

COMPOSITIO MATHEMATICA

AHMED ABBES

EMMANUEL ULLMO

À propos de la conjecture de Manin pour les courbes elliptiques modulaires

Compositio Mathematica, tome 103, n° 3 (1996), p. 269-286

http://www.numdam.org/item?id=CM_1996__103_3_269_0

© Foundation Compositio Mathematica, 1996, tous droits réservés.

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

NUMDAM

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

A propos de la conjecture de Manin pour les courbes elliptiques modulaires

AHMED ABBES ET EMMANUEL ULLMO

Université Paris–Sud, URA 752, Bat. 425, 91405 Orsay cedex, France, e-mail:
abbes/ullmo@matups.matups.fr

Received 20 April 1995; accepted in final form 4 July 1995

Résumé. On prouve que la constante de Manin d'une courbe elliptique, semi-stable sur $\mathbb{Q}$, de Weil forte, ayant bonne réduction en 2, vaut 1.

Mots clefs: courbes elliptiques de Weil fortes, congruences entre formes modulaires, constante de Manin.

1. Introduction

Soient E une courbe elliptique de Weil forte [7] sur $\mathbb{Q}$ et $\varphi : X_0(N) \rightarrow E$ sa paramétrisation modulaire. Par un théorème de Carayol [3] N est le conducteur de E . Soient $E_{\mathbb{Z}}$ le modèle de Néron de E sur $\mathbb{Z}$, $\Omega_{E/\mathbb{Z}}^1$ le faisceau des différentielles relatives de $E_{\mathbb{Z}}$ sur $\mathbb{Z}$ et α_E une différentielle de Néron c'est à dire une $\mathbb{Z}$ -base de $H^0(E_{\mathbb{Z}}, \Omega_{E/\mathbb{Z}}^1)$. La différentielle $\varphi^*(\alpha_E)$ est un vecteur propre pour tous les opérateurs de Hecke T_p . Elle est donnée par $\varphi^*(\alpha_E) = c_E f_E dq/q$ où f_E est une forme primitive pour $\Gamma_0(N)$ et c_E est une constante rationnelle appelée constante de Manin. On choisit α_E tel que c_E soit positive. Manin conjecture que c_E vaut 1. Soit m le plus grand carré parfait divisant N , il est facile de voir que $c_E \in \mathbb{Z}[\frac{1}{m}]$. Edixhoven [5] montre que c_E est en fait un entier. Mazur [8] a prouvé que c_E est une unité de $\mathbb{Z}[\frac{1}{2m}]$. Ce résultat a été amélioré par Raynaud qui a montré que si m est impair alors la valuation 2-adique $v_2(c_E) \leq 1$ (voir Proposition 3.1).

THÉORÈME A. Soient E une courbe elliptique de Weil forte de conducteur N et p un nombre premier ne divisant pas N . La constante de Manin c_E n'est pas divisible par p .

Pour $p > 2$, le Théorème A est contenu dans les travaux de Mazur. Néanmoins, l'information nouvelle donnée en 2 permet de déduire le corollaire suivant:

COROLLAIRE B. Soient E une courbe elliptique de Weil forte de conducteur impair N et m le plus grand carré parfait divisant N .

- (i) c_E est une unité de $\mathbb{Z}[\frac{1}{m}]$.
- (ii) Si N est sans facteurs carrés et premier à 2 alors la constante de Manin c_E de E vaut 1.

On prouve le théorème A en calculant le degré de la paramétrisation de Weil forte de deux manières différentes. La première est due à Zagier [13], elle compare le degré de la paramétrisation au nombre de congruence r (le plus grand entier r tel qu'il existe une forme modulaire parabolique g de poids 2 pour $\Gamma_0(N)$ à coefficients dans $\mathbb{Z}$, orthogonale à f_E pour le produit scalaire de Petersson et congrue à f_E modulo r). La seconde méthode est géométrique. Elle établit un deuxième lien entre le degré de la paramétrisation φ et le nombre de congruence r faisant intervenir la constante de Manin c_E . Par cette méthode on est naturellement amené à considérer des congruences de f_E relativement à l'espace cotangent en l'origine au modèle de Néron de la jacobienne de $X_0(N)$. On obtient le théorème A en comparant ces deux notions de congruence.

Nous avons inclus dans ce texte (Proposition 3.1) la démonstration du résultat de Raynaud : *si m est impair alors la valuation 2-adique $v_2(c_E) \leq 1$* . Le point central de ce résultat traite du défaut d'exactitude des modèles de Néron semi-abéliens sur un anneau de valuation discrète complet de corps de fractions de caractéristique 0, de corps résiduel de caractéristique $p > 0$ et d'indice de ramification absolu e dans le cas limite $e = p - 1$. Il a été annoncé pour la première fois dans une lettre de M. Raynaud à J. F. Mestre et J. Oesterlé. M. Raynaud nous a communiqué cette lettre et a accepté que nous la publiions en annexe à ce papier.

Notons que dans cette lettre Raynaud a prouvé la conjecture de Manin pour les courbes elliptiques semi-stables sauf peut être dans les deux cas suivants (voir Corollaire A.4)

- (i) E est une courbe elliptique à réduction ordinaire en 2 telle que le groupe des points de 2-torsion $E[2]$ soit produit d'un groupe étale par un groupe de type multiplicatif (comme dans un relèvement canonique de Serre–Tate),
- (ii) E a mauvaise réduction semi-stable en 2 et la valuation 2-adique du discriminant minimal de E est multiple de 2.

Dans le cas semi-stable, il reste donc à prouver la conjecture de Manin pour le cas (ii).

2. Formes modulaires et algèbre de Hecke

2.1. FORMES MODULAIRES

Soit $N \geq 1$ un entier tel que $X_0(N)$ soit de genre non nul. On désigne par $M_0(N)$ l'espace de modules grossier des courbes elliptiques généralisées munies d'un sous-schéma en groupes cyclique d'ordre N qui coupe toute composante irréductible de chaque fibre géométrique. C'est une courbe projective sur $\text{Spec } \mathbb{Z}$ lisse sur $\text{Spec } \mathbb{Z}[1/N]$ dont la fibre générique est $X_0(N)_{\mathbb{Q}}$. Soient m le plus grand carré parfait divisant N et $S = \text{Spec } \mathbb{Z}[\frac{1}{m}]$. La structure de $M_0(N)_S$ a été étudiée par Deligne et Rapoport [4]. Soit p un diviseur premier de N qui ne divise pas m , la fibre $M_0(N)_{\mathbb{F}_p}$ est formée de deux copies de $M_0(\frac{N}{p})_{\mathbb{F}_p}$ qui se coupent

transversalement aux points supersinguliers. La courbe relative $M_0(N)_S$ est donc semi-stable sur S . On désigne par Ω le faisceau dualisant relatif de $M_0(N)_S$ sur S . Pour tout $p \in S$, le morphisme canonique :

$$H^0(M_0(N)_S, \Omega) \otimes_{\mathbb{Z}[\frac{1}{m}]} \mathbb{F}_p \xrightarrow{\sim} H^0(M_0(N)_{\mathbb{F}_p}, \Omega)$$

est un isomorphisme.

On note $\mathcal{S}_{\mathbb{C}}(2, \Gamma_0(N))$ l'espace des formes modulaires paraboliques de poids 2 pour $\Gamma_0(N)$. Il s'identifie canoniquement avec $H^0(X_0(N)_{\mathbb{C}}, \Omega^1)$ où Ω^1 est le faisceau des différentielles holomorphes sur $X_0(N)_{\mathbb{C}}$. Soit $R \subset \mathbb{C}$ un anneau, on désigne par $\mathcal{S}_R(2, \Gamma_0(N))$ le sous-groupe de $\mathcal{S}_{\mathbb{C}}(2, \Gamma_0(N))$ des formes modulaires dont le q -développement (développement de Fourier en la pointe ∞) est à coefficients dans R et par $B^0(R) \subset R[[q]]$ le groupe de ces q -développements. Il est bien connu que $B^0(\mathbb{Z}) \otimes_{\mathbb{Z}} R = B^0(R)$ (ceci découle aussi du Lemme 2.1 de ce texte). On définit pour tout anneau R :

$$B^0(R) = B^0(\mathbb{Z}) \otimes_{\mathbb{Z}} R \subset R[[q]].$$

On note $\mathcal{S}_m = \mathcal{S}_{\mathbb{Z}[\frac{1}{m}]}(2, \Gamma_0(N))$ et $\mathcal{S}_{\mathbb{Z}} = \mathcal{S}_{\mathbb{Z}}(2, \Gamma_0(N))$.

La paire formée par la courbe de Tate sur $\mathbb{Z}[\frac{1}{m}][[q]]$ et son sous-groupe μ_N induit le morphisme:

$$\tau: \text{Spec} \left(\mathbb{Z} \left[\frac{1}{m} \right] [[q]] \right) \rightarrow M_0(N)_S$$

qui identifie $\mathbb{Z}[\frac{1}{m}][[q]]$ au complété formel de $M_0(N)_S$ le long de la section relative à la pointe ∞ . Le q -développement sur $\mathbb{Z}[\frac{1}{m}]$ est le morphisme induit par τ

$$q\text{-exp}: H^0(M_0(N)_S, \Omega) \rightarrow \mathbb{Z} \left[\frac{1}{m} \right] [[q]].$$

C'est un morphisme injectif :

$$q\text{-exp}: H^0(M_0(N)_S, \Omega) \rightarrow B^0 \left(\mathbb{Z} \left[\frac{1}{m} \right] \right). \quad (1)$$

Mazur [6] montre que le q -développement (1) est un isomorphisme sur $\mathbb{Z}$ pour N premier. Dans le cas général, le q -développement n'est pas un isomorphisme sur $\mathbb{Z}[\frac{1}{m}]$. Toutefois, il induit un isomorphisme en toute place p ne divisant pas N

$$q\text{-exp}: H^0(M_0(N)_{\mathbb{F}_p}, \Omega) \xrightarrow{\sim} B^0(\mathbb{F}_p).$$

On note $J_0(N)_{\mathbb{Q}}$ la jacobienne de $X_0(N)_{\mathbb{Q}}$ et $J_0(N)_S$ son modèle de Néron sur S . On désigne par $M_0(N)^l$ le plus grand ouvert de $M_0(N)$ lisse sur S (obtenu en enlevant les points doubles en caractéristique p divisant N et ne divisant pas m). Le plongement canonique $X_0(N)_{\mathbb{Q}} \rightarrow J_0(N)_{\mathbb{Q}}$ qui envoie ∞ sur 0 se prolonge en un morphisme $M_0(N)^l \rightarrow J_0(N)_S$. Ce dernier induit un isomorphisme

$$H^0(J_0(N)_S, \Omega_{J/S}^1) \xrightarrow{\sim} H^0(M_0(N)^l, \Omega) = H^0(M_0(N)_S, \Omega)$$

où $\Omega^1_{J/S}$ est le faisceau des différentielles de $J_0(N)_S$ sur S .

2.2. ALGÈBRE DE HECKE

L'algèbre de Hecke $\mathbb{T}$ est la sous-algèbre de l'algèbre des endomorphismes de $J_0(N)_{\mathbb{Q}}$ engendrée par les opérateurs de Hecke T_p pour p premier ne divisant pas N et les opérateurs d'Atkin U_l pour l premier divisant N (que l'on note aussi T_l). Soit p un nombre premier, l'opérateur T_p est l'endomorphisme de $J_0(N)_{\mathbb{Q}}$ associé à la correspondance de $X_0(N)$ définie du point de vue modulaire par :

$$(E, A) \mapsto \sum_B (E/B, (A+B)/B)$$

où E est une courbe elliptique, A un sous-groupe d'ordre N et B parcourt les sous-groupes d'ordre p de E qui coupent trivialement A . Soit d un diviseur de N tel que d et $\frac{N}{d}$ sont premiers entre eux, l'involution d'Atkin W_d est l'involution de $X_0(N)$ définie du point de vue modulaire par :

$$(E, A) \mapsto (E/A_1, (A + E_d)/A_1)$$

où E est une courbe elliptique, A un sous-groupe d'ordre N , E_d est le sous-groupe des points de d -torsion de E et A_1 l'unique sous-groupe d'ordre d de A .

Quand N est premier, Ribet [10] et Mazur [6] ont montré que $\mathbb{T}$ coïncide avec l'algèbre des endomorphismes de $J_0(N)_{\mathbb{Q}}$.

L'algèbre $\mathbb{T}$ est libre sur $\mathbb{Z}$ de rang g le genre de $X_0(N)$. Elle agit sur $\mathcal{S}_{\mathbb{C}}(2, \Gamma_0(N)) = H^0(X_0(N)_{\mathbb{C}}, \Omega^1) = H^0(J_0(N)_{\mathbb{C}}, \Omega^1)$. Cette action est donnée pour toute forme f de q -développement $f(z) = \sum_{n \geq 1} a_n(f)q^n = \sum_{n \geq 1} a_n q^n$ par :

$$\begin{aligned} T_p^* f &= \sum_n a_{pn} q^n + p \sum_n a_n q^{pn} \\ U_l^* f &= \sum_n a_{ln} q^n \end{aligned} \tag{2}$$

Pour tout entier $n = p^k$ et $k \geq 2$, on pose $T_n = T_p T_{p^{k-1}} - p T_{p^{k-2}}$ si p ne divise pas N et $T_n = (T_p)^k$ sinon et pour $n = \prod_i p_i^{\alpha_i}$ on pose $T_n = \prod_i T_{p_i^{\alpha_i}}$. On a la relation $a_1(T_n^* f) = a_n(f)$.

L'algèbre de Hecke $\mathbb{T}$ préserve $\mathcal{S}_{\mathbb{Z}}(2, \Gamma_0(N))$ et agit par suite sur $B^0(R)$ pour tout anneau R . Elle agit aussi sur $H^0(J_0(N)_S, \Omega^1_{J/S}) = H^0(M_0(N)_S, \Omega)$. Cette action coïncide avec l'action de $\mathbb{T}$ sur $B^0(\mathbb{Z}[\frac{1}{m}])$ via le q -développement.

LEMME 2.1. L'accouplement

$$\mathbb{T} \times \mathcal{S}_{\mathbb{Z}} \rightarrow \mathbb{Z},$$

$$(t, f) \mapsto a_1(t^* f)$$

est parfait.

Preuve. On a sur $\mathbb{C}$ l'accouplement parfait

$$\mathbb{T}_{\mathbb{C}} \times \mathcal{S}_{\mathbb{C}}(2, \Gamma_0(N)) \rightarrow \mathbb{C},$$

$$(t, f) \mapsto a_1(t^* f),$$

où $\mathbb{T}_{\mathbb{C}} = \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{C}$. Il induit donc un isomorphisme

$$\mathcal{S}_{\mathbb{C}}(2, \Gamma_0(N)) \xrightarrow{a_1} \text{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}, \mathbb{C}).$$

Il s'agit de voir que le morphisme induit sur $\mathbb{Z}$

$$\mathcal{S}_{\mathbb{Z}} \xrightarrow{a_1} \text{Hom}_{\mathbb{Z}}(\mathbb{T}, \mathbb{Z})$$

est un isomorphisme. L'injectivité est assurée par l'injectivité sur $\mathbb{C}$. Soit ψ une forme $\mathbb{Z}$ -linéaire sur $\mathbb{T}$. L'isomorphisme sur $\mathbb{C}$ implique l'existence d'une forme modulaire $f \in \mathcal{S}_{\mathbb{C}}(2, \Gamma_0(N))$ telle que $\psi(t) = a_1(t^* f)$. La forme f est en fait dans $\mathcal{S}_{\mathbb{Z}}$ car le coefficient a_n de son q -développement à l'infini est $\psi(T_n)$ qui est dans $\mathbb{Z}$. Ceci implique la surjectivité du morphisme a_1 et termine la preuve du lemme.

Une forme f de $\mathcal{S}_{\mathbb{C}}(2, \Gamma_0(N))$ est dite primitive si elle est nouvelle (orthogonale à l'espace des formes anciennes pour le produit scalaire de Petersson), forme propre pour tous les opérateurs de Hecke et normalisée par $a_1(f) = 1$ où a_1 est le premier coefficient de son q -développement. On lui associe alors le caractère χ_f de $\mathbb{T}$ défini par $t^* f = \chi_f(t) f$ pour tout $t \in \mathbb{T}$.

3. Congruence entre formes modulaires et constante de Manin

On reprend les notations de l'introduction où E est une courbe elliptique de Weil forte de conducteur N et $\varphi: X_0(N) \rightarrow E$ sa paramétrisation modulaire. Soient m le plus grand carré parfait divisant N et $S = \text{Spec } \mathbb{Z}[\frac{1}{m}]$. Le morphisme φ induit deux morphismes sur $\mathbb{Q}$:

$$\varphi_1: E \rightarrow J_0(N)_{\mathbb{Q}}$$

$$\varphi_2: J_0(N)_{\mathbb{Q}} \rightarrow E.$$

On désigne par A le noyau du morphisme φ_2 . Comme E est de Weil forte, le schéma en groupes A est connexe. C'est une variété abélienne. Soit $A^{\vee}$ la variété duale de A . On note A_S (resp. $A_S^{\vee}$) les modèles de Néron de A (resp. de $A^{\vee}$) sur S . On rappelle que $J_0(N)_S$ désigne le modèle de Néron de $J_0(N)_{\mathbb{Q}}$ sur S et E_S celui de E sur S . Par la propriété universelle des modèles de Néron les morphismes φ_1 et φ_2 se prolongent en

$$E_S \xrightarrow{\varphi_1} J_0(N)_S \longrightarrow A_S^{\vee},$$

$$A_S \longrightarrow J_0(N)_S \xrightarrow{\varphi_2} E_S.$$

Soient φ_1^* et φ_2^* les morphismes:

$$H^0(J_0(N)_S, \Omega_{J/S}^1) \xrightarrow{\varphi_1^*} H^0(E_S, \Omega_{E/S}^1)$$

$$H^0(E_S, \Omega_{E/S}^1) \xrightarrow{\varphi_2^*} H^0(J_0(N)_S, \Omega_{J/S}^1)$$

induits par φ_1 et φ_2 .

PROPOSITION 3.1 (Mazur–Raynaud). *Soient E une courbe elliptique de Weil forte de conducteur N et m le plus grand carré parfait divisant N . Si m est impair alors la valuation 2-adique $v_2(c_E) \leq 1$.*

Preuve. Considérons la suite exacte de variétés abéliennes $1 \rightarrow A_{\mathbb{Q}} \rightarrow J_0(N)_{\mathbb{Q}} \rightarrow E_{\mathbb{Q}} \rightarrow 1$ et la suite $A_{\mathbb{Z}_2} \rightarrow J_0(N)_{\mathbb{Z}_2} \rightarrow E_{\mathbb{Z}_2}$ des $\mathbb{Z}_2$ -modèles de Néron correspondante. Comme $J_0(N)_{\mathbb{Z}_2}$ est à réduction semi-abélienne, le théorème A.1 (voir annexe) implique l'existence d'un entier r ($= 1$ ou 0) tel que la suite

$$0 \rightarrow \mathrm{Lie}(A_{\mathbb{Z}_2}) \rightarrow \mathrm{Lie}(J_0(N)_{\mathbb{Z}_2}) \rightarrow \mathrm{Lie}(E_{\mathbb{Z}_2}) \rightarrow (\mathbb{Z}/2\mathbb{Z})^r \rightarrow 0$$

est exacte. Soit H le conoyau du morphisme $\mathrm{Lie}(A_{\mathbb{Z}_2}) \rightarrow \mathrm{Lie}(J_0(N)_{\mathbb{Z}_2})$. C'est un $\mathbb{Z}_2$ -module libre de rang 1. On désigne par $H^{\vee}$ son dual sur $\mathbb{Z}_2$ et par β une base de $H^{\vee}$. On a alors les deux suites exactes

$$0 \rightarrow H^{\vee} \rightarrow H^0(J_0(N)_{\mathbb{Z}_2}, \Omega^1) \rightarrow H^0(A_{\mathbb{Z}_2}, \Omega^1) \rightarrow 0, \quad (3)$$

$$0 \rightarrow H^0(E_{\mathbb{Z}_2}, \Omega^1) \rightarrow H^{\vee} \rightarrow (\mathbb{Z}/2\mathbb{Z})^r \rightarrow 0. \quad (4)$$

Considérons le diagramme suivant

$$\begin{array}{ccc} H^{\vee} \otimes \mathbb{F}_2 & \xrightarrow{i} & H^0(M_0(N)_{\mathbb{F}_2}, \Omega) \\ & & \downarrow q\text{-exp} \\ & & \mathbb{F}_2[[q]] \end{array}$$

où i est injectif à cause de la suite (3).

On remarque que le q -développement de $\bar{\beta}$ (classe de β modulo 2) est non nul. En effet, si N est impair $M_0(N)_{\mathbb{F}_2}$ est lisse et la nullité du q -développement de $\bar{\beta}$ implique que $\bar{\beta} = 0$ ce qui n'est pas le cas. Si N est pair alors $M_0(N)_{\mathbb{F}_2}$ est formée de deux composantes irréductibles. La nullité du q -développement de $\bar{\beta}$ implique que $\bar{\beta}$ est nulle sur la composante irréductible de la pointe ∞ . Or $\bar{\beta}$ est propre pour l'involution d'Atkin W_N qui échange les deux composantes irréductibles. Il s'en suit que $\bar{\beta}$ est nulle sur $M_0(N)_{\mathbb{F}_2}$ ce qui n'est pas le cas.

Si $r = 0$ alors $\alpha_E = \beta$ et le q -développement de $\bar{\beta}$ est donné par la classe de $c_E(q + a_2q^2 + \dots)$ modulo 2 où $q + a_2q^2 + \dots$ est le q -développement de f_E . Il découle que $v_2(c_E) = 0$.

Si $r = 1$ alors $\alpha_E = 2\beta$ et c_E est multiple de 2. Le q -développement de $\overline{\beta}$ est alors donné par la classe de $c_E/2(q + a_2q^2 + \dots)$ modulo 2. Ceci implique que $v_2(c_E) = 1$.

LEMME 3.1. *On désigne par $W(f_E)$ l'orthogonal à la forme primitive f_E dans $\mathcal{S}_{\mathbb{C}}(2, \Gamma_0(N))$ pour le produit scalaire de Petersson. On a alors la suite exacte de $\mathbb{T}$ -modules:*

$$0 \rightarrow W(f_E) \rightarrow \mathcal{S}_{\mathbb{C}}(2, \Gamma_0(N)) \xrightarrow{\varphi_1^*} H^0(E_{\mathbb{C}}, \Omega^1) \rightarrow 0. \tag{5}$$

Preuve. Comme $\varphi_1^* \neq 0$ et $\dim H^0(E_{\mathbb{C}}, \Omega^1) = 1$ alors φ_1^* est surjectif. Il reste à prouver que $W(f_E)$ est dans le noyau de φ_1^* . La théorie d'Atkin-Lehner [1] implique que $W(f_E)$ est somme directe de classes, chaque classe est formée de formes propres pour tous les opérateurs T_p (p premier à N) avec les mêmes valeurs propres. Soient g une forme d'une telle classe et $g = \sum_{n \geq 1} b_n q^n$ son développement de Fourier à l'infini. Soit $f_E = \sum_{n \geq 1} a_n q^n$ le développement de Fourier de f_E . Soit p un premier ne divisant pas N . L'opérateur de Hecke T_p agit sur E comme la multiplication par a_p . Il s'en suit que $T_p^*(\varphi_1^*(g)) = a_p \varphi_1^*(g)$. Or $T_p^*(\varphi_1^*(g)) = \varphi_1^*(T_p(g)) = b_p \varphi_1^*(g)$. Comme les classes de f_E et de g sont différentes, il existe au moins un p tel que $a_p \neq b_p$, on déduit que $\varphi_1^*(g) = 0$. Ceci termine la preuve du lemme.

On considère l'analogue de la suite exacte (5) sur $\mathbb{Z}[\frac{1}{m}]$:

$$0 \rightarrow L_1 \rightarrow H^0(M_0(N)_S, \Omega) \xrightarrow{\varphi_1^*} I \rightarrow 0, \tag{6}$$

où I est l'image de $H^0(J_0(N)_S, \Omega^1_{J/S}) = H^0(M_0(N)_S, \Omega)$ dans $H^0(E_{\mathbb{C}}, \Omega^1)$ et

$$L_1 = W(f_E) \cap H^0(M_0(N)_S, \Omega).$$

On a alors une injection canonique de I dans $H^0(E_S, \Omega^1_{E/S})$ dont le conoyau sera noté $\mathcal{D}$.

$$0 \rightarrow I \rightarrow H^0(E_S, \Omega^1_{E/S}) \rightarrow \mathcal{D} \rightarrow 0.$$

En fait on a la proposition suivante qui montre que $\mathcal{D}$ est trivial mais ce résultat basé sur le Théorème A.1 de Raynaud n'est pas indispensable (et ne sera pas utilisé) pour la preuve du Théorème A.

PROPOSITION 3.2. *Soient E une courbe elliptique de Weil forte de conducteur N , et m le plus grand carré parfait divisant N . On a la suite exacte de $\mathbb{Z}[\frac{1}{m}]$ -modules libres*

$$\begin{aligned} 0 \rightarrow W(f_E) \cap H^0(J_0(N)_S, \Omega^1_{J/S}) &\rightarrow H^0(J_0(N)_S, \Omega^1_{J/S}) \\ &\xrightarrow{\varphi_1^*} H^0(E_S, \Omega^1_{E/S}) \rightarrow 0 \end{aligned}$$

Preuve. Le seul point non évident est la surjectivité de φ_1^* . Soit $p \in S$ un nombre premier différent de 2. Comme E est de Weil forte, φ_1 est une immersion fermée sur $\mathbb{Q}$. Le modèle de Néron $J_0(N)_{\mathbb{Z}}$ est à réduction semi-abélienne, par un théorème de Raynaud ([2] théorème 4 page 187) le morphisme qui étend φ_1 aux modèles de Néron sur $\mathbb{Z}_p$ est aussi une immersion fermée. D'où la surjectivité de φ_1^* sur $\mathbb{Z}_p$ pour $p \neq 2$.

Si 2 ne divise pas m , le théorème précédent ne s'applique plus sur $\mathbb{Z}_2$. On utilise alors le Théorème A.1 qui implique en particulier que la suite des algèbres de Lie

$$0 \rightarrow \mathrm{Lie}(E_{\mathbb{Z}_2}) \rightarrow \mathrm{Lie}(J_0(N)_{\mathbb{Z}_2}) \rightarrow \mathrm{Lie}(A_{\mathbb{Z}_2}^{\vee})$$

est exacte. Ceci montre que le conoyau de $\mathrm{Lie}(E_{\mathbb{Z}_2}) \rightarrow \mathrm{Lie}(J_0(N)_{\mathbb{Z}_2})$ est sans torsion donc libre. On en déduit la surjectivité de la flèche duale c'est à dire de φ_1^* sur $\mathbb{Z}_2$. Ceci termine la preuve de la Proposition 3.2.

La suite exacte (6) sera comparée à une autre suite exacte obtenue en remplaçant $H^0(M_0(N)_S, \Omega)$ par $\mathcal{S}_m = \mathcal{S}_{\mathbb{Z}[\frac{1}{m}]}(2, \Gamma_0(N))$. On a alors le diagramme suivant:

$$\begin{array}{ccccccc} 0 & \longrightarrow & L_1 & \longrightarrow & H_0(M_0(N)_s, \Omega) & \xrightarrow{\varphi_1^*} & I \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & L_2 & \longrightarrow & \mathcal{S}_m & \longrightarrow & \varphi_1^*(\mathcal{S}_m) \longrightarrow 0 \end{array}$$

où $\varphi_1^*(\mathcal{S}_m)$ est l'image de $\mathcal{S}_m$ par φ_1^* dans $H^0(E_{\mathbb{C}}, \Omega^1)$ et $L_2 = W(f_E) \cap \mathcal{S}_m$.

Le conoyau de la flèche naturelle $I \rightarrow \varphi_1^*(\mathcal{S}_m)$ sera noté $\mathcal{C}$.

On appelle nombre de congruence et on note r l'entier positif défini par l'une des propriétés équivalentes suivantes:

- (i) $r = \#(\mathcal{S}_{\mathbb{Z}}(2, \Gamma_0(N)) / (W(f_E) \cap \mathcal{S}_{\mathbb{Z}}(2, \Gamma_0(N)) \oplus \mathbb{Z}f_E))$.
- (ii) r est le plus grand entier tel qu'il existe une forme modulaire g dans $\mathcal{S}_{\mathbb{Z}}(2, \Gamma_0(N)) \cap W(f_E)$ vérifiant $f_E \equiv g \pmod{r}$ (c'est à dire que f_E et g ont même q -développement dans $B^0(\mathbb{Z}/r\mathbb{Z})$).

PROPOSITION 3.3. Soient E une courbe elliptique de Weil forte de conducteur N , et m le plus grand carré parfait divisant N . Soit $p \in S = \mathrm{Spec} \mathbb{Z}[\frac{1}{m}]$ et v_p la valuation p -adique, on a:

$$v_p(\deg \varphi) + v_p(\#\mathcal{C}) = v_p(r) + v_p(c_E) + v_p(\#D).$$

Preuve. Le degré de la paramétrisation modulaire $\varphi: X_0(N) \rightarrow E$ est

$$\deg \varphi = \#H^0(E_{\mathbb{Z}}, \Omega^1) / \mathbb{Z}\varphi_1^*(c_E f_E),$$

où $E_{\mathbb{Z}}$ est le modèle de Néron de E sur $\mathbb{Z}$. En effet $\varphi_2 \circ \varphi_1$ est la multiplication par $\deg \varphi$ sur E et $\varphi_2^*(\alpha_E) = c_E f_E$. On considère les suites exactes

$$0 \rightarrow I/\mathbb{Z} \left[\frac{1}{m} \right] \varphi_1^*(c_E f_E) \rightarrow \varphi_1^*(\mathcal{S}_m)/\mathbb{Z} \left[\frac{1}{m} \right] \varphi_1^*(c_E f_E) \rightarrow \mathcal{C} \rightarrow 0,$$

$$0 \rightarrow I/\mathbb{Z} \left[\frac{1}{m} \right] \varphi_1^*(c_E f_E) \rightarrow H^0(E_S, \Omega_{E/S}^1)/\mathbb{Z} \left[\frac{1}{m} \right] \varphi_1^*(c_E f_E) \rightarrow \mathcal{D} \rightarrow 0.$$

Elles montrent que

$$\begin{aligned} & \#(\varphi_1^*(\mathcal{S}_m)/\mathbb{Z} \left[\frac{1}{m} \right] \varphi_1^*(c_E f_E)) \# \mathcal{D} \\ &= (c_E)_m \#(\varphi_1^*(\mathcal{S}_m)/\mathbb{Z} \left[\frac{1}{m} \right] \varphi_1^*(f_E)) \# \mathcal{D} = (\deg \varphi)_m \# \mathcal{C}, \end{aligned} \quad (7)$$

où $(\deg \varphi)_m$ (resp. $(c_E)_m$) est le plus grand diviseur de $\deg \varphi$ (resp. de c_E) premier à m . Le morphisme φ_1^* établit un isomorphisme entre

$$\mathcal{S}_m / \left(\mathbb{Z} \left[\frac{1}{m} \right] f_E \oplus L_2 \right) \xrightarrow{\sim} \varphi_1^*(\mathcal{S}_m)/\mathbb{Z} \left[\frac{1}{m} \right] \varphi_1^*(f_E).$$

D'autre part on a un isomorphisme

$$\begin{aligned} & \mathcal{S}_{\mathbb{Z}}(2, \Gamma_0(N)) / (W(f_E) \cap \mathcal{S}_{\mathbb{Z}}(2, \Gamma_0(N)) \oplus \mathbb{Z} f_E) \otimes \mathbb{Z} \left[\frac{1}{m} \right] \\ & \xrightarrow{\sim} \mathcal{S}_m / \left(L_2 \oplus \mathbb{Z} \left[\frac{1}{m} \right] f_E \right). \end{aligned}$$

Il découle que $\#(\varphi_1^*(\mathcal{S}_m)/\mathbb{Z}[\frac{1}{m}]\varphi_1^*(f_E)) = r_m$ où r_m est le plus grand diviseur de r premier à m . On obtient la proposition en prenant la valuation p -adique dans l'équation (7).

Remarque. En utilisant la Proposition 3.2, la Proposition 3.3 devient:

$$v_p(\deg(\varphi)) + v_p(\# \mathcal{C}) = v_p(r) + v_p(c_E).$$

PROPOSITION 3.4. *Sous les conditions et avec les notations précédentes, tout diviseur premier de $\# \mathcal{C}$ divise N . De plus $\mathcal{C}$ est trivial si N est premier.*

Preuve. Soit p un nombre premier ne divisant pas N . On a l'isomorphisme (voir Section 2.1)

$$H^0(M_0(N)_{\mathbb{F}_p}, \Omega) \xrightarrow{\sim} \mathcal{S}_m \otimes_{\mathbb{Z}[\frac{1}{m}]} \mathbb{F}_p.$$

On en déduit l'isomorphisme

$$I \otimes_{\mathbb{Z}[\frac{1}{m}]} \mathbb{F}_p \xrightarrow{\sim} \varphi_1^*(\mathcal{S}_m) \otimes_{\mathbb{Z}[\frac{1}{m}]} \mathbb{F}_p.$$

D'où p ne divise pas $\#C$. Le cas de N premier découle de l'isomorphisme

$$H^0(M_0(N)_{\mathbb{Z}}, \Omega) \xrightarrow{\sim} S_{\mathbb{Z}}.$$

Pour prouver le Théorème A, on a besoin d'introduire quelques notations et de rappeler un résultat de Zagier [13]. Considérons le diagramme

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \longrightarrow & J_0(N)_{\mathbb{Q}} & \xrightarrow{\varphi_2} & E \longrightarrow 0 \\ & & & & \varphi_1 \uparrow & & \\ & & & & E & & \end{array}$$

Il induit une isogénie

$$\begin{aligned} \beta : E \times A &\rightarrow J_0(N)_{\mathbb{Q}} \\ (x, y) &\mapsto \varphi_1(x) - y \end{aligned}$$

dont le noyau est $A \cap \varphi_1(E)$. Ce noyau est isomorphe à $(\mathbb{Z}/\deg \varphi \mathbb{Z})^2$ car $\varphi_2 \circ \varphi_1$ est la multiplication par $\deg \varphi$ sur E .

On note $\text{End}^0(V) = \text{End}(V) \otimes_{\mathbb{Z}} \mathbb{Q}$ pour toute variété abélienne V . L'isogénie β induit la décomposition $\text{End}^0(J_0(N)_{\mathbb{Q}}) \simeq \text{End}^0(E) \times \text{End}^0(A)$. Soit e l'idempotent de $\text{End}^0(J_0(N)_{\mathbb{Q}})$ qui est l'identité sur E et 0 sur A . C'est un élément de $\mathbb{T}_{\mathbb{Q}} \subset \text{End}^0(J_0(N)_{\mathbb{Q}})$. Le lemme suivant est dû à Zagier [13]:

LEMME 3.2 (Zagier). (i) *Le dénominateur de e dans $\text{End}(J_0(N)_{\mathbb{Q}})$ (c'est à dire le plus petit entier positif m tel que $me \in \text{End}(J_0(N)_{\mathbb{Q}})$) est $\deg \varphi$.*

(i) *Le dénominateur de e dans $\mathbb{T}$ est r .*

(ii) *Le degré de la paramétrisation $\deg \varphi$ divise r . On a $r = \deg \varphi$ si N est premier.*

Preuve. Le (iii) découle de (i) et (ii) et de l'inclusion $\mathbb{T} \subset \text{End}(J_0(N)_{\mathbb{Q}})$ qui est une égalité si N est premier [6] (cette divisibilité a été annoncée dans l'autre sens dans [13]).

On montre le premier point (i) en utilisant l'isogénie β . le second (ii) est moins évident. On désigne par $\mathbb{T}'$ l'image de $\mathbb{T}$ dans $\text{End}^0(A)$ et par χ_E le caractère de $\mathbb{T}$ associé à la forme primitive f_E . Soit $\mathcal{B}$ le conoyau du morphisme $\mathbb{T} \rightarrow \mathbb{Z} \oplus \mathbb{T}'$ somme directe du caractère χ_E et du morphisme naturel de $\mathbb{T}$ dans $\mathbb{T}'$, c'est un groupe cyclique. Ce morphisme envoie un élément t de $\mathbb{T}$ sur le couple $(et, (1-e)t)$. On en déduit que le dénominateur de e dans $\mathbb{T}$ est $\#\mathcal{B}$. Le (ii) du Lemme 3.2 découle alors du lemme suivant:

LEMME 3.3. *On a l'égalité:*

$$\#\mathcal{B} = \#((\mathbb{Z} \oplus \mathbb{T}')/\mathbb{T}) = \#(S_{\mathbb{Z}}/(f_E \mathbb{Z} \oplus S_{\mathbb{Z}}(2, \Gamma_0(N)) \cap W(f_E))) = r.$$

Preuve. On considère la suite exacte:

$$0 \rightarrow \mathbb{T} \rightarrow \mathbb{Z} \oplus \mathbb{T}' \rightarrow \mathcal{B} \rightarrow 0 \quad (8)$$

et la suite duale:

$$0 \rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z} \oplus \mathbb{T}', \mathbb{Z}) \rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{T}, \mathbb{Z}) \rightarrow \text{Ext}_{\mathbb{Z}}^1(\mathcal{B}, \mathbb{Z}) \rightarrow 0 \quad (9)$$

Le Lemme 2.1 implique l'isomorphisme:

$$\mathcal{S}_{\mathbb{Z}} \xrightarrow{a_1} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, \mathbb{Z}).$$

Sous cette identification, on établit l'isomorphisme

$$f_E \mathbb{Z} \oplus \mathcal{S}_{\mathbb{Z}}(2, \Gamma_0(N)) \cap W(f_E) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z} \oplus \mathbb{T}', \mathbb{Z}).$$

Le Lemme 3.3 découle de la suite exacte (9) et de l'égalité $\#B = \#Ext_{\mathbb{Z}}^1(B, \mathbb{Z})$.

Preuve (du Théorème A). Soit p un nombre premier ne divisant pas N . La Proposition 3.3 implique que $v_p(\deg \varphi) + v_p(\#C) = v_p(r) + v_p(c_E) + v_p(\#D)$ où v_p est la valuation p -adique. La Proposition 3.4 implique que $v_p(\#C) = 0$. Par le Lemme 3.2, $\deg \varphi$ divise r . D'où

$$v_p(r) + v_p(c_E) + v_p(\#D) = v_p(\deg \varphi) \leq v_p(r).$$

Ceci montre que $v_p(c_E) = 0$ et termine la preuve du théorème. Il découle aussi que $v_p(\#D) = 0$ ce qui redonne pour les premiers ne divisant pas N la Proposition 3.2.

Appendice

A. Défaut d'exactitude des modèles de Néron semi-abéliens (d'après M. Raynaud)

Soit R un anneau de valuation discrète complet de corps de fractions K de caractéristique 0, de corps résiduel k de caractéristique $p > 0$ et d'indice de ramification absolu e .

Considérons une suite exacte de K -variétés abéliennes:

$$0 \rightarrow A_K \rightarrow B_K \rightarrow C_K \rightarrow 0$$

et les modèles de Néron sur R correspondants:

$$A \rightarrow B \rightarrow C.$$

On suppose que B est semi-abélien. Il en est donc de même de A et C . Le morphisme $B \rightarrow C$ est alors plat (mais pas nécessairement surjectif) et son noyau A' est donc égal à l'adhérence schématique de A_K dans B . Le morphisme $A \rightarrow B$ se factorise à travers A' et on a $A = A'$ si et seulement si A' est lisse, c'est à dire si le morphisme $B \rightarrow C$ est lisse, ou encore si le morphisme $\mathrm{Lie}(B) \rightarrow \mathrm{Lie}(C)$ est surjectif. C'est toujours le cas si $e < p - 1$ ([2] Théorème 4 p. 187). Le théorème suivant traite le cas limite $e = p - 1$, où on contrôle encore la situation.

THÉOREME A.1 (Raynaud). *Soit R un anneau de valuation discrète complet de corps de fractions K de caractéristique 0, de corps résiduel k de caractéristique $p > 0$ et d'indice de ramification absolu e . Soient $0 \rightarrow A_K \rightarrow B_K \rightarrow C_K \rightarrow 0$ une suite exacte de K -variétés abéliennes et les modèles de Néron sur R correspondants*

$A \rightarrow B \rightarrow C$. On suppose que B est semi-abélien et que $e = p - 1$. Alors il existe un entier r tel que la suite

$$0 \rightarrow \mathrm{Lie}(A) \rightarrow \mathrm{Lie}(B) \rightarrow \mathrm{Lie}(C) \rightarrow (R/pR)^r \rightarrow 0$$

est exacte.

On donnera des énoncés plus précis et plus techniques dans le cas où C_K est une courbe elliptique.

Tous les schémas en groupes considérés dans la suite sont commutatifs.

Soit G un R -schéma en groupes fini et plat annulé par une puissance de p . Il existe une suite exacte de R -schémas en groupes finis et plats:

$$0 \rightarrow G^c \rightarrow G \rightarrow G^{et} \rightarrow 0$$

où G^c est connexe et G^{et} est étale sur R . Le sous-schéma en groupes G^c est ouvert et fermé, il est le plus grand sous-schéma en groupes connexe contenu dans G .

On désigne par G^μ le plus grand sous-schéma en groupes de G de type multiplicatif. G^μ et G^{et} s'échangent par dualité de Cartier. Comme G est d'ordre une puissance de p , G^μ est connexe. On a donc la filtration en trois crans:

$$0 \subset G^\mu \subset G^c \subset G.$$

On désigne par G^b (b pour biconnexe) le quotient intermédiaire G^c/G^μ .

Si $u : G \rightarrow H$ est un morphisme entre deux R -schémas en groupes finis et plats, u est compatible avec les filtrations précédentes. En effet, il est clair pour des raisons topologiques que u envoie G^c dans H^c . Par dualité, on trouve que $u_{/G^\mu}$ se factorise à travers H^μ . Rappelons que lorsque $e < p - 1$, la catégorie des R -schémas en groupes finis et plats est abélienne et le foncteur $G \rightarrow G_K$ est pleinement fidèle ([9] Corollaire 3.3.6).

Lorsque $e = p - 1$, il est encore vrai que le foncteur $G \rightarrow G_K$ est pleinement fidèle à condition de se limiter:

- soit à la catégorie (*) des R -schémas en groupes connexes (i.e. $G^{et} = 0$)
- soit à la catégorie (**) duale de la précédente (i.e. $G^\mu = 0$).

Ceci résulte facilement de [9] par dévissage de la Proposition 3.3.2–3) et de 3.3.7.

En revanche si on accepte à la fois des groupes étales et des groupes de type multiplicatif, on perd la pleine fidélité. En effet, R contient les racines p -èmes de 1, et on peut envoyer $\mathbb{Z}/p\mathbb{Z}$ dans μ_p en envoyant 1 sur une racine d'ordre p . La flèche obtenue est alors un isomorphisme sur K sans être un isomorphisme sur R .

Il est commode de dire qu'un K -schéma en groupes fini est de type étale (resp. connexe, resp. multiplicatif, resp. biconnexe) s'il se prolonge en un R -schéma en groupes fini et plat étale (resp. connexe, resp. multiplicatif, resp. biconnexe). *Un K -schéma en groupes peut donc être à la fois de type multiplicatif et de type étale,*

mais alors il est nécessairement annulé par p car un hensélisé strict de R ne contient pas les racines p^2 -èmes de 1.

Un S -groupe p -divisible, où S est un schéma, est un système inductif $G = \varinjlim G(n)$, où $G(n)$ est un schéma en groupes fini et plat annulé par p^n , et où les flèches de transition sont des monomorphismes qui s'insèrent dans des suites exactes courtes fppf:

$$0 \rightarrow G(n) \rightarrow G(n+m) \rightarrow G(m) \rightarrow 0.$$

$$g \quad \rightarrow \quad p^n g.$$

Nous dirons qu'un K -groupe p -divisible est de type entier (resp. étale, resp. connexe, resp. multiplicatif, resp. biconnexe) s'il est la fibre générique d'un R -groupe p -divisible (resp. d'un R -groupe p -divisible étale, resp. connexe, resp. multiplicatif, resp. biconnexe).

Rappelons le résultat fondamental de J. Tate ([12] Théorème 4): *le foncteur $G \mapsto G_K$ des R -groupes p -divisibles dans les K -groupes p -divisibles est pleinement fidèle.*

En particulier lorsqu'un K -groupe p -divisible a un type celui-ci est unique, contrairement à ce qui peut se passer pour un groupe fini. Notons aussi que le type est invariant par isogénie.

Soit A le R -modèle de Néron d'un K -schéma abélien A_K . On suppose A semi-abélien.

Soit $A(n)$ le noyau de la multiplication par p^n dans A . C'est un schéma en groupes quasi-fini et plat. Notons $A(n)^f$ la partie finie de $A(n)$. $A(n)^f$ possède une filtration en trois crans $A(n)^\mu \subset A(n)^c \subset A(n)^f$. On désigne par $A(\infty)$ (resp. $A_K(\infty)$) le système inductif formé par les $A(n)$ (resp. $A_K(n)$). On définit les systèmes inductifs

$$A^\mu = \varinjlim A(n)^\mu \quad A^c = \varinjlim A(n)^c \quad A^b = \varinjlim A(n)^b$$

Alors on a une suite exacte de R -groupes p -divisibles:

$$0 \rightarrow A^\mu \rightarrow A^c \rightarrow A^b \rightarrow 0.$$

Par passage à la fibre générique on obtient une filtration du K -groupe p -divisible $A_K(\infty)$:

$$0 \subset (A^\mu)_K \subset (A^c)_K \subset A_K(\infty)$$

LEMME A.1. *Soit A un R -schéma semi-abélien. Alors le quotient $A_K(\infty)/(A^c)_K$ est de type étale. On le note $A_K^{\text{ét}}$.*

Preuve. La fibre spéciale connexe A_k^0 de A est extension d'une variété abélienne A'_k de dimension a' par un tore T_k de dimension t . Soit a la dimension de A_K qui est aussi la dimension de A_k : $a = t + a'$.

On désigne par $A'_k(\infty)$ le k -groupe p -divisible des points de p -torsion de A'_k et par $0 \subset (A'_k)^\mu \subset (A'_k)^c \subset A'_k(\infty)$ sa filtration canonique. Soit m' la hauteur

de $(A'_k)^\mu$. Comme A'_k est isogène à sa duale, $(A'_k)^{et}$ est aussi de hauteur m' et par suite $(A'_k)^b$ est de hauteur $2a' - 2m'$.

On a les suites exactes:

$$0 \rightarrow T_k(\infty) \rightarrow A_k(\infty) \rightarrow A'_k(\infty) \rightarrow 0,$$

$$0 \rightarrow T_k(\infty) \rightarrow (A_k)^\mu \rightarrow (A'_k)^\mu \rightarrow 0.$$

La hauteur de $(A^\mu)_k = (A_k)^\mu$ est donc $t + m'$. Finalement A^c est de hauteur $t + m' + 2a' - 2m' = t + 2a' - m' = 2a - (t + m')$.

On désigne par E_K le dual de Cartier de $((A^\vee)^\mu)_K$ où $A^\vee$ est le R -modèle de Néron de la variété duale de A_K . C'est un quotient de type étale de $A_K(\infty)$. Comme A_K est isogène à sa duale, E_K est de hauteur $t + m'$. Le K -morphisme de $(A^c)_K$ dans E_K se prolonge par le théorème de Tate (rappelé au début de cette section) en un R -morphisme de A^c dans un R -groupe p -divisible étale, il est donc nul. D'où une flèche surjective de $A_K(\infty)/(A^c)_K$ dans E_K . Comme ces deux groupes p -divisibles ont la même hauteur $t + m'$, cette flèche est un isomorphisme.

Remarque. Si A_K n'a pas bonne réduction $A_K(\infty)$ n'est pas de type entier. Considérons une suite exacte de K -variétés abéliennes:

$$0 \rightarrow A_K \rightarrow B_K \rightarrow C_K \rightarrow 0$$

et la suite des R -modèles de Néron correspondants supposés semi-abéliens:

$$A \rightarrow B \rightarrow C.$$

On a une suite exacte de K -groupes p -divisibles:

$$0 \rightarrow A_K(\infty) \rightarrow B_K(\infty) \rightarrow C_K(\infty) \rightarrow 0$$

et une filtration de $B_K(\infty)$ en trois crans:

$$0 \subset (B^\mu)_K \subset (B^c)_K \subset B_K(\infty)$$

dont les quotients successifs sont respectivement de type multiplicatif, biconnexe et étale (Lemme A.1). Cette filtration induit sur $A_K(\infty)$ une filtration par des groupes qui ne sont pas nécessairement divisibles. C'est ce phénomène qui va entraîner le défaut de lissité de la flèche $B \rightarrow C$.

LEMME A.2. *Les flèches $B^\mu \rightarrow C^\mu$ et $B^c \rightarrow C^c$ sont des épimorphismes de groupes p -divisibles (c'est à dire que les morphismes correspondant de groupes formels sont fidèlement plats).*

Preuve. Les épimorphismes de groupes p -divisibles découlent du fait que C^0 est un quotient plat de B^0 .

LEMME A.3. (i) $(B^c)_K \cap A_K(\infty)$ est extension d'un groupe fini de type étale E_K annulé par p , par $(A^c)_K$.

- (ii) $(B^\mu)_K \cap A_K(\infty)$ est extension d'un groupe fini F_K par $(A^\mu)_K$; le morphisme canonique $F_K \rightarrow E_K$ est un isomorphisme. En particulier F_K est de type étale.
- (iii) Les morphismes $A^\mu \rightarrow B^\mu$, $A^b \rightarrow B^b$ et $A^c \rightarrow B^c$ sont des immersions fermées.

Preuve. (i) Il existe un K -groupe p -divisible L_K et un épimorphisme:

$$(B^c)_K \cap A_K(\infty)/(A^c)_K \rightarrow L_K \rightarrow 0$$

tels que tout morphisme de $(B^c)_K \cap A_K(\infty)/(A^c)_K$ dans un K -groupe p -divisible se factorise à travers L_K . L_K est de type entier car pour tout n , $L_K(n)$ est la fibre générique d'un R -schéma en groupes fini et plat [9]. On désigne par L le R -groupe p -divisible de fibre générique L_K . Le morphisme

$$(B^c)_K \cap A_K(\infty)/(A^c)_K \rightarrow A_K(\infty)/(A^c)_K$$

induit un monomorphisme de K -groupes p -divisibles $L_K \rightarrow A_K(\infty)/(A^c)_K$ et par suite un morphisme de L dans un R -groupe p -divisible étale. La composante connexe L^c s'envoie sur 0, elle est donc nulle. De même le morphisme:

$$(B^c)_K \cap A_K(\infty)/(A^c)_K \rightarrow (B^c)_K/(A^c)_K$$

induit un monomorphisme $L_K \rightarrow (B^c)_K/(A^c)_K$ et donc un morphisme de L dans un R -groupe p -divisible connexe. Ce morphisme est nul car L est étale. Ceci montre que L_K est nul. La composante divisible de $(B^c)_K \cap A_K(\infty)$ est donc $(A^c)_K$. Le quotient fini $(B^c)_K \cap A_K(\infty)/(A^c)_K = E_K$ est à la fois de type connexe et étale (car contenu dans $A_K(\infty)/(A^c)_K$). Il est donc annulé par p .

(ii) On prouve de même que les quotients $(B^\mu)_K \cap (A^c)_K/(A^\mu)_K$ et $(B^\mu)_K \cap A_K(\infty)/(A^c)_K$ sont finis. On en déduit que la composante p -divisible de $(B^\mu)_K \cap A_K(\infty)$ est $(A^\mu)_K$. Considérons le diagramme:

$$\begin{array}{ccccccc} 0 & \longrightarrow & (A^\mu)_K & \longrightarrow & (B^\mu)_K \cap A_K(\infty) & \longrightarrow & F_K \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & (A^c)_K & \longrightarrow & (B^c)_K \cap A_K(\infty) & \longrightarrow & E_K \longrightarrow 0 \end{array}$$

Le quotient $(B^c)_K \cap A_K(\infty)/(B^\mu)_K \cap A_K(\infty)$ est contenu dans $(B^b)_K$, en particulier, il n'a pas de quotient non nul de type étale. On en déduit que la flèche canonique

$$(A^b)_K \rightarrow (B^c)_K \cap A_K(\infty)/(B^\mu)_K \cap A_K(\infty)$$

est un isomorphisme. Par le lemme du serpent le morphisme naturel $E_K \rightarrow F_K$ est aussi un isomorphisme.

(iii) se teste sur la fibre générique puisqu'on est dans la catégorie (*).

Notons p^r le rang de F_K de sorte que sur l'extension maximale non ramifiée de K , F_K devient isomorphe à $(\mathbb{Z}/p\mathbb{Z})^r$.

Rappelons qu'on a un isomorphisme canonique entre R -modules libres:

$$\varprojlim s^* \Omega_{A(n)^c/R}^1 \rightarrow s^* \Omega_{A/R}^1$$

(s est la section unité) ou encore une identification entre leurs duals sur R : $\text{Lie}(A^c) = \text{Lie}(A)$. On a aussi la suite exacte de R -modules libres:

$$0 \rightarrow \text{Lie}(A^\mu) \rightarrow \text{Lie}(A^c) \rightarrow \text{Lie}(A^b) \rightarrow 0$$

et des suites exactes analogues pour B et C .

Preuve. (du Théorème A.1). Le théorème découle des deux suites exactes

$$0 \rightarrow \text{Lie}(A^b) \rightarrow \text{Lie}(B^b) \rightarrow \text{Lie}(C^b) \rightarrow 0, \quad (10)$$

$$0 \rightarrow \text{Lie}(A^\mu) \rightarrow \text{Lie}(B^\mu) \rightarrow \text{Lie}(C^\mu) \rightarrow (R/pR)^r \rightarrow 0. \quad (11)$$

La suite exacte (10) résulte de l'assertion correspondante sur les groupes p -divisibles:

$$0 \rightarrow A^b \rightarrow B^b \rightarrow C^b \rightarrow 0. \quad (12)$$

En effet $A^b \rightarrow B^b$ est une immersion fermée et $B^b \rightarrow C^b$ est un épimorphisme. D'autre part, il résulte de la preuve du Lemme A.3 que la suite $0 \rightarrow (A^b)_K \rightarrow (B^b)_K \rightarrow (C^b)_K \rightarrow 0$ est exacte. D'où la hauteur de B^b (qui est aussi la hauteur de $(B^b)_K$) est la somme des hauteurs de A^b et de C^b . On en déduit l'exactitude au centre de la suite (12).

Soient $H(n)$ le noyau du morphisme $B(n)^\mu \rightarrow C(n)^\mu$ et H la limite inductive des $H(n)$. Pour tout n , $H(n)$ est un schéma en groupes fini et plat sur R . On a les suites exactes:

$$0 \rightarrow H \rightarrow B^\mu \rightarrow C^\mu \rightarrow 0$$

$$0 \rightarrow A^\mu \rightarrow H \rightarrow F \rightarrow 0$$

où F est un groupe multiplicatif annulé par p par le Lemme A.3 (ii). La suite exacte (11) découle de ces deux suites exactes et du fait que le R -module des différentielles invariantes de μ_{p^n} est $R/p^n R$.

COROLLAIRE A.1. *Les conditions suivantes sont équivalentes:*

- (1) $\text{Lie}(B) \rightarrow \text{Lie}(C)$ est surjectif.
- (2) $B \rightarrow C$ est lisse.
- (3) Le noyau de $B^\mu \rightarrow C^\mu$ est p -divisible (et est alors A^μ).
- (4) $(B(1)^\mu)_K \cap A_K(\infty) = (A(1)^\mu)_K$.

(5) $(B(1)^\mu)_K \rightarrow (C(1)^\mu)_K$ est surjectif.

(6) $A_K^{\text{ét}} \rightarrow B_K^{\text{ét}}$ est injectif.

(7) $A_K^{\text{ét}}(1) \rightarrow B_K^{\text{ét}}(1)$ est injectif.

Preuve. L'équivalence de (1) et (2) est claire et on a vu qu'elle est équivalente à (3). Les conditions (4) et (5) sont des reformulations de (3). La condition (6) équivaut à (3) compte-tenu de l'isomorphisme $F_K \xrightarrow{\sim} E_K$ du Lemme A.3. La condition (7) est une reformulation de (6).

COROLLAIRE A.2. Soit $0 \rightarrow (C_K)^\vee \rightarrow (B_K)^\vee \rightarrow (A_K)^\vee \rightarrow 0$ la suite exacte duale de la précédente et $C^\vee$, $B^\vee$ et $A^\vee$ les R -modèles de Néron correspondants. Alors $B \rightarrow C$ est lisse si et seulement si $B^\vee \rightarrow A^\vee$ est lisse.

Preuve. La condition (5) du Corollaire A.1 devient par dualité la condition (7) pour la suite duale.

COROLLAIRE A.3. $\text{Lie}(B) \rightarrow \text{Lie}(C)$ est surjectif dans les cas suivants:

- (i) Le plus grand sous-groupe de $A_K(1)$ non ramifié sur R est égal à $(A(1)^\mu)_K$. C'est en particulier le cas si $A_K^{\text{ét}} = 0$.
- (ii) Le plus grand quotient de $C_K(1)$ non ramifié sur R est $C_K^{\text{ét}}(1)$. C'est en particulier le cas si $C^\mu = 0$.

Les conditions (i) et (ii) s'échangent par dualité compte-tenu du fait que C^μ est nul si et seulement si $(C^\vee)_K^{\text{ét}} = 0$.

COROLLAIRE A.4. Supposons que C_K est une courbe elliptique. Alors $\text{Lie}(B) \rightarrow \text{Lie}(C)$ est surjectif sauf peut être si $C_K(1)$ est non ramifié sur R . Il revient au même de dire que $\text{Lie}(B) \rightarrow \text{Lie}(C)$ est surjectif sauf peut être dans les cas suivants:

- (i) C est une courbe elliptique à réduction ordinaire telle que $C(1)$ soit produit d'un groupe étale par un groupe de type multiplicatif (comme dans un relèvement canonique de Serre-Tate),
- (ii) C_K à réduction torique et (sur l'hensélisé strict de R), la période q 'à la Tate' est une puissance p -ème

Preuve. Une courbe elliptique est auto-duale et on applique la condition (ii) du Corollaire A.3.

Remerciements

Nous remercions M. Raynaud pour son aide et d'avoir accepté que nous publiions sa lettre. Nous sommes très reconnaissant à B. Edixhoven et J. Tilouine pour leurs remarques et commentaires qui ont été d'une grande utilité pour l'élaboration de ce travail.

References

1. Atkin, A. O. L. and Lehner, J.: Hecke operators on $\Gamma_0(m)$, *Math. Ann.* 185 (1970), 134–160.

2. Bosch, S., Lütkebohmert, W., and Raynaud, M.: *Néron Models*, Springer-Verlag, New York, 1990.
3. Carayol, H.: Sur les représentations l -adiques associées aux formes modulaires de Hilbert, *Ann. Sc. Ens* 19 (1986), 409–468.
4. Deligne, P., and Rapoport, M.: *Schémas de modules des courbes elliptiques, dans Modular functions of one variable II*, Lectures Notes in Mathematics 349, Springer-Verlag, New York, 1973.
5. Edixhoven, B.: On the Manin constants of modular elliptic curves, in: *Arithmetic algebraic geometry*, Progress in Math. 89, pp. 25–39, Birkhäuser, 1989.
6. Mazur, B.: Modular curves and the Eisenstein ideal, *Pub. Math. IHES* 47 (1977), 33–186.
7. Mazur, B.: *Courbes Elliptiques et Symboles Modulaires*, Séminaire Bourbaki, exposé 414, Juin 1972.
8. Mazur, B.: Rational isogenies of prime degree, *Invent. Math.* 44 (1978), 129–162.
9. Raynaud, M.: Schémas en groupes de type $(p, \dots, p)$, *Bul. S.M.F. t.* 102 (1974), 241–280.
10. Ribet, K.: Endomorphisms of semi-stable abelian varieties over number fields, *Ann. of Math.* 101 (1975), 555–562.
11. Shimura, G.: *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten, Publishers and Princeton University Press, 1971.
12. Tate, J.: *p -Divisible groups*, Proceedings of a conference on local fields, Nuffic summer school Driebergen, 1966, pp. 158–183.
13. Zagier, D.: Modular parametrizations of elliptic curves, *Canad. Math. Bull.* 28 (3) (1985), 372–384.