lambda \mapsto \beta_\lambda$  sont injectives et d'images disjointes. On dira que leurs images sont les pointes *au dessus de 0 et  $\infty$*  respectivement (car elles sont au dessus des pointes 0 et  $\infty$  de  $X_0(N)$ ).

Si  $N$  est pair, pour  $\lambda \in (\mathbf{Z}/N\mathbf{Z})^*$  de représentant  $\tilde{\lambda} \in S$ , notons  $\gamma_\lambda$  (resp.  $\delta_\lambda$ ) la classe de  $\frac{1}{2\tilde{\lambda}}$  (resp.  $\lambda/(N/2)$ ) dans  $P_1(N)$ . Ces pointes ne dépendent que de  $\pm\lambda$  modulo  $N/2$ . Les applications  $\pm\lambda \pmod{N/2} \mapsto \gamma_\lambda$  et  $\pm\lambda \pmod{N/2} \mapsto \delta_\lambda$  sont injectives et d'images disjointes. On dira que leurs images sont les pointes *au dessus de  $1/2$  et  $2/N$*  respectivement (car elles sont au dessus des pointes  $1/2$  et  $2/N$  de  $X_0(N)$ ).

**Proposition 6** *L'ensemble  $P_1(N)^+$  coïncide avec l'ensemble des pointes au dessus de 0 ou  $\infty$  si  $N$  est impair. Il coïncide avec l'ensemble des pointes au dessus de 0,  $\infty$ ,  $1/2$  ou  $2/N$  si  $N$  est pair.*

*Démonstration.*- Soient  $u$  et  $v$  des entiers premiers entre eux. Notons  $\nu$  le pgcd de  $v$  et  $N$ . La pointe  $\Gamma_1(N)u/v$  ne dépend que du couple  $(v \pmod{N}, u \pmod{\nu}) \in (\mathbf{Z}/N\mathbf{Z}) \times \cup_{d|N}(\mathbf{Z}/d\mathbf{Z})^*$  au signe près. Puisque sa conjuguée complexe est  $\Gamma_1(N)(-u/v)$ , elle est réelle si et seulement si on a  $v \equiv -v \pmod{N}$  ou  $u \equiv -u \pmod{\nu}$ . C'est-à-dire si et seulement si  $2v \equiv 0 \pmod{N}$  ou  $2 \equiv 0 \pmod{\nu}$ . La pointe  $\Gamma_1(N)u/v$  est donc réelle si et seulement si on a  $\nu = 1, 2, N/2$  ou  $N$ . Cela revient à dire que cette pointe est au dessus de 0,  $\infty$ ,  $1/2$  ou  $2/N$ .

*Remarques.*- 1) La courbe  $X_1(N)$  ne possède que des pointes réelles si et seulement si  $N$  est un diviseur de 4 ou de  $2p$  où  $p$  est un nombre premier impair.

2) Les lemmes 5, 6, 7 et 8 établissent le lien entre nos deux classifications des pointes. Si  $N$  est impair, toutes les pointes sont de type AB. Si  $N$  est pair, les pointes au dessus de 0 et au dessus de  $2/N$  sont de type BB et les pointes au dessus de  $\infty$  et  $1/2$  sont de type AB.

### 2.2 Les ensembles $A$ et $B$

Notons  $E_N$  l'ensemble des éléments d'ordre  $N$  de  $(\mathbf{Z}/N\mathbf{Z})^2$  au signe près. L'application  $\pm\Gamma_1(N) \backslash \mathrm{SL}_2(\mathbf{Z}) \rightarrow E_N$  qui à  $\pm\Gamma_1(N) \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  associe la classe de  $(c, d)$  est bijective et compatible à l'action à droite de  $\mathrm{SL}_2(\mathbf{Z})$ . Notons  $A_N$  et  $B_N$  les images de  $A$  et  $B$  dans  $E_N$ .

**Proposition 7** *On a*

$$A_N = \{\pm(\lambda, \lambda), \pm(\lambda, -\lambda)/\lambda \in (\mathbf{Z}/N\mathbf{Z})^*\}.$$

*De plus, si  $N$  est impair, on a*

$$B_N = \{\pm(\lambda, 0), \pm(0, \lambda)/\lambda \in (\mathbf{Z}/N\mathbf{Z})^*\},$$

*si  $N$  est pair mais pas divisible par 4, on a*

$$B_N = \{\pm(\lambda, 0), \pm(0, \lambda)/\lambda \in (\mathbf{Z}/N\mathbf{Z})^*\} \cup \{\pm(\lambda, N/2), \pm(N/2, \lambda)/\lambda \in (\mathbf{Z}/N\mathbf{Z})^* \cup 2(\mathbf{Z}/N\mathbf{Z})^*\}.$$

*enfin si  $N$  est divisible par 4, on a*

$$B_N = \{\pm(\lambda, 0), \pm(0, \lambda), \pm(\lambda, N/2), \pm(N/2, \lambda)/\lambda \in (\mathbf{Z}/N\mathbf{Z})^*\}.$$

*Démonstration.*- Soit  $\pm(u, v) \in E_N$ , avec  $u$  et  $v$  dans  $\mathbf{Z}/N\mathbf{Z}$ . Lorsqu'on identifie  $E$  à  $E_N$ , l'involution  $-c$  de  $E$  définit une involution de  $E_N$  donnée par la formule  $\pm(u, v) = \pm(v, u)$ . On a de plus  $\pm(u, v)\sigma = \pm(-v, u)$ .

On a  $\pm(u, v) \in A_N$  si et seulement si on a  $\pm(-u, v) = \pm(u, v)\sigma = \pm(-v, u)$ . Cela revient à dire que  $\pm u = \pm v$ . Comme  $(u, v)$  est d'ordre  $N$ , on a  $u$  et  $v$  dans  $(\mathbf{Z}/N\mathbf{Z})^*$ , d'où la formule de  $A_N$ .

On a  $\pm(u, v) \in B_N$  si et seulement si on a  $\pm(-u, v) = \pm(u, v)$ . Cela revient à dire que  $2u = 0$  ou  $2v = 0$ . La formule pour  $B_N$  résulte ensuite du fait que  $(u, v)$  est d'ordre  $N$ .

### 2.3 Démonstration du théorème 2

Il faut déterminer le graphe  $\mathcal{G}_\Gamma$  introduit dans la section 1.5 et appliquer le théorème 1. Identifions-le au graphe  $\mathcal{G}_N$  dont les sommets sont les pointes  $P_1(N)^+$  et dont les arêtes sont les orbites sous  $\sigma$  de  $A_N$  et  $B_N$  (via les identifications de la section 2.1).

**Lemme 5** *Soit  $\lambda \in (\mathbf{Z}/N\mathbf{Z})^*$ . Considérons l'arête  $\{\pm(\lambda, \lambda), \pm(-\lambda, \lambda)\} \in A_N^\sigma$ . Si  $N$  est impair, ses extrémités associées sont  $\alpha_{2\lambda}$  et  $\beta_{\lambda-1}$ . Si  $N$  est pair ses extrémités sont  $\gamma_\lambda$  et  $\beta_{\lambda-1}$ .*

*Démonstration.*- Soit  $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$  tel que  $\lambda = \gamma + N\mathbf{Z} = \delta + N\mathbf{Z}$ . On a alors  $\lambda^{-1} = \alpha - \beta + N\mathbf{Z}$ . On a  $g1 = (\alpha + \beta)/(\gamma + \delta)$  et  $g(-1) = (\alpha - \beta)/(\gamma - \delta)$ . On a donc  $\Gamma_1(N)g1 = \Gamma_1(N)(\alpha + \beta)/(\gamma + \delta)$ , qui est  $\alpha_{2\lambda}$  si  $N$  est impair (puisqu'on a  $\alpha + \delta \equiv 2\lambda \pmod{N}$ ) et  $\gamma_\lambda$  sinon. De plus, on a  $\Gamma_1(N)g1 = \Gamma_1(N)\frac{(\alpha-\beta)}{N} = \beta_{\lambda^{-1}}$  car on a  $1 = \alpha\delta - \beta\gamma \equiv (\alpha - \beta)\lambda \pmod{N}$ .

**Lemme 6** Soit  $\lambda \in (\mathbf{Z}/N\mathbf{Z})^*$ . Considérons l'arête  $\{\pm(\lambda, 0), \pm(0, \lambda)\} \in B_N^\sigma$ . Ses extrémités associées sont  $\alpha_\lambda$  et  $\beta_{\lambda^{-1}}$ .

*Démonstration.*- Soit  $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$  tel que  $0 = \gamma + N\mathbf{Z}$  et  $\lambda = \delta + N\mathbf{Z}$ . On a  $\lambda^{-1} = \alpha + N\mathbf{Z}$ . On a  $g\infty = \alpha/\gamma$  et donc  $\Gamma_1(N)g\infty = b_{\lambda^{-1}}$ . On a  $g0 = \beta/\delta$  et donc  $\Gamma_1(N)g0 = \alpha_\lambda$ .

**Lemme 7** Supposons  $N$  pair. Soit  $\lambda \in (\mathbf{Z}/N\mathbf{Z})^*$ . Considérons l'arête  $\{\pm(\lambda, N/2), \pm(N/2, \lambda)\} \in B_N^\sigma$ . Ses extrémités associées sont  $\alpha_\lambda$  et  $\delta_{\lambda^{-1}}$ .

*Démonstration.*- Soit  $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$  tel que  $N/2 \equiv \gamma \pmod{N}$  et  $\lambda = \delta + N\mathbf{Z}$ . On a  $g\infty = \alpha/\gamma$  et donc  $\Gamma_1(N)g\infty = \delta_{\lambda^{-1}}$ . On a  $g0 = \beta/\delta$  et donc  $\Gamma_1(N)g0 = \alpha_\lambda$ .

**Lemme 8** Supposons  $N$  pair, mais non divisible par 4. Soit  $\lambda = 2\mu \in 2(\mathbf{Z}/N\mathbf{Z})^*$ . L'arête  $\{\pm(\lambda, N/2), \pm(N/2, \lambda)\} \in B_N^\sigma$  a pour extrémités les pointes  $\gamma_\mu$  et  $\delta_{(\lambda+N/2)^{-1}}$ .

*Démonstration.*- Soit  $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$  tel que  $N/2 \equiv \gamma \pmod{N}$  et  $\lambda = \delta + N\mathbf{Z}$ . On a  $\lambda + N/2 \in (\mathbf{Z}/N\mathbf{Z})^*$  et donc  $\alpha \equiv \delta_{(\lambda+N/2)^{-1}} \pmod{N/2}$ . On a  $g\infty = \alpha/\gamma$  et donc  $\Gamma_1(N)g\infty = \delta_{(\lambda+N/2)^{-1}}$ . On a  $g0 = \beta/\delta$  et donc  $\Gamma_1(N)g0 = \gamma_\mu$ .

Passons maintenant à la démonstration du théorème 2. Pour cela nous allons identifier le groupe des composantes de  $\mathcal{G}_N$  à un quotient de  $(\mathbf{Z}/N\mathbf{Z})^*/\pm 1$  par l'application qui à la composante de  $\alpha_\lambda$  associe la classe de  $\lambda$ .

Supposons  $N$  impair. On a  $P_1(N)^+ = \{\alpha_\lambda, \beta_\lambda/\lambda \in (\mathbf{Z}/N\mathbf{Z})^*\}$ . D'après les lemmes 5 et 6,  $\alpha_\lambda, \beta_{\lambda^{-1}}$  et  $\alpha_{2\lambda}$  sont dans la même composante connexe de  $\mathcal{G}_N$  pour tout  $\lambda \in (\mathbf{Z}/N\mathbf{Z})^*$ . Comme  $\mathcal{G}_N$  est régulier de valence 2, l'itération de ce processus épuise la composante connexe de  $\alpha_\lambda$ . Il en résulte que la composante connexe de  $\alpha_\lambda$  est  $\{\alpha_\lambda, \beta_{\lambda^{-1}}, \alpha_{2\lambda}, \beta_{(2\lambda)^{-1}}, \dots\} = \{\alpha_{k\lambda}, \beta_{(k\lambda)^{-1}}/k \in 2^{\mathbf{Z}}\}$ . Ainsi, l'application qui à  $\lambda \in (\mathbf{Z}/N\mathbf{Z})^*$  associe la composante connexe de  $\alpha_\lambda$  définit une bijection entre l'ensemble des composantes connexes de  $\mathcal{G}_N$  et l'ensemble  $(\mathbf{Z}/N\mathbf{Z})^*/\pm 2^{\mathbf{Z}}$ .

Supposons  $N$  pair, mais pas divisible par 4. On a  $P_1(N)^+ = \{\alpha_\lambda, \beta_\lambda/\lambda \in (\mathbf{Z}/N\mathbf{Z})^*\} \cup \{\gamma_\lambda, \delta_\lambda/\lambda \in 2(\mathbf{Z}/N\mathbf{Z})^*\}$ . Soit  $\lambda \in (\mathbf{Z}/N\mathbf{Z})^*$ . D'après les lemmes 7 et 8,  $\gamma_\lambda$  et  $\delta_{(2\lambda+N/2)^{-1}}$  sont les extrémités d'une même arête, de même que  $\delta_{(2\lambda+N/2)^{-1}}$  et  $\alpha_{2\lambda+N/2}$ , de même que  $\alpha_{2\lambda+N/2}$  et  $\beta_{(2\lambda+N/2)^{-1}}$ , de même que  $\beta_{(2\lambda+N/2)^{-1}}$  et  $\gamma_{2\lambda+N/2}$ . Or la pointe  $\gamma_\lambda$  ne dépend que de la classe de  $\lambda$  modulo  $N/2$ . C'est pourquoi on a l'identification entre les composantes connexes de  $\mathcal{G}_N$  et  $(\mathbf{Z}/(N/2)\mathbf{Z})^*/\pm 2^{\mathbf{Z}}$ .

Enfin supposons  $N$  divisible par 4. Soit  $\lambda \in (\mathbf{Z}/N\mathbf{Z})^*$ . La combinaison des lemmes 5, 6, 7 et 8 indique que la composante connexe de  $\alpha_\lambda$  est  $\{\alpha_\lambda, \beta_{\lambda^{-1}}, \gamma_\lambda, \beta_{(\lambda+N/2)^{-1}}, \alpha_{\lambda+N/2}, \delta_{\lambda^{-1}}\}$ . Ainsi les composantes connexes de  $\mathcal{G}_N$  sont en bijection avec  $(\mathbf{Z}/(N/2)\mathbf{Z})^*/\pm 1$ .

## 2.4 Action de Hecke

Considérons l'involution  $W_N$  de  $X_1(N)$  qui à  $\Gamma_1(N)z$  associe  $\Gamma_1(N)(-1/Nz)$ . Elle est définie sur  $\mathbf{R}$  (mais pas sur  $\mathbf{Q}$ ). Elle opère sur  $C_\infty(J_1(N))$  de même que les opérateurs de Hecke et les opérateurs diamants.

**Proposition 8** Soit  $p$  un nombre premier. Soit  $\lambda \in (\mathbf{Z}/N\mathbf{Z})^*$ . Considérons la composante connexe  $a_\lambda$  (resp.  $b_\lambda$ ) de la pointe  $\alpha_\lambda$  (resp.  $\beta_\lambda$ ) dans le graphe  $\mathcal{G}_N$ . Si  $p$  ne divise pas  $N$ , on a la formule suivante pour l'action de la correspondance de Hecke  $T_p$  :

$$T_p a_\lambda = p a_{p\lambda} + a_\lambda,$$

et

$$T_p b_\lambda = b_{\lambda/p} + p b_\lambda.$$

Si  $p$  divise  $N$ , les formules sont :

$$T_p a_\lambda = p a_{p\lambda},$$

et

$$T_p b_\lambda = p b_\lambda.$$

De plus, on a

$$W_N a_\lambda = b_{-\lambda} = a_{-\lambda-1}.$$

En particulier, lorsque  $N$  est impair, les opérateurs  $T_2$  et  $W_N T_2 W_N$  sont l'identité sur  $C_\infty(J_1(N))$ . L'action de l'involution  $W_N$  se déduit de  $\lambda \mapsto \lambda^{-1}$  sur  $(\mathbf{Z}/N\mathbf{Z})^*$  lorsqu'on identifie  $C_\infty(J_1(N))$  à un quotient de  $\mathbf{F}_2[(\mathbf{Z}/N\mathbf{Z})^*]_0$  comme dans le théorème 3.

*Démonstration.* - Lorsque  $p$  ne divise pas  $N$ , rappelons quelle est l'action de la correspondance  $T_p$  sur les pointes de  $P_1(N)$ . On a

$$T_p \Gamma_1(N) \frac{u}{v} = \sum_{i=0}^{p-1} \Gamma_1(N) \frac{u+iv}{pv} + \Gamma_1(N) \frac{pmu+nv}{pNu+pv},$$

où  $m$  et  $n$  sont des entiers tels que  $mp - nN = 1$ . Comme on a posé  $\alpha_\lambda = \Gamma_1(N)1/\tilde{\lambda}$ , un calcul facile et classique montre que  $T_p \alpha_\lambda = p\alpha_{p\lambda} + \alpha_\lambda$ . On obtient de même  $T_p \beta_\lambda = \beta_{\lambda/p} + p\beta_\lambda$ , d'où les formules cherchées pour  $T_p$ .

Lorsque  $p$  divise  $N$ , les formules s'obtiennent par des calculs analogues.

L'identité  $W_N a_\lambda = b_{-\lambda}$  est évidente. L'égalité  $b_{-\lambda} = a_{-\lambda-1}$  résulte du lemme 6.

On a donc, dans  $\mathbf{F}_2[P_1(N)^+]^0$ ,  $T_2 \alpha_\lambda = c_{2\lambda}$ . Lorsque  $N$  est impair, les pointes  $\alpha_\lambda$  et  $\alpha_{2\lambda}$  définissent les mêmes composantes connexes de  $\mathcal{G}_N$ . La correspondance  $T_2$  est donc l'identité sur  $\mathbf{F}_2[\mathcal{C}_{\Gamma_1(N)}]$  et donc encore l'identité sur  $C_\infty(J_1(N))$ .

*Remarque .* - Lorsque  $N$  est impair,  $C_\infty(J_1(N))$  ne s'identifie pas au plus grand quotient de  $\mathbf{F}_2[P_1(N)^+]^0$  sur lequel  $T_2$  et  $W_N T_2 W_N$  sont l'identité. Il faut en plus passer au quotient dans lequel les pointes  $\alpha_\lambda$  et  $\beta_{\lambda-1}$  sont identifiées. (Si on tient compte de l'action des opérateurs diamants, il suffit d'identifier  $\Gamma_1(N)0 = \alpha_1$  et  $\Gamma_1(N)\infty = \beta_1$ . En effet les images de ces pointes par le  $\lambda$ -ème opérateur diamant sont  $\alpha_\lambda$  et  $\beta_{\lambda-1}$ .)

En somme, on peut identifier le groupe  $C_\infty(J_1(N))$  au plus grand quotient de  $\mathbf{F}_2[P_1(N)^\infty]^0$  sur lequel  $T_2$  est l'identité, où  $P_1(N)^\infty$  est l'ensemble des pointes de  $X_1(N)$  au dessus de l'infini (un tel ensemble est stable par l'action des opérateurs de Hecke, mais pas par l'action de  $W_N$ ). Nous n'avons pas d'explication au rôle particulier joué par le nombre premier 2 dans cette description.

### 3 Représentations galoisiennes et modules de Hecke

#### 3.1 Rappels sur les représentations galoisiennes

Reprenons les notations de l'introduction, en ne nous limitant pas à la caractéristique 2. Soit  $p$  un nombre premier. Soit  $\mathbf{F}_q$  un corps fini de caractéristique  $p$ . Notons  $q$  son cardinal. Soit  $V$  un espace vectoriel de dimension 2 sur  $\mathbf{F}_q$ . Soit  $\rho : \text{Gal}(\mathbf{Q}/\mathbf{Q}) \rightarrow \text{GL}(V)$  une représentation irréductible et impaire. Elle est modulaire.

Notons  $f$  la forme modulaire associée. Supposons que  $f$  soit de poids 2 et de niveau  $N_\rho$  ou  $N_\rho p$ , où  $N_\rho$  est le conducteur de  $\rho$ . Notons  $N$  le niveau de  $f$ . Notons  $\sum_{n=1}^{\infty} a_n q^n$  le  $q$ -développement de  $f$ . Considérons l'anneau  $\mathbf{T}$  engendré par les opérateurs de Hecke  $T_n$ ,  $n \geq 1$  et les opérateurs «diamants». Notons  $\mathfrak{M}$  l'idéal maximal de  $\mathbf{T}$  engendré par  $p$  et les éléments de la forme  $T_n - a_n$ . Alors, il existe un entier  $r \geq 1$  tel que le module galoisien  $J_1(N)[\mathfrak{M}]$  est isomorphe à  $\rho^r$  [2]. On a  $r > 1$  si et seulement si  $\rho$  est non ramifiée en  $p$  et l'image par  $\rho$  d'une substitution de Frobenius en  $p$  est scalaire [9, 18] (critère de Wiese).

Supposons  $\rho$  non ramifiée en  $p$ , telle que  $\rho(\text{Frob}_p)$  possède une seule valeur propre  $\alpha = a_p$ . Alors  $\rho(\text{Frob}_p)$  peut-être ou non semi-simple. L'algèbre  $\mathbf{T}$  contient l'opérateur  $U_p = T_p$ . On peut paraphraser le critère de Wiese de la façon suivante. On a la semi-simplicité si et seulement l'une des condition équivalentes suivantes est vérifiée :

- (i) On a  $r > 1$ .
- (ii) L'opérateur  $U_p - \alpha$  est nul sur  $J_1(N)[\mathfrak{M}]$ .
- (iii) Le  $\mathbf{T}/\mathfrak{M}$ -espace vectoriel  $\mathcal{M}^0/\mathfrak{M}\mathcal{M}^0$  est de dimension  $> 2$  (il est de dimension 2 sinon).
- (iv) On a  $(U_p - \alpha)\mathcal{M}^0 \subset \mathfrak{M}\mathcal{M}^0$ .

Considérons l'algèbre de Hecke étendue  $\hat{\mathbf{T}}$  définie comme le sous-anneau de  $\text{End}\mathcal{M}^0$  engendré par  $\mathbf{T}$  et  $U_\infty = c$ . Lorsque  $p$  est différent de 2 (la raison de cette restriction apparaît dans la section 3.2), on peut ajouter la condition suivante.

- (v) Le  $\hat{\mathbf{T}}/\mathfrak{M}$ -espace  $\mathcal{M}^0/\mathfrak{M}\mathcal{M}^0$  n'est pas monogène (il est libre de rang 1 sinon).

*Question.* - Soit  $\ell$  un nombre premier différent de  $p$ . Supposons  $\rho$  non ramifiée en  $\ell$  et que  $\rho(\text{Frob}_\ell)$  possède une seule valeur propre. Y a-t-il un critère analogue à celui qui précède pour déterminer si  $\rho(\text{Frob}_\ell)$  est semi-simple ?

Cette question nous paraît analogue au problème de la semi-simplicité de  $\rho(c)$ . Signalons que la réponse ne semble pas résider dans l'action de l'opérateur  $U_\ell$  agissant sur les points de  $p$ -division de la partie  $\ell$ -ancienne de  $J_1(N, \ell)$  (jacobienne de la courbe modulaire associée au groupe  $\Gamma_1(N) \cap \Gamma_0(\ell)$ ).

## 3.2 Formes modulaires modulo 2

Supposons que  $p = 2$ . Nous nous proposons de répondre à la question posée dans l'introduction, en gardant en tête le critère de Wiese donné dans la section 2.1.

Reprenons les notations de l'introduction et de la section 3.1. Le poids de la représentation  $\rho$  est égal à 1 (resp. 2, resp. 4) si  $\rho$  est non ramifiée (resp. ramifiée, mais peu ramifiée, resp. très ramifiée) [17]. Il existe alors une forme modulaire  $f$  de poids 2 et de niveau  $N$  (resp.  $N$ , resp.  $2N$ ) associée à  $\rho$ .

**Proposition 9** *Les assertions suivantes sont équivalentes.*

- (i) On a  $\rho(c) = 1$ .
- (ii) Le  $\mathbf{T}/\mathfrak{M}$ -espace vectoriel  $\mathcal{M}^0/\mathfrak{M}\mathcal{M}^0$  est de dimension  $2r$  (il est de dimension  $r$  sinon).
- (iii) On a  $(1 - U_\infty)\mathcal{M}^0 \subset \mathfrak{M}\mathcal{M}^0$ .
- (iv) On a  $\mathcal{M}^{0+} \subset \mathfrak{M}\mathcal{M}^0$ .

*Démonstration.*- On a  $\rho(c)$  égal à l'identité si et seulement si la conjugaison complexe agit trivialement sur  $J_1(N)[\mathfrak{M}]$ . Or ce dernier  $\mathbf{T}/\mathfrak{M}$ -espace vectoriel est isomorphe au dual de Pontryagin de  $\mathcal{M}^0/\mathfrak{M}\mathcal{M}^0$  de façon compatible aux actions des conjugaisons complexes déjà considérées. La trivialité de  $\rho(c)$  revient donc à affirmer que  $(1 - U_\infty)\mathcal{M}^0 \subset \mathfrak{M}\mathcal{M}^0$ . Cela montre l'équivalence de (i), (ii) et (iii).

Il reste à montrer l'équivalence de (iii) et (iv). Cela revient à montrer que  $\mathfrak{M}$  n'est pas dans le support du  $\mathbf{T}$ -module  $\mathcal{M}^{0+}/(1 + U_\infty)\mathcal{M}^0 \simeq C_\infty(J_1(N))$ . Comme  $\rho$  est irréductible,  $\mathfrak{M}$  n'est pas de type Eisenstein et ne peut donc être dans le support de  $C_\infty(J_1(N))$  d'après la proposition 5.

*Remarque.*- La comparaison avec le critère de Wiese dans la section 3.1, amène curieusement à voir le  $\mathbf{T}$ -module  $\mathcal{M}^0$  muni de l'opérateur  $U_\infty$  comme «ancien» en la place infinie (sans pour autant qu'on puisse identifier un espace «nouveau» dont serait issu les deux sous-modules  $\mathcal{M}^{0+}$  et  $\mathcal{M}^{0-}$ ).

**Corollaire 5** *Supposons que  $\rho(c) = 1$ . L'idéal engendré par 2 est ramifié au dessus de  $\mathfrak{M}$  dans  $\mathbf{T}$ .*

*Démonstration.*- Supposons 2 non ramifié au dessus de  $\mathfrak{M}$ . Considérons le localisé  $\mathcal{M}_{(\mathfrak{M})}^0$  en  $\mathfrak{M}$  de  $\mathcal{M}^0$ . Comme  $\rho$  est irréductible, l'idéal  $\mathfrak{M}$  n'est pas de type Eisenstein, si bien qu'on a  $(1 + c)\mathcal{M}_{(\mathfrak{M})}^0 = \mathcal{M}_{(\mathfrak{M})}^{0+}$  et donc  $\mathcal{M}_{(\mathfrak{M})}^{0+} \subset \mathfrak{M}\mathcal{M}_{(\mathfrak{M})}^0$ . L'idéal engendré par 2 est non ramifié au dessus de  $\mathfrak{M}$  dans  $\mathbf{T}_{(\mathfrak{M})}$ , il est donc engendré par 2. On a donc  $(1 + c)\mathcal{M}_{(\mathfrak{M})}^0 \subset 2\mathcal{M}_{(\mathfrak{M})}^0$ . Cela entraîne que le groupe  $\mathcal{M}_{(\mathfrak{M})}^{0+}$  est 2-divisible, ce qui est absurde puisque  $\mathfrak{M}$  est de caractéristique résiduelle 2.

*Exemple.*- Considérons la courbe modulaire  $X_0(37)$ . Sa jacobienne  $J_0(37)$  est de genre 2. Le groupe des composantes réelles de  $J_0(37)$  est nul [12], si bien que le corollaire ci-dessus s'adapte à  $J_0(37)$  au lieu de  $J_1(37)$ . La variété abélienne  $J_0(37)$  est isogène au produit de courbes elliptiques non mutuellement isogènes  $E_1$  et  $E_2$  dont les discriminants sont  $> 0$ . Les points de 2-division de  $E_1$  et  $E_2$  sont tous réels, si bien que les représentations galoisiennes associées à  $E_1[2]$  et  $E_2[2]$  sont dotées d'une action triviale de la conjugaison complexe. Comme aucun idéal maximal de caractéristique résiduelle 2 de l'algèbre de Hecke de  $J_0(37)$  n'est de type Eisenstein [11], ces représentations sont irréductibles. Le corollaire 5 entraîne que ces deux représentations de  $\text{Gal}(\mathbf{Q}/\mathbf{Q})$  sont isomorphes.

Ainsi, la situation  $\rho(c) = 1$  entraîne une congruence entre formes modulaires de même niveau. Ce phénomène admet-il une incarnation en théorie des déformations ? Il trouve une illustration supplémentaire dans le corollaire suivant qui est un cas particulier d'un résultat de Calegari et Emerton [3].

**Corollaire 6** *Soit  $E$  une courbe elliptique sur  $\mathbf{Q}$  sans point  $\mathbf{Q}$ -rationnel d'ordre 2 et de discriminant  $> 0$ . Soit  $\pi : X_0(N) \rightarrow E$  un morphisme non constant défini sur  $\mathbf{R}$ . Alors, le degré de  $\pi$  est pair.*

*Démonstration.*- Comme le discriminant de  $E$  est  $> 0$  tous les points d'ordre 2 de  $E(\mathbf{C})$  sont réels. La représentation galoisienne  $\rho$  définie par les points de 2-division de  $E$  est de type (1) (au sens de l'introduction) et est irréductible (car  $E$  est sans point rationnel d'ordre 2). Considérons  $H_1(E, \mathbf{Z})$  qui est un  $\mathbf{Z}$ -module libre de rang 2 munit d'une action de  $G_\infty$ . Comme on a  $E[2] \simeq H_1(E, \mathbf{Z})/2H_1(E, \mathbf{Z})$ , et que l'action de  $c$  est triviale sur  $E[2]$ , il existe une base  $(x^+, x^-)$  du  $\mathbf{Z}$ -module  $H_1(E, \mathbf{Z})$  telle que  $cx^+ = x^+$  et  $cx^- = x^-$ . Comme il s'agit d'une base et que le produit d'intersection est un accouplement parfait, on a la formule pour le produit d'intersection :  $x^+ \bullet x^- = 1$ , quitte à changer  $x^+$  en son opposé.

Venons-en à la paramétrisation modulaire. Considérons l'application  $\pi^* : H_1(E, \mathbf{Z}) \rightarrow H_1(X_0(N), \mathbf{Z})$  déduite de  $\pi$ . On a  $\pi^*(x^+) \bullet \pi^*(y) = \deg(\pi)x^+ \bullet x^- = \deg(\pi)$ . Les éléments  $\pi^*(x^+)$  et  $\pi^*(y)$  sont propres pour les opérateurs de Hecke et invariants et anti-invariants respectivement par  $c$ . Notons  $I_E$  l'idéal premier minimal de  $\mathbf{T}$  qui est le noyau commun des applications  $\mathbf{T} \rightarrow H_1(X_0(N), \mathbf{Z})$  qui à  $t$  associent  $t\pi^*(x^+)$  et  $t\pi^*(x^-)$

respectivement. Il est premier à l'annulateur  $I$  de  $\hat{C}_\infty(J_0(N)) \simeq H_1(X_0(N), \mathbf{Z})^+ / (1+c)H_1(X_0(N), \mathbf{Z})$ . En effet, d'une part, l'annulateur de  $\hat{C}_\infty(J_0(N))$  dans  $\mathbf{T}$  est à support dans les idéaux maximaux d'Eisenstein de caractéristique résiduelle 2 et, d'autre part,  $I_E$  est contenu dans un seul idéal maximal de caractéristique résiduelle 2, qui n'est pas d'Eisenstein puisque la représentation galoisienne  $\rho$  est irréductible.

Dans  $\mathbf{T}$ , posons  $1 = t_E + t_C$  où  $t_E \in I_E$  et  $t_C \in I$ . Il existe  $y$  et  $z$  dans  $H_1(X_0(N), \mathbf{Z})$  tels que  $\pi^*(x^+) = (1+c)y + z$  avec  $t_C z \in (1+c)H_1(X_0(N), \mathbf{Z})$ . On a  $z = t_E z + t_C z \in t_E z + (1+c)H_1(X_0(N), \mathbf{Z})$ . On peut donc supposer que  $z$  appartient à  $I_E H_1(X_0(N), \mathbf{Z})$ , si bien que  $z \bullet \pi^*(x^-) = 0$  par auto-adjonction des opérateurs de Hecke pour l'accouplement  $\bullet$ . On a donc

$$\deg(\pi) = \pi^*(x^+) \bullet \pi^*(x^-) = (1+c)y \bullet \pi^*(x^-) + z \bullet \pi^*(x^-) = 2y \bullet \pi^*(x^-) \in 2\mathbf{Z}.$$

*Remarques.*- 1) Le corollaire 6 reste valable si on remplace la paramétrisation par  $X_0(N)$  par la paramétrisation par  $X_1(N)$  (ou par toute autre courbe modulaire).

2) L'hypothèse d'absence de point rationnel d'ordre 2 est nécessaire. En effet,  $X_0(15)$  est elle-même une courbe elliptique de discriminant  $> 0$ , et tous ses points d'ordre 2 sont rationnels.

## Références

- [1] BELYI, G. V. On Galois Extensions of a Maximal Cyclotomic Field. *Mathematics of the USSR-Izvestiya*, 14(2) :247–256, 1980.
- [2] BOSTON, N. ; LENSTRA, H. ; RIBET, K. Quotients of group rings arising from two-dimensional representations. *C. R. Acad. Sci. Paris Sér. I Math.*, 312(4) :323–326, 1991.
- [3] CALEGARI, F. ; EMERTON, M. Elliptic curves of odd modular degree. *Israel J. Math.*, 169 :417–444, 2009.
- [4] CONRAD, B. ; EDIXHOVEN, S. ; STEIN, W.  $J_1(p)$  has connected fibers. *Doc. Math.*, 8 :331–408, 2003.
- [5] EDIXHOVEN, S. L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiniennes des courbes modulaires est «Eisenstein». In *Courbes modulaires et courbes de Shimura (Orsay, 1987/1988)*, pages 159–170. Astérisque 196–197, 1991.
- [6] JAFFEE, H. Degeneration of real elliptic curves. *J. London Math. Soc. (2)*, 17(1) :19–27, 1978.
- [7] KHARE, C. ; WINTENBERGER, J-P. Serre's modularity conjecture. I. *Invent. Math.*, 178(3) :485–504, 2009.
- [8] KHARE, C. ; WINTENBERGER, J-P. Serre's modularity conjecture. II. *Invent. Math.*, 178(3) :505–586, 2009.
- [9] KILFORD, L. J. P. ; WIESE, G. On the failure of the Gorenstein property for Hecke algebras of prime weight. *Experiment. Math.*, 17 :37–52, 2008.
- [10] MANIN Y. Parabolic points and zeta function of modular curves. *Math. USSR Izvestija*, 6(1) :19–64, 1972.
- [11] MAZUR, B. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, 47 :33–186, 1977.
- [12] MEREL, L. L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de  $J_0(p)$ . *J. Reine Angew. Math.*, 477 :71–115, 1996.
- [13] PHARAMOND dit D'COSTA L. Géométrie réelle des dessins d'enfant. *Journal de théorie des nombres de Bordeaux*, 16(3) :639–691, 2004.
- [14] RIBET, K. On the component groups and the Shimura subgroup of  $J_0(N)$ . In *Séminaire de Théorie des Nombres, 1987–1988 (Talence, 1987–1988)*. 1988.
- [15] SERRE, J-P. *Groupes algébriques et corps de classes*. Hermann, Paris, 1959.
- [16] SERRE J-P. *Corps locaux*. Hermann, Paris, 1968.
- [17] SERRE J-P. Sur les représentations modulaires de degré 2 de  $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ . *Duke Math. J.*, 54(1) :179–230, 1987.
- [18] WIESE, G. Multiplicities of Galois representations of weight one, With an appendix by Niko Naumann. *Algebra and Number Theory*, 1(1) :67–85, 2007.